From: Young, Brian A. (OPCL)
Subject: RE: Privacy Forum - Surveillance Technologies Panel - RESCHEDULED for October 25
To: O'Shea, Michael
Sent: September 28, 2016 9:03 AM (UTC-04:00)

Great! Thanks very much, Mike.

I'll be in touch regarding next steps.

-Brian

Brian A. Young
Senior Counsel
Office of Privacy and Civil Liberties (OPCL)
U.S. Department of Justice
(b) (6) (office)
(b) (6) (mobile)
(202) 307-0693 (fax)
SECRET: (b) (6)
TS: (b) (6)

From: O'Shea, Michael
Sent: Tuesday, September 27, 2016 5:37 PM
To: Young, Brian A. (OPCL)
Subject: Re: Privacy Forum - Surveillance Technologies Panel - RESCHEDULED for October 25

Duplicative Information - See Document ID 0.7.12327.58002

From: Young, Brian A. (OPCL)
Subject: RE: Privacy Forum - Surveillance Technologies Panel - RESCHEDULED for October 25
To: Young, Brian A. (OPCL)
Sent: September 29, 2016 10:49 AM (UTC-04:00)

Chris's number is (b) (6)

Brian A. Young
Senior Counsel
Office of Privacy and Civil Liberties (OPCL)
U.S. Department of Justice
(b) (6) (office)
(b) (6) (mobile)
(202) 307-0693 (fax)
SECRET: (b) (6)
TS: (b) (6)

From: Young, Brian A. (OPCL)
Sent: Wednesday, September 28, 2016 8:26 AM
To: Quinn, Maura F. (DEA); Gleason, Robert (Chris) (DEA)
Subject: RE: Privacy Forum - Surveillance Technologies Panel - RESCHEDULED for October 25

From: Mogil, Joshua (ODAG)
Subject: Privacy Forum 10/25
To: Bruck, Andrew J. (ODAG)
Sent: September 29, 2016 12:21 PM (UTC-04:00)
Attached: Tuesday- Privacy Forum Remarks.docx

Erika wrote these for last winter, when the DAG was slated to do this. It got delayed a few more times, but here is the draft that Erika wrote.

<<Tuesday- Privacy Forum Remarks.docx>>

From: Young, Brian A. (OPCL)
Subject: RE: Privacy Forum - Surveillance Technologies Panel - RESCHEDULED for October 25
To: Gleason, Robert (Chris) (DEA)
Cc: (b)(6), (7)(C), (7)(F) per DEA (DEA)
Sent: October 5, 2016 9:02 AM (UTC-04:00)

Thanks Chris.

And thank you very much, (b)(6), (7)(C), for agreeing to help us!

I'll be in touch about scheduling a planning call.

-Brian

Brian A. Young
Senior Counsel
Office of Privacy and Civil Liberties (OPCL)
U.S. Department of Justice
(b) (6) (office)
(b) (6) (mobile)
(202) 307-0693 (fax)
SECRET: (b) (6)
TS: (b) (6)

From: Gleason, Robert (Chris) [mailto:(b) (6)]
Sent: Wednesday, October 05, 2016 7:37 AM
To: Young, Brian A. (OPCL)
Cc: (b)(6), (7)(C), (7)(F) per DEA (DEA)
Subject: RE: Privacy Forum - Surveillance Technologies Panel - RESCHEDULED for October 25

Good morning, Brian,

(b)(6), (7)(C), (7)(F) per DEA will represent DEA at the forum. She is the Acting Chief of our Technology Law Unit and will do an outstanding job on the panel.

Best,

Chris Gleason

From: Young, Brian A. (OPCL) (JMD)
Sent: Monday, October 03, 2016 10:04 AM
To: Gleason, Robert (Chris)
Subject: RE: Privacy Forum - Surveillance Technologies Panel - RESCHEDULED for October 25

Hi Chris.

Thanks so much for getting back to me. Yes, it's the same general plan for how the panel will go. I'd like to have at least one, maybe two planning calls with the panelists before the forum. So the sooner you could let me know who will be the panelist, the better.

Thanks again,
Brian

Brian A. Young
Senior Counsel
Office of Privacy and Civil Liberties (OPCL)
U.S. Department of Justice
(b) (6) (office)
(b) (6) (mobile)
(202) 307-0693 (fax)
SECRET: (b) (6)
TS: (b) (6)

From: Gleason, Robert (Chris) [mailto:(b)(6), (7)(C) per DEA]
Sent: Monday, October 03, 2016 10:00 AM
To: Young, Brian A. (OPCL)
Subject: Re: Privacy Forum - Surveillance Technologies Panel - RESCHEDULED for October 25

Hi, Brian,

I am not in the office today, but we have discussed the forum. We will be able to participate in it. We are in the process of identifying who that will be, and I will let you know ASAP. I have seen the "script" that you had worked out with Maura Quinn and the other the panel members before the January date. Is that still your basic plan for how this will go?

Sent from my iPhone

On Oct 3, 2016, at 9:43 AM, Young, Brian A. (OPCL) (JMD) <(b) (6) > wrote:

> Hi Chris.
>
> Is there a good time I can give you a call about this either today or tomorrow?
>
> Thanks,
> Brian
>
> Brian A. Young
> Senior Counsel
> Office of Privacy and Civil Liberties (OPCL)
> U.S. Department of Justice
> (b) (6) (office)
> (b) (6) (mobile)
> (202) 307-0693 (fax)
> SECRET: (b) (6)
> TS: (b) (6)
>
>

From: Young, Brian A. (OPCL)
Sent: Wednesday, September 28, 2016 8:26 AM
To: Quinn, Maura F. (DEA); Gleason, Robert (Chris) (DEA)
Subject: RE: Privacy Forum - Surveillance Technologies Panel - RESCHEDULED for October 25

Duplicative Information - See Document ID 0.7.12327.58005

From: Lane Scott, Kristi Z (OPCL)
Subject: DAG Privacy Forum Remarks Draft (1-21-16) (AAP edits)
To: Winn, Peter A. (OPCL)
Sent: October 5, 2016 3:58 PM (UTC-04:00)
Attached: DAG Privacy Forum Remarks Draft (1-21-16) (AAP edits).docx

From: Winn, Peter A. (OPCL)
Subject: FW: DAG Privacy Forum Remarks Draft (1-21-16) (AAP edits)
To: Lane Scott, Kristi Z (OPCL)
Sent: October 11, 2016 4:57 PM (UTC-04:00)
Attached: DAG Privacy Forum Remarks Draft (1-21-16) (AAP edits).docx

Is this the latest draft? If so, I will edit it tonight and get it to you in the morning, so we can get it to Erika by COB Wednesday (tomorrow).

Peter

From: Lane Scott, Kristi Z (OPCL)
Sent: Wednesday, October 05, 2016 3:58 PM
To: Winn, Peter A. (OPCL)
Subject: DAG Privacy Forum Remarks Draft (1-21-16) (AAP edits)

From: Winn, Peter A. (OPCL)
Subject: DAG Remarks
To: Lane Scott, Kristi Z (OPCL)
Sent: October 12, 2016 4:01 PM (UTC-04:00)
Attached: DAG Privacy Forum Remarks PAW Edits.docx

I suggest you add something about (b) (5) and any other items you can think would be important. I didn't try to come up with the language because you know these issues better than I do.

Peter

Peter A. Winn
Director, Office of Privacy and Civil Liberties
United States Department of Justice
National Place Building, Suite 1000
1331 Pennsylvania Avenue, NW
Washington DC 20530
Office (b) (6)
Cell (b) (6)
Fax (202) 307-0693
(b) (6)

From: Young, Brian A. (OPCL)
Subject: RE: Privacy Forum - Surveillance Technologies Panel - RESCHEDULED for October 25
To: Douglass, Sean (OLP)
Sent: October 13, 2016 11:07 AM (UTC-04:00)

Hi Sean.

When you get a chance, if you could please send me a bio of yourself, that would be great.

Talk to you this afternoon.

Thanks,
Brian

Brian A. Young
Senior Counsel
Office of Privacy and Civil Liberties (OPCL)
U.S. Department of Justice
(b) (6) (office)
(b) (6) (mobile)
(202) 307-0693 (fax)
SECRET: (b) (6)
TS: (b) (6)

From: Douglass, Sean (OLP)
Sent: Tuesday, September 27, 2016 4:24 PM
To: Young, Brian A. (OPCL)
Cc: Winn, Peter A. (OPCL); Lane Scott, Kristi Z (OPCL); Quinn, Maura F. (DEA); Bordley, Ed (USMS); O'Shea, Michael
Subject: RE: Privacy Forum - Surveillance Technologies Panel - RESCHEDULED for October 25

From: Winn, Peter A. (OPCL)
Subject: DAG Remarks
To: Young, Brian A. (OPCL)
Sent: October 14, 2016 1:32 PM (UTC-04:00)
Attached: DAG Privacy Forum Remarks PAW Edits.docx

As discussed.

Peter A. Winn
Director, Office of Privacy and Civil Liberties
United States Department of Justice
National Place Building, Suite 1000
1331 Pennsylvania Avenue, NW
Washington DC 20530
Office (b) (6)
Cell (b) (6)
Fax (202) 307-0693
(b) (6)

From: Young, Brian A. (OPCL)
Subject: RE: DAG Remarks
To: Winn, Peter A. (OPCL)
Sent: October 14, 2016 3:02 PM (UTC-04:00)
Attached: DAG Privacy Forum Remarks - bay edits 10-14-16.docx

Hi Peter.

My suggested edits are attached.

Thanks,
Brian

Brian A. Young
Senior Counsel
Office of Privacy and Civil Liberties (OPCL)
U.S. Department of Justice
(b) (6) (office)
(b) (6) (mobile)
(202) 307-0693 (fax)
SECRET: (b) (6)
TS: (b) (6)

From: Winn, Peter A. (OPCL)
Sent: Friday, October 14, 2016 1:32 PM
To: Young, Brian A. (OPCL)
Subject: DAG Remarks

Duplicative Information - See Document ID 0.7.12327.57468

From: Winn, Peter A. (OPCL)
Subject: OPCL Draft of DAG Remarks for Privacy Forum
To: Brown Lee, Erika (ODAG)
Cc: Lane Scott, Kristi Z (OPCL); Young, Brian A. (OPCL)
Sent: October 14, 2016 3:54 PM (UTC-04:00)
Attached: DAG Privacy Forum Remarks OPCL DRAFT.docx

Hi Erika,

Here is the OPCL draft of the DAG's remarks, for your review.

Peter

Peter A. Winn
Director, Office of Privacy and Civil Liberties
United States Department of Justice
National Place Building, Suite 1000
1331 Pennsylvania Avenue, NW
Washington DC 20530
Office (b) (6)
Cell (b) (6)
Fax (202) 307-0693
(b) (6)

From: Alvaro Bedoya
Subject: Confidential PDF
To: Brown Lee, Erika (ODAG)
Sent: October 13, 2016 1:38 PM (UTC-04:00)
Attached: The Perpetual Lineup_CONFIDENTIAL_LEE.pdf

Dear Erika,

As promised, here is a full draft of the report. Please know that this is highly confidential; thank you for making sure this PDF doesn't leak.

Most of the report focuses on state & local use, but we definitely talk about FBI a lot. The following 25 pages are the key pages on FBI NGI-IPS and FBI FACE Services:

1-10
15-16
22-24
82-85
121 (the FACE Services scorecard)
(94-96: Methodology of the scorecard for FBI FACE Services)

The information on FBI is culled primarily from GAO and from FOIA docs we got in response to roughly 100+ requests.

The *Washington Post* story on this goes live at 12:01am on Tuesday, October 18th, but the final version of the report won't be released until 8:30am that morning.

I'm available anytime tomorrow *other* than 10-12:30am and 2-2:30pm to talk. Just say the time and I'll get on the line.

I think it is highly likely that ACLU and other advocacy organizations may make a request to DOJ Civil Rights to act on the racial disparity issues raised by the report on the same day the report is released. ACLU is lead on that, though.

Best,
Alvaro

ALVARO M. BEDOYA
Executive Director | Center on Privacy & Technology
Georgetown University Law Center
O: (b) (6) | M: (b) (6)
E: (b) (6) | T: @alvarombedoya

Join our mailing list! Subscribe here.

THE PERPETUAL LINE-UP

UNREGULATED POLICE FACE RECOGNITION IN AMERICA

GEORGETOWN LAW
Center on Privacy & Technology

www.perpetuallineup.org

OCTOBER __, 2016

THE PERPETUAL LINE-UP

UNREGULATED POLICE FACE RECOGNITION IN AMERICA

GEORGETOWN LAW
Center on Privacy & Technology

Clare Garvie, *Associate*
Alvaro M. Bedoya, *Executive Director*
Jonathan Frankle, *Staff Technologist*

RESEARCH

Moriah Dougherty, *Research Assistant*
Katie Evans, *Associate*
Edward George, *Chief Research Assistant*
Sabrina McCubbin, *Research Assistant*
Harrison Rudolph, *Law Fellow*
Ilana Ullman, *Google Policy Fellow*
Sara Ainsworth, *Research Assistant*
David Houck, *Research Assistant*
Megan Iorio, *Research Assistant*
Matthew Kahn, *Research Assistant*
Eric Olson, *Research Assistant*
Jaime Petenko, *Research Assistant*
Kelly Singleton, *Research Assistant*

DESIGN

Rootid.in

www.perpetuallineup.org

OCTOBER __, 2016

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

There is a knock on your door. It's the police. There was a robbery in your neighborhood. They have a suspect in custody and an eyewitness. But they need your help: Will you come down to the station to stand in the line-up?

Most people would probably answer "no." This summer, the Government Accountability Office revealed that close to 64 million Americans do not have a say in the matter: 16 states let the FBI use face recognition technology to compare the faces of suspected criminals to their driver's license and ID photos, creating a virtual line-up of their state residents. In this line-up, it's not a human that points to the suspect—it's an algorithm.

But the FBI is only part of the story. Across the country, state and local police departments are building their own face recognition systems, many of them more advanced than the FBI's. We know very little about these systems. We don't know how they impact privacy and civil liberties. We don't know how they address accuracy problems. And we don't know how any of these systems—local, state, or federal—affect racial and ethnic minorities.

One in two American adults is in a law enforcement face recognition network.

This report closes these gaps. The result of a year-long investigation and over 100 records requests to police departments around the country, it is the most comprehensive survey to date of law enforcement face recognition and the risks that it poses to privacy, civil liberties, and civil rights. Combining FBI data with new information we obtained about state and local systems, we find that law enforcement face recognition affects over 117 million Americans. It is also unregulated. A few agencies have instituted meaningful protections to prevent the misuse the technology. In many more cases, it is out of control.

The benefits of face recognition are real. It has been used to catch violent criminals and fugitives. The law enforcement officers who use the technology are men and women of good faith. They do not want to invade our privacy or create a police state. They are simply using every tool available to protect the people that they are sworn to serve. Police use of face recognition is inevitable. This report does not aim to stop it.

Rather, this report offers a framework to reason through the very real risks that face recognition creates. It urges Congress and state legislatures to address these risks through commonsense regulation comparable to the Wiretap Act. These reforms must be accompanied by key actions by law enforcement, the National Institute of Standards and Technology (NIST), face recognition companies, and community leaders.

A. KEY FINDINGS

Our general findings are set forth below. Specific findings for 25 local and state law enforcement agencies can be found in the **City & State Backgrounders** (p. TK). Our **Face Recognition Scorecard** (p. TK) evaluates these agencies' impact on privacy, civil liberties, civil rights, transparency and accountability. The records underlying all of our conclusions are available online.

1. **Law enforcement face recognition networks include over 117 million Americans—and may soon include many more.** Face recognition is neither new nor rare. FBI face recognition searches are more common than federal court-ordered wiretaps. At least one out of four state or local police departments has the option to run face recognition searches through their or another agency's system. At least 26 states (and potentially as many as 30) allow law enforcement to run or request searches against their databases of driver's license and ID photos. Roughly one in two American adults has their photos searched this way.

2. **Different uses of face recognition create different risks. This report offers a framework to tell them apart.** A face recognition search conducted in the field to verify the identity of someone who has been legally stopped or arrested is different, in principle and effect, than an investigatory search of an ATM photo against a driver's license database, or continuous, real-time scans of people walking by a surveillance camera. The former is targeted and public. The latter are generalized and invisible. While some agencies, like the San Diego Association of Governments, limit themselves to more targeted use of the technology, others are embracing high and very high risk deployments.

3. **By tapping into driver's license databases, the FBI is using biometrics in a way it's never done before.** Historically, FBI fingerprint and DNA databases have been primarily or exclusively made up of information from *criminal* arrests or investigations. By running face recognition searches against 16 states' driver's license photo databases, the FBI has built a biometric network that primarily includes *law-abiding Americans*. This is unprecedented and highly problematic.

4. **Major police departments are exploring real-time face recognition, which lets police continuously scan the faces of pedestrians from street surveillance cameras.** Real-time face recognition seems like science fiction. It is real. Contract documents and agency statements show that at least five major police departments—including agencies in Chicago, Dallas, and Los Angeles—either claimed to run real-time face recognition off of street cameras, bought technology that can do so, or expressed a written interest in buying it. Nearly all major face recognition companies offer real-time software.

5. **Law enforcement face recognition is unregulated and in many instances out of control.** No state has passed a law comprehensively regulating police face recognition. We are not aware of any agency that requires warrants for searches or limits them to serious crimes. This has consequences. The Maricopa County Sheriff's Offices enrolled all of Honduras' driver's licenses and mug shots into its database. The Pinellas County Sheriff's Office system runs 8,000 monthly searches on the faces of seven million Florida drivers—without requiring that officers have even a reasonable suspicion before running a search. The county public defender reports that the Sheriff's Office has never disclosed the use of face recognition in *Brady* evidence.

6. **Most law enforcement agencies are not taking adequate steps to protect free speech.** There is a real risk that police face recognition will be used to stifle free speech. There is also a history of FBI and police surveillance of civil rights protests. Of the 52 agencies that we found to use (or have used) face recognition, we found only one, the Ohio Bureau of Criminal Investigation, whose face recognition use policy expressly prohibits its officers from using face recognition to track individuals engaging in political, religious, or other protected free speech.

7. **Most law enforcement agencies do little to ensure that their systems are accurate.** Face recognition is less accurate than fingerprinting, particularly when used in real-time or on large databases. Yet we found only two agencies, the San Francisco Police Department and the Seattle region's South Sound 911 that conditioned purchase of the technology on accuracy tests or thresholds. There is a need for testing. One major face recognition company, FaceFirst, publicly advertises a 95% accuracy rate but disclaims liability for failing to meet that threshold in contracts with the San Diego Association of Governments. Unfortunately, independent accuracy tests are voluntary and infrequent.

8. **The human backstop to accuracy is non-standardized and overstated.** Companies and police departments largely rely on police officers to decide whether a candidate photo is in fact a match. Yet a recent study showed that, without specialized training, human users make the wrong decision about a match half the time. We found only eight face recognition systems where specialized personnel reviewed and narrowed down potential matches. The training regime for examiners remains a work in progress.

9. **Face recognition will disproportionately affect African Americans. Many police departments do not realize that.** In a Frequently Asked Questions document, the Seattle Police Department says that its face recognition system "does not see race." Yet an FBI co-authored study suggests that face recognition may be less accurate on black people. Also, due to disproportionately high arrest rates, systems that rely on mug shot databases likely include a disproportionate number of African Americans. Despite these findings, there is no independent testing regime for racially biased error rates. In interviews, two major face recognition companies admitted that they did not run these tests internally, either.

Face recognition may be least accurate for those it is most likely to affect: African Americans.

10. **Agencies are keeping critical information from the public.** Ohio's face recognition system remained almost entirely unknown to the public for five years. The New York Police Department acknowledges using face recognition; press reports suggest it has an advanced system. Yet NYPD denied our records request entirely. The Los Angeles Police Department has repeatedly announced new face recognition initiatives—including a

"smart car" equipped with face recognition and real-time face recognition cameras—yet the agency claimed to have "no records responsive" to our document request. Of 52 agencies, only four (less than 10%) have a publicly available use policy. And only one agency, the San Diego Association of Governments, received legislative approval for its policy.

11. **Major face recognition systems are not audited for misuse.** Maryland's system, which includes the license photos of over two million residents, was launched in 2011. It has never been audited. The Pinellas County Sheriff's Office system is almost 15 years old and may be the most frequently used system in the country. When asked if his office audits searches for misuse, Sheriff Bob Gualtieri replied, "No, not really." Despite assurances to Congress, the FBI has not audited use of its face recognition system, either. Only nine of 52 agencies (17%) indicated that they log and audit their officers' face recognition searches for improper use. Of those, only one agency, the Michigan State Police, provided documentation showing that their audit regime was actually functional.

B. RECOMMENDATIONS

1. **Congress and state legislatures should pass commonsense laws to regulate law enforcement face recognition.** Such laws would require the FBI or the police to have a reasonable suspicion of criminal conduct prior to a face recognition search. After-the-fact investigative searches—which are invisible to the public—would be limited to felonies.

   Mug shots, not driver's license and ID photos, should be the default photo databases for face recognition, and they should be periodically scrubbed to eliminate the innocent. Except for identity theft and fraud cases, searches of license and ID photos should require a court order issued upon a showing of probable cause, and should be restricted to identity theft and serious crimes. If these searches are allowed, the public should be notified at their department of motor vehicles.

   If deployed pervasively on surveillance video or police-worn body cameras, real-time face recognition will redefine the nature of public spaces. At the moment, it is also inaccurate. 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.

Real-time face recognition will redefine the nature of public spaces. It should be strictly limited.

Use of face recognition to track people on the basis of their political or religious beliefs or their race or ethnicity should be banned. All face recognition use should be subject to public reporting and internal audits.

To lay the groundwork for future improvements in face recognition, Congress should provide funding to NIST to increase the frequency of accuracy tests, create standardized, independent testing for racially biased error rates, and create photo databases that facilitate such tests.

State and federal financial assistance for police face recognition systems should be contingent on public reporting, accuracy and bias tests, legislative approval—and public posting—of a face recognition use policy, and other standards in line with these recommendations.

A **Model Face Recognition Act**, for Congress or a state legislature, is included in the **Appendix**.

2. **The FBI and Department of Justice (DOJ) should require individualized suspicion for face recognition searches, limit those searches to certain crimes, and promote public oversight, internal accountability, and accuracy.** The FBI should refrain from searching driver's license and ID photos in the absence of express approval for those searches from a state legislature. If it proceeds with those searches, the FBI should restrict them to investigations of serious crimes where FBI officials have probable cause to implicate the search subject. The FBI should periodically scrub its mug shot database to eliminate the innocent, require reasonable suspicion for state searches of that database, and restrict those searches to investigations of felonies. Overall access to the database should be contingent on legislative approval of an agency's use policy. The FBI should audit all searches for misuse, and test its own face recognition system, and the state systems that the FBI accesses, for accuracy and racially biased error rates.

   The DOJ Civil Rights Division should evaluate the disparate impact of police face recognition, first in jurisdictions where it has open investigations and then in state and local law enforcement more broadly. DOJ should also develop procurement guidance for state and local agencies purchasing face recognition programs with federal funding.

   The FBI should be transparent about its use of face recognition. It should reverse its current proposal to exempt its face recognition system from key Privacy Act requirements. It should also publicly and annually identify the photo databases it searches and release statistics on the number and nature of searches, arrests, and the convictions stemming from those searches, and the crimes that those searches were used to investigate.

3. **State and local police should follow suit.** Many police departments have run searches of driver's license and ID photos without express legislative approval. Police should observe a moratorium on those searches until legislatures vote on whether or not to allow them.

   Police should develop use policies for face recognition, publicly post those policies, and seek approval for them from city councils or other local legislative bodies. City councils should involve their communities in deliberations regarding support for this technology, and consult with

privacy and civil liberties organizations in reviewing proposed use policies.

When buying software and hardware, police departments should condition purchase on accuracy and bias tests and periodic tests of the systems in operational conditions over the contract period. They should avoid sole source contracts and contracts that disclaim vendor responsibility for accuracy.

All agencies should implement audits to prevent and identify misuse and a system of trained face examiners to maximize accuracy. Regardless of their approach to contracting, all agencies should regularly test their systems for accuracy and bias.

A **Model Police Face Recognition Use Policy** is included in the **Appendix**.

4. **The National Institute of Standards and Technology (NIST) should expand the scope and frequency of accuracy tests, issue best practices for accuracy tests, and develop diverse photo sets for testing.** NIST should create regular tests for algorithmic bias on the basis of race, gender and age, increase the frequency of existing accuracy tests, develop tests that mirror law enforcement workflows, and deepen its focus on tests for real-time face recognition. To help empower others to conduct testing, NIST should develop a set of best practices for accuracy tests and develop and distribute new photo datasets to train and evaluate algorithms. To help efforts to diminish racially biased error rates, NIST should ensure that these datasets reflect the diversity of the American population.

5. **Face recognition companies should privately and publicly test their systems for algorithmic bias on the basis of race, gender, and age.** Companies should also voluntarily publish performance results for modern, publicly available benchmarks—giving police departments and city councils more bases upon which to draw comparisons.

6. **Community leaders should press police and the FBI to be transparent and work to enact policies to protect privacy, civil liberties, and civil rights.** Citizens are paying for police and FBI face recognition systems. They have a right to know how those systems are being used. If those agencies refuse, advocates should take them to court. Citizens should also press legislators and law enforcement agencies for laws and use policies that protect privacy, civil liberties, and civil rights, and prevent misuse and abuse. Law enforcement and legislatures will not act without concerted community action.

   This report provides the resources that citizens will need to effect this change. In addition to the **City and State Backgrounders** and the **Face Recognition Scorecard**, a list of questions that citizens can ask their elected representative or law enforcement agency is in the **Recommendations**.

II. INTRODUCTION

Figure TK. Chris Wilson at the University of South Florida campus. (Photo: Center on Privacy & Technology)

Chris Wilson is a soft-spoken Classics major working towards her second Bachelor's degree at the University of South Florida. She enjoys learning Latin and studying ancient Greece and Rome. "I'm a history nut," she says.

But Chris is not just a scholar—she is also a civil rights leader. For her, social justice is at the core of education: "A lot of students believe that we have to put up with the way things are—and that's not right." Chris sees it as her responsibility to "pop the bubble."

Earlier this year, Chris helped organize a protest against the treatment of black students at the Florida State Fair. In 2014, a 14 year-old honors student, Andrew Joseph III, had been killed by a passing car after being ejected by police from the Florida State Fair along with dozens of other students, most of them African American.[1]

[1] *See* Sara DiNatale, *Two years after Andrew Joseph III, 14, died outside the Florida State Fair, his parents' fight is just starting*, Tampa Bay Times (Feb. 4, 2016), http://www.tampabay.com/news/publicsafety/two-years-after-teenager-andrew-joseph-iii-died-outside-the-florida-state/2264205.

On February 7, 2016—the second anniversary of Andrew's death—Chris and three others locked themselves together just inside the fairground gates and called for a boycott. Police ordered them to leave. Chris and her friends stayed where they were.[2]

Figure TK. The protesters are arrested by the Hillsborough County Sheriff's Office for trespass.

Chris was arrested for trespass, a misdemeanor. The Hillsborough County Sheriff's Office took her to a local station, fingerprinted her, took her mug shot, and released her that evening. She had never been arrested before, and so she was informed that she was eligible for a special diversion program. She paid a fine, did community service, and the charges against her were dropped.

Chris was not told that as a result of her arrest, her mug shot has likely been added to not one, but two separate face recognition databases run by the FBI and the Pinellas County

[2] *Interview with Chris Wilson* (July 29, 2016) (notes on file with authors); *See also* WFTS Webteam, *Black Lives Matter protesters arrested at Florida State Fair*, WFTS Tampa Bay (Feb. 8, 2016), http://www.abcactionnews.com/news/local-news/black-lives-matter-protesters-arrested-at-state-fair.

Sheriff's Office.[3] These two databases alone are searched thousands of times a year by over 200 state, local, and federal law enforcement agencies.[4]

The next time Chris participates in a protest, the police won't need to ask her for her name in order to identify her. They won't need to talk to her at all. They only need to take her photo. FBI co-authored research suggests that these systems may be *least* accurate for African Americans, women, and young people aged 18 to 30.[5] Chris is 26. She is black. Unless she initiates a special court proceeding to expunge her record, she will be enrolled in these databases for the rest of her life.[6]

What happened to Chris doesn't affect only activists: Increasingly, law enforcement face recognition systems also search state driver's license and ID photo databases. In this way, roughly one out of every two American adults (48%) has had their photo enrolled in a criminal face recognition network.[7]

They may not know it, but Chris Wilson and over 117 million Americans are now part of a virtual, perpetual line-up. What does this mean for them? What does this mean for our society? Can police use face recognition to identify only suspected criminals—or can they use it to identify anyone they want? Can police use it to identify people participating in protests? How accurate is this technology, and does accuracy vary on the basis of race, gender or age? Can communities debate and vote on the use of this technology? Or is it being rolled out in secret?

---

[3] In September 2014, the Hillsborough County Sheriff's Office (HCSO) finalized a Memorandum of Understanding with the Pinellas County Sheriff's Office (PCSO) to enroll all existing and future mug shot photos in the PCSO face recognition database. *See* the Hillsborough County Sheriff's Office, *Memorandum of Understanding*, Document. 014030–014034 at 014031. PCSO staff confirmed that all new mug shots taken by the HCSO are enrolled in the PCSO database. *See Correspondence between Jake Ruberto, Technical Support Specialist, Pinellas County Sheriff's Office, and Clare Garvie* (July 28, 2016), Document p. 016831. The FBI has confirmed that Chris Wilson's arrest record is in the Next Generation Identification database, but has refused to indicate whether her mug shot was enrolled in the FBI's face recognition database, the Interstate Photo System. Florida is one of seven states that have the ability to search the Interstate Photo System. *See* U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 13 (May 2016).

[4] The GAO found that the FBI alone conducted 118,490 face recognition searches of its face recognition database, the Next Generation Interstate Photo System (NGI-IPS) from December 2011 to December 2015, and that states authorized to access to the system conducted 20,000 searches in the four years ending in December 2015. *See* U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 49, 12 (May 2016). The Pinellas County Sheriff's Office (PCSO) system is searched by 242 local, state and federal agencies around 8,000 times a month. *See* Pinellas County Sheriff's Office, *Face Analysis Comparison & Evaluation System: FACES Training 2015*, Document p. 014383–014417 at 014396.

[5] *See* Brendan Klare *et. al, Face Recognition Performance: Role of Demographic Information*, 7 IEEE Transactions on Info. Forensics and Sec. 1789, 1789 (Dec. 2012), https://assets.documentcloud.org/documents/2850196/Face-Recognition-Performance-Role-of-Demographic.pdf. In the report, co-author Richard W. Vorder Bruegge is identified as the FBI's subject matter expert for face recognition. *Id*. at 1801.

[6] *See* Ernest J. Babcock, *Privacy Impact Assessment for the Next Generation Identification (NGI) Interstate Photo System*, Federal Bureau of Investigation, Department of Justice (Sept. 2015), https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/interstate-photo-system (explaining that absent the request of a submitting agency or a court order, photos will be retained until the subject is 110 years of age, "or seven years after notification of death with biometric confirmation"); *Interview with Sheriff Bob Gualtieri and Jake Ruberto* (July 26, 2016) (notes on file with authors) (explaining that the PCSO system retains photos indefinitely in the absence of a court order).

[7] *See below* Figure TK and accompanying text.

FBI and police face recognition systems have been used to catch violent criminals and fugitives. Their value to public safety is real and compelling. But should these systems be used to track Chris Wilson? Should they be used to track you?

III. BACKGROUND

A. WHAT IS FACE RECOGNITION TECHNOLOGY?

Face recognition is the automated process of comparing two images of faces to determine whether they represent the same individual.

Before face recognition can identify someone, an algorithm must first find that person's face within the photo. This is called face detection. Once detected, a face is "normalized"—scaled, rotated, and aligned so that every face that the algorithm processes is in the same position. This makes it easier to compare the faces. Next, the algorithm extracts features from the face—characteristics that can be numerically quantified, like eye position or skin texture. Finally, the algorithm examines pairs of faces and issues a numerical score reflecting the similarity of their features.

Face recognition is inherently probabilistic: It does not produce binary "yes" or "no" answers, but rather identifies more likely or less likely matches.[8] Most police face recognition systems will output either the top few most similar photos or all photos above a certain similarity threshold. Law enforcement agencies call these photos "candidates" for further investigation.

Some facial features may be better indicators of similarity than others. Many face recognition algorithms figure out which features matter most through training. During training, an algorithm is given pairs of face images of the same person. Over time, the algorithm learns to pay more attention to the features that were the most reliable signals that the two images contained the same person.

If a training set skews towards a certain race, the algorithm may be better at identifying members of that group.

The make-up of a training set can influence the kinds of photos that an algorithm is most adept at examining. If a training set is skewed towards a certain race, the algorithm may be better at identifying members of that group as compared to individuals of other races.[9]

The mathematical machinery behind a face recognition algorithm can include millions of variables that are optimized in the process of training. This intricacy is what gives an algorithm the capacity to learn, but it also makes it very difficult for a human to examine an algorithm or generalize about its behavior.

B. THE UNIQUE RISKS OF FACE RECOGNITION

Most law enforcement technology tracks *your* technology—your car, your phone, or your computer. Biometric technology tracks your body.[10] The difference is significant.

[8] *See generally*, Joseph N. Pato and Lynette I. Millett, eds., *Biometric Recognition: Challenges and Opportunities,* 36–45 (National Academies Press 2010) (hereinafter "Pato Report").
[9] *See below* Section TK (racial bias section).

Americans change smartphones every two and a half years, and replace cars every five to six and a half years.[11] Fingerprints are proven to be stable for more than a decade, and are believed to be stable for life.[12] Separately, many states' driver's license renewal requirements ensure that state governments consistently have an up-to-date image of a driver's face.[13]

Face recognition allows tracking from far away, in secret, and on large numbers of people.

Here, we can begin to see how face recognition creates opportunities for tracking—and risks—that other biometrics, like fingerprints, do not. Along with names, faces are the most prominent identifiers in human society—online and offline. Our faces—not fingerprints—are on our driver's licenses, passports, social media pages, and online dating profiles. Except for extreme weather, holidays, and religious restrictions, it is generally not considered socially acceptable to cover one's face; often, it's illegal.[14] You only leave your fingerprints on the things you touch. When you walk outside, your face is captured by every smartphone and security camera pointed your way, whether or not you can see them.

Face recognition isn't just a different biometric; those differences allow for a different *kind of tracking* that can occur from far away, in secret, and on large numbers of people.

Professor Laura Donohue explains that up until the 21st century, governments used biometric identification in a discrete, one-time manner to identify specific individuals. This identification has usually required that person's proximity or cooperation—making the process transparent to that person. These identifications have typically occurred in the course of detention or in a secure government facility. Donohue refers to this form of biometric identification as Immediate Biometric Identification, or IBI. A prime example of IBI would be the practice of fingerprinting someone during booking for an arrest.

In its most advanced forms, face recognition allows for a different kind of tracking. Donohue calls it Remote Biometric Identification, or RBI. In RBI, the government uses biometric technology to identify multiple people in a continuous, ongoing manner. It can identify them from

---

[10] Technically, biometric technology also analyzes human behavior, such as gait or keystroke patterns. This report will not focus on this aspect of biometrics. *See* Pato Reportat 18 (defining biometrics as "the automated recognition of individuals based on their behavioral and biological characteristics.").

[11] *See* Thomas Gryta, *Americans Keep Their Cellphones Longer,* Wall Street Journal (Apr. 18, 2016), http://www.wsj.com/articles/americans-keep-their-cellphones-longer-1461007321 (average phone replaced every 28 months in Q4 2015, according to Citigroup); *Average Age of Light Vehicles in the U.S. Rises Slightly in 2015 to 11.5 years, IHS Reports*, IHS Markit (July 29, 2015), http://press.ihs.com/press-release/automotive/average-age-light-vehicles-us-rises-slightly-2015-115-years-ihs-reports (average length of new vehicle ownership is 77.8 months, used vehicle ownership 63 months).

[12] *See* Soweon Yoon and Anil K. Jain, *Longitudinal study of fingerprint recognition*, 112 Proc. of the Nat'l Acad. of Sci. 8556 (July 14, 2015) (establishing the stability of high quality fingerprints for at least 12 years; citing anecdotal belief in stability of fingerprints over a lifetime).

[13] *See generally Driver's License Renewal*, American Automobile Association, http://drivinglaws.aaa.com/tag/drivers-license-renewal/ (last visited Sept. 23, 2016) (showing that most states require driver's licenses to be renewed every four to eight years).

[14] *See e.g.,* Ga. Code Ann., § 16-11-38 (2010); La. Stat. Ann. § 14:313 (2011); N.Y. Penal Law § 240.35 (McKinney 2010); Va. Code Ann. § 18.2-422 (2006).

afar, in public spaces. Because of this, the government does not need to notify those people or get their consent. Identification can be done in secret.

This is not business as usual: This is a capability that is "significantly different from that which the government has held at any point in U.S. history."[15]

C. HOW DOES LAW ENFORCEMENT USE FACE RECOGNITION?

The first successful fully automated face recognition algorithm was developed in the early 1990s.[16] Today, law enforcement agencies mainly use face recognition for two purposes. **Face verification** seeks to confirm someone's claimed identity. **Face identification** seeks to identify an unknown face. This report focuses on face identification by state and local police and the FBI.

Figure TK. A California policeman displays a mobile face recognition app. (Photo: Sandy Huffaker/The New York Times/Redux)

[15] *See* Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 Minn. L. Rev. 407, 415 (2012). Professor Donohue notes that face recognition is just the first of a new generation of biometrics—including iris identification and gait analysis—that allow for RBI. *Id*. Of all of these technologies, however, face recognition is by far the most widely deployed.

[16] Matthew Turk & Alex Pentland, *Eigenfaces for Recognition*, 3 J. Cognitive Neurosci. 71, 72 (1991); *See also* A. Jay Goldstein, Leon D. Harmon, & Ann B. Lesk, *Identification of Human Faces*, 59 Proc. of the IEEE 748, 748 (1971). Attempts to automate aspects of face recognition go back decades earlier, but these techniques were not fully automated. Goldstein et al asked human jurors to examine images and manually identify and classify facial features (such as "eyebrow eight" and "chin profile") on scales from 1 to 5. A computer was then given a description of a target in the form of a list of features and asked to use the juror's coding to find a match. In contrast, Turk and Pentland created a computer program that automatically compares images of faces.

Law enforcement performs face identification for a variety of tasks. Here are four of the most common:

- **Stop and Identify.** On patrol, a police officer encounters someone who either refuses or is unable to identify herself. The officer takes her photo with a smartphone or a tablet, processes that photo through software installed on that device or on a squad car computer, and receives a near-instantaneous response from a face recognition system. That system may compare that "probe" photo to a database of mug shots, driver's license photos, or face images from unsolved crimes, also known as an "unsolved photo file." **(**As part of this process, the probe photo may also be enrolled in a database.) This process is known as field identification.

- **Arrest and Identify.** A person is arrested, fingerprinted and photographed for a mug shot. Police enroll that mug shot in their own face recognition database. Upon enrollment, the mug shot may be searched against the existing entries, which may include mug shots, license photos, and an unsolved photo file. Police may also submit the arrest record, including mug shot and fingerprints, to the FBI for inclusion in its face recognition database, where a similar search is run upon enrollment.

- **Investigate and Identify.** While investigating a crime, the police obtain a photo or video still of a suspect from a security camera, smartphone, or social media post—or they surreptitiously photograph the suspect. They use face recognition to search that image against a database of mug shots, driver's licenses, or an unsolved photo file and obtain a list of candidates for further investigation, or, in the case of the unsolved photo file, learn if the individual is wanted for another crime. Alternately, when police believe that a suspect is using a pseudonym, they search a mug shot of that suspect against these same databases.

- **Real-time Video Surveillance.** The police are looking for an individual or a small number of individuals. They upload images of those individuals to a "hot list." A face recognition program extracts faces from live video feeds of one or more security cameras and continuously compares them, in real-time, to the faces of the people on the hot list. Every person that walks by those security cameras is subjected to this process. When it finds a match, the system may send an alert to a nearby police officer. Today, real-time face recognition is computationally expensive and is not instantaneous.[17] Searches can also be run on archival video.

Face recognition is also used for **driver's license de-duplication**. In this process, a department of motor vehicles compares the face of every new applicant for a license or other identification document to the existing faces in its database, flagging individuals who may be using a pseudonym to obtain fraudulent identification. Suspects are referred to law enforcement.

[17] The task of sifting through dozens of high-resolution video frames each second and checking the faces that are found against databases of hundreds (let alone millions) of photos demands an enormous amount of expensive computing power. In the absence of this computing infrastructure, the video footage might need to be stored and processed minutes, hours, or even weeks later. Even when this infrastructure is available, the results will never be provided to an officer instantaneously—each step of the process, from recording the image and transmitting it to a computer to the face recognition itself takes a small but appreciable amount of time.

However, because de-duplication is typically conducted by DMVs, not law enforcement, this use of the technology will not be a focus of this report.

SIDEBAR 1: Face Recognition at the FBI

The FBI has used face recognition to support FBI and state and local police investigations since at least 2011.[18] The FBI hosts one of the largest face recognition databases in the country, the Next Generation Identification Interstate Photo System (NGI-IPS). It is also home to a unit, Facial Analysis, Comparison, and Evaluation (FACE) Services, that supports other FBI agents by running or requesting face recognition searches of the FBI face recognition database, other federal databases, and state driver's license photo and mug shot databases. (This report will refer to NGI-IPS as "the FBI face recognition database (NGI-IPS)," and will refer to FBI FACE Services as "the FBI face recognition unit (FACE Services)." The network of databases that the unit searches will be called "the FBI FACE Services network.")

The FBI face recognition database (NGI-IPS) is mostly made up of the mug shots accompanying criminal fingerprints submitted to the FBI by state, local, and federal law enforcement agencies. It contains nearly 25 million state and federal criminal photos.[19] Police in seven states can run face recognition searches against the FBI face recognition database, as can the FBI face recognition unit.[20]

The FBI face recognition unit (FACE Services) runs face recognition searches against a network of databases that includes 411.9 million photos. Over 185 million of these photos are drawn from 12 states that let the FBI to search their driver's license and other ID photos; another 50 million are from four additional states that let the FBI to search both driver's license photos and mug shots.[21] While we do not know the total number of individuals that those photos implicate, there are close to 64 million licensed drivers in those 16 states.[22]

The FBI is expanding the reach of the FACE Services network, but the details are murky. In October 2015, the FBI began a pilot program to search photos against the State Department's passport database, but it is unclear if the FBI is searching the photos of all 125 million U.S. passport holders, or if it is searching a subset of that database.[23]

---

[18] *See* U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 7, 15 (May 2016) (the Facial Analysis, Comparison, and Evaluation (FACE) Services unit began supporting investigations in August 2011).

[19] *See* U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 46 (May 2016). It also contains almost 5 million "civil photos," including photos submitted to the FBI for employment or immigration background checks, although these photos are not searched unless they are matched to people already enrolled in the criminal file. *See generally* Ernest J. Babcock, *Privacy Impact Assessment for the Next Generation Identification (NGI) Interstate Photo System*, Federal Bureau of Investigation, Department of Justice (Sept. 2015), https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/interstate-photo-system.

[20] U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 12–13 (May 2016).

[21] U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 47–48 (May 2016).

[22] *See* Federal Highway Administration, U.S. Department of Transportation, *Highway Statistics 2014* 5 (Sept. 2015), http://www.fhwa.dot.gov/policyinformation/statistics/2014/pdf/dl22.pdf.

[23] *See* U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 48 n. c (May 2016); U.S. Department of State, Bureau of Consular Affairs, *U.S. Passports & International Travel: Passport Statistics*,

In a May 2016 report, the Government Accountability Office reported that the FBI was negotiating with 18 additional states and the District of Columbia to access their driver's license photos. In August, the GAO re-released the report, deleting all references to the 18 states and stating that there were "no negotiations underway."[24] The FBI now suggests that FBI agents had only conducted outreach to those states to explore the possibility of their joining the FACE Services network.[25]

The GAO report found that the FBI had failed to issue mandatory privacy notices required by federal law, failed to conduct adequate accuracy testing of the FBI face recognition database (NGI-IPS) and the state databases that the FBI face recognition unit accessed, and failed to audit the state searches of the FBI face recognition database or any of the face recognition unit's searches.[26]

Despite these findings, the FBI is proposing to exempt the FBI face recognition database from key Privacy Act provisions that guarantee Americans the right to review and correct non-investigatory information held by law enforcement—and the right to sue if their privacy rights are violated.[27]

D. OUR RESEARCH

Thanks to the May 2016 Government Accountability Office report, the public now has access to basic information about the FBI's face recognition programs and their privacy and accuracy issues. (**Sidebar 1**.)

By comparison, the public knows very little about the use of face recognition by state and local police, even though many of their systems are older, used more aggressively, and more likely to have a greater impact on the average citizen. No one has combined what we know about FBI systems with information about state and local face recognition to paint a comprehensive, national picture of how face recognition is changing policing in America, and the impact of these changes on our rights and freedoms.

This report closes these gaps. It begins with a threshold question: What uses of face recognition present greater or fewer risks to privacy, civil liberties, and civil rights? After

---

https://travel.state.gov/content/passports/en/passports/statistics.html (last visited Sept. 21, 2016) (showing that as of 2015, there are 125,907,176 valid U.S. passports in circulation).

[24] *Compare* U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 51 (May 2016) (uncorrected copy, on file with authors) *with* U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 51 (May 2016) (corrected copy) http://www.gao.gov/assets/680/677098.pdf.

[25] *See* Privacy SOS, *In bizarre reversal, FBI suddenly claims it is not negotiating with states over face recognition access*, ACLU of Massachusetts (Aug 10, 2016), https://privacysos.org/blog/fbi-changes-tune-about-face-recognition-and-state-rmvs/.

[26] *See* U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 18–32 (May 2016).

[27] *See* Privacy Act of 1974; Implementation, 81 Fed. Reg. 27288, 27289 (proposed May 5, 2016) (to be codified at 28 C.F.R. pt. 16); Center on Privacy & Technology et. al., Comment on Proposed Rule to Exempt Next Generation Identification System from Provisions of the Privacy Act and the Modified System of Records Notice for that System (July 6, 2016), https://www.regulations.gov/document?D=DOJ-OPCL-2016-0008-0114 (explaining the impact of the proposed exemptions).

proposing a **Risk Framework** for law enforcement face recognition, the report explores the following questions, each of which is answered in our **Findings**:

- **Deployment.** Who is using face recognition, how often are they using it, and where do those deployments fall on the Risk Framework?
- **Fourth Amendment.** How do agencies using face recognition protect our right to be free from unreasonable searches and seizures?
- **Free Speech.** How do they ensure that face recognition does not chill our right to free speech, assembly, and association?
- **Accuracy.** How do they ensure that their systems are accurate?
- **Racial Bias.** How does law enforcement face recognition impact racial and ethnic minorities?
- **Transparency and Accountability.** Are agencies using face recognition in a way that is transparent, accountable to the public, and subject to internal oversight?

To answer all of these questions, we submitted detailed public records requests to over 100 law enforcement agencies across the country. In total, our requests yielded more than 15,000 pages of responsive documents. Ninety agencies provided responsive documents—or substantive responses—of some kind. These responses suggested that at least 52 state and local law enforcement agencies that we surveyed were now using, or have previously used or obtained, face recognition technology. (We will refer to these agencies as "52 agencies.") Of the 52 agencies, eight formerly used or acquired face recognition but have since discontinued those programs. Conversely, several other responsive agencies have opened their systems to hundreds of *other* agencies.[28]

To support our public records research, we conducted dozens of interviews with law enforcement agencies, face recognition companies, and face recognition researchers and conducted a fifty-state legal survey of biometrics and related surveillance laws, and an in-depth review of the technical literature on face recognition. We confirmed our findings through two site visits to law enforcement agencies with advanced face recognition systems. (Our full research methodology, including a breakdown of our records requests and a template for those requests can be found in the **Appendix**.)

After assessing these risks, this report proposes concrete recommendations for Congress, state legislatures, federal, state and local law enforcement agencies, the National Institute of Standards and Technology, face recognition companies, and community leaders.

[28] *See below* Appendix TK for a list of all agencies we surveyed, grouped by type of response received.

IV. A RISK FRAMEWORK OF LAW ENFORCEMENT FACE RECOGNITION

In this section, we categorize police uses of face recognition according to the risks that they create for privacy, civil liberties, and civil rights. Some uses of the technology create new and sensitive risks that may undermine longstanding, legally recognized rights. Other uses are far less controversial and are directly comparable to longstanding police practices. Any regulatory scheme should account for those differences.

A. RISK FACTORS

The overall risk level of a particular deployment of face recognition will depend on a variety of factors. As this report will explain, it is unclear how the Supreme Court would interpret the Fourth Amendment or First Amendment to apply to law enforcement face recognition; there are no decisions that directly answer these questions.[29] In the absence of clear guidance, we can look at general Fourth Amendment and First Amendment principles, social norms, and police practices to identify five risk factors for face recognition. When applied, these factors will suggest different regulatory approaches for different uses of the technology.

- **Targeted vs. Dragnet Search.** Are searches run on a discrete, targeted basis for individuals suspected of a crime? Or are they continuous, generalized searches on groups of people—or anyone who walks in front of a surveillance camera?

At its core, the Fourth Amendment was intended to prevent generalized, suspicionless searches. The Fourth Amendment was inspired by the British Crown's use of general warrants, also known as Writs of Assistance, that entitled officials to search the homes of any colonial resident.[30] This is why the Amendment requires that warrants be issued only upon a showing of probable cause and a particularized description of who or what will be searched or seized.[31]

For its part, the First Amendment does not protect only our right to free speech. It also protects our right to peaceably assemble, to petition our government for a redress of grievances, and to express ourselves anonymously.[32] These rights are not total and the cases interpreting them are at times contradictory.[33] But police use of face recognition to continuously identify anyone on the street—without individualized suspicion—could chill our basic freedoms of expression and association, particularly when face recognition is used at political protests.

- **Targeted vs. Dragnet Database**. Are searches run against a mug shot database, or an even smaller watchlist composed of handful of individuals? Or are searches run against driver's license photo databases that include millions of law-abiding Americans?

---

[29] *See below* Sections TK Findings: Fourth Amendment and TK Findings: First Amendment for a discussion on the Fourth Amendment and First Amendment implications of law enforcement face recognition.
[30] *See* William J. Cuddihy, *The Fourth Amendment: Origins and Original Meaning 602–1791* 537–548 (2009).
[31] *See* U.S. Const. amend. IV.
[32] U.S. Const. amend. I; *see generally* NAACP v. Alabama ex rel. Patterson, 357 U.S. 449 (1958); Talley v. California, 362 U.S. 60 (1960); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995).
[33] *See below* Section TK Findings: Free Speech.

Government searches against dragnet databases have been among the most controversial national security and law enforcement policies of the 21st century. Public protest after Edward Snowden's leaks of classified documents centered on the NSA's collection of most domestic call records in the U.S. Notably, searches of the data collected were more or less targeted; the call records database was not.[34] In 2015, Congress voted to end the program.[35]

- **Transparent vs. Invisible Searches.** Is the face recognition search conducted in a manner that is visible to a target? Or is that search intentionally or inadvertently invisible to its target?

While they may stem from legitimate law enforcement necessity, secret searches merit greater scrutiny than public, transparent searches. "It should be obvious that those government searches that proceed in secret have a greater need for judicial intervention and approval than those that do not," writes Professor Susan Freiwald. As she explains, "[i]nvestigative methods that operate out in the open may be challenged at the time of the search by those who observe it." You can't challenge a search that you don't know about.[36]

- **Real-time vs. After-the-Fact Searches.** Does a face recognition search aim to identify or locate someone right now? Or is it run to investigate a person's past behavior?

Courts have generally applied greater scrutiny—and required either a higher level of individualized suspicion, greater oversight, or both—to searches that track real-time, contemporaneous behavior, as opposed to past conduct. For example, while there is a split in the federal courts as to whether police need probable cause to obtain historical geolocation records, most courts have required warrants for real-time police tracking.[37] Similarly, while federal law enforcement officers obtain warrants prior to requesting real-time GPS tracking of a suspect's phone by a wireless carrier, and prior to using a "Stingray" (also known as a cell-site simulator) which effectively conducts a real-time geolocation search, courts have generally not extended that standard to requests for historical geolocation records.[38]

---

[34] *See generally* Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* 21-37 (Jan. 23 2014). A search of a telephone number within the database required one of 22 NSA officials to find that there is a "reasonable, articulable suspicion" that the number is associated with terrorism. *Id.* at 8–9. However, the NSA did not comply with this requirement for a number of years. *See Memorandum Opinion*, Foreign Intelligence Surveillance Court (2009) (Judge Bates) at 16 n. 14, https://assets.documentcloud.org/documents/775818/fisc-opinion-unconstitutional-surveillance-0.pdf ("Contrary to the government's repeated assurances, NSA had been routinely running queries of the metadata using querying terms that did not meet the required standards for querying.").

[35] *See* Ellen Nakashima, *NSA's bulk collection of Americans' phone records ends Sunday*, Washington Post (Nov. 27, 2015), https://www.washingtonpost.com/world/national-security/nsas-bulk-collection-of-americans-phone-records-ends-sunday/2015/11/27/75dc62e2-9546-11e5-a2d6-f57908580b1f_story.html.

[36] *See* Susan Freiwald, *First Principles of Communications Privacy*, 2007 Stan. Tech. L. Rev. 3, ¶62 (2007).

[37] *See, e.g.,* Tracey v. State, 152 So.3d 504, 515 (Fla. 2014) ("[T]he federal courts are in some disagreement as to whether probable cause or simply specific and articulable facts are required for authorization to access [historical cell-site location information]."); United States v. Espudo, 954 F. Supp. 2d 1029, 1038–39 (S.D. Cal. 2013) (noting that a significant majority of courts "has found that real-time cell site location data is not obtainable on a showing less than probable cause.").

[38] *See Geolocation Technology and Privacy: Before the H. Comm. on Oversight and Gov't Reform,* 114th Cong. 2–4 (2016) (statement of Richard Downing, Acting Deputy Assistant Attorney General, Department of Justice) (explaining the practice of obtaining warrants prior to requesting real-time GPS records from wireless carriers, the policy of obtaining warrants prior to use of cell-site simulators, and the practice of

- **Established vs. Novel Use.** Is a face recognition search generally analogous to longstanding fingerprinting practices or modern DNA analysis? Or is it unprecedented?

In 1892, Sir Francis Galton published *Finger Prints*, a seminal treatise arguing that fingerprints were "an incomparably surer criterion of identity than any other bodily feature."[39] Since then, law enforcement agencies have adopted fingerprint technology for everyday use. A comparable shift occurred in the late 20th Century around forensic DNA analysis. Regulation of face recognition should take note of the existing ways in which biometric technologies are used by American law enforcement.

At the same time, we should not put precedent on a pedestal. As Justice Scalia noted in his dissent in *Maryland v. King*, a case that explored the use of biometrics in modern policing, "[t]he great expansion in fingerprinting came before the modern era of Fourth Amendment jurisprudence, and so [the Supreme Court was] never asked to decide the legitimacy of the practice."[40] A specific use of biometrics may be old, but that doesn't mean it's legal.

B. RISK FRAMEWORK

Applying these criteria to the most common police uses of face recognition, three categories of deployments begin to emerge:

- **Moderate Risk Deployments** are more targeted than other uses and generally resemble existing police use of biometrics.

- **High Risk Deployments** involve the unprecedented use of dragnet biometric databases of law-abiding Americans.

- **Very High Risk Deployments** apply continuous face recognition searches to video feeds from surveillance footage and police-worn body cameras, creating profound problems for privacy and civil liberties.

These categories are summarized in **Figure TK** and explained below. Note that not every criterion maps neatly onto a particular deployment.

---

obtaining historical cell-site location records upon a lower showing of "specific and articulable facts" that records are sought are relevant and material to an ongoing criminal investigation).

[39] Francis Galton, *Finger Prints* 2 (1892).

[40] Maryland v. King, 133 S. Ct. 1958, 1988 (2013) (Scalia, J., dissenting) (citing United States v. Kincade, 379 F.3d 813, 874 (9th Cir. 2004)).

Figure TK. Risk Framework for Law Enforcement Face Recognition

	Less Risk	More Risk
Stop and Identify (Mug shot Database)	• Targeted Search • Targeted Database • Transparent	• Real-Time • Novel Use
Arrest and Identify (Mug shot Database)	• Targeted Search • Targeted Database • Established Use	• Invisible
Investigate and Identify (Mug shot Database)	• Targeted Search • Targeted Database • After-the-Fact • Established Use	• Invisible
Stop and Identify (License Database)	• Targeted Search • Transparent	• Dragnet Database • Real-Time • Novel Use
Arrest and Identify (License Database)	• Targeted Search	• Dragnet Database • Invisible • Novel Use
Investigate and Identify (License Database)	• Targeted Search • After-the-Fact	• Dragnet Database • Invisible • Novel Use
Real-Time Video Surveillance	• Targeted Database	• Dragnet Search • Invisible • Real-Time • Novel Use
Historical Video Surveillance	• Targeted Database • After-the-Fact	• Dragnet Search • Invisible • Novel Use

1. MODERATE RISK DEPLOYMENTS.

The primary characteristic of moderate risk deployments is the combination of a targeted search with a relatively targeted database.

When a police officer uses face recognition to identify someone during a lawful stop (Stop and Identify), when someone is enrolled and searched against a face recognition database after an arrest (Arrest and Identify), or when police departments or the FBI use face recognition systems to identify a specific criminal suspect captured by a surveillance camera (Investigate and Identify), they are conducting a targeted search pursuant to an particularized suspicion—and adhering to a basic Fourth Amendment standard.

Mug shot databases are not entirely "targeted." They're not limited to individuals charged with felonies or other serious crimes, and many of them include people like Chris Wilson—people who had charges dismissed or dropped, who were never charged in the first place, or who were found innocent of those charges. In the FBI face recognition database (NGI-IPS), for example, over half of all arrest records fail to indicate a final disposition.[41] The failure of mug shot databases to separate the innocent from the guilty—and their inclusion of people arrested for peaceful, civil disobedience—are serious problems that must be addressed. That said, systems that search against mug shots are unquestionably *more* targeted than systems that search against a state driver's license and ID photo database.

Most face recognition searches are effectively invisible.

Two of the three moderate risk deployments—while invisible to the search subject—mirror longstanding police practices. The enrollment and search of mug shots in face recognition databases (Arrest and Identify) parallels the decades-old practice of fingerprinting arrestees during booking. Similarly, using face recognition to compare the face of a bank robber—captured by a security camera—to a database of mug shots (Investigate and Identify) is clearly comparable to the analysis of latent fingerprints at crime scenes.

The other lower risk deployment, Stop and Identify, is effectively novel.[42] It is also necessarily conducted in close to real-time. On the other hand, a Stop and Identify search is the only use of face recognition that is somewhat transparent. When an officer stops you and asks to take your picture, you may not know that he's about to use face recognition—but it certainly raises questions.[43] The vast majority of face recognition searches are effectively invisible.[44]

2. HIGH RISK DEPLOYMENTS.

High risk deployments are quite similar to moderate risk deployments—except for the databases that they employ. When police or the FBI run face recognition searches against the photos of every driver in a state, they create a virtual line-up of millions of law-abiding Americans—and cross a line that American law enforcement has generally avoided.

Law enforcement officials emphasize that they are merely searching driver's license photos that people have voluntarily chosen to provide to state government. "Driving is a privilege," said Sheriff Gualtieri of the Pinellas County Sheriff's Office.[45]

---

[41] Ellen Nakashima, *FBI wants to exempt its huge fingerprint and photo database from privacy protections*, Washington Post (June 1, 2016) ("According to figures supplied by the FBI, 43 percent of all federal arrests and 52 percent of all state arrests—or 51 percent of all arrests in NGI—lack final dispositions, such as whether a person has been convicted or even charged.")

[42] Police use of field fingerprint identification began in 2002, around the time when the first police face recognition systems were deployed. *See Minnesota police test handheld fingerprint reader*, Associated Press (Aug. 17, 2009), http://usatoday30.usatoday.com/tech/news/techinnovations/2004-08-17-mobile-printing_x.htm.

[43] Field identifications have triggered some of the few community complaints about face recognition reported in national press. *See* Timothy Williams, *Facial Recognition Moves from Overseas Wars to Local Police*, N.Y. Times (Aug. 12, 2015); Ali Winston, *Facial recognition, once a battlefield tool, lands in San Diego County*, Center for Investigative Reporting (Nov. 7, 2013).

[44] *See below* Section TK Findings: Transparency and Accountability.

[45] *Interview with PCSO Sheriff Bob Gualtieri and Technical Support Specialist Jake Ruberto* (July 26, 2016) (notes on file with authors).

People in rural states—and states with voter ID laws—may chafe at the idea that getting a driver's license is a choice, not a necessity. Most people would also be surprised to learn that by getting a driver's license, they "volunteer" their photos to a face recognition network searched thousands of times a year for criminal investigations.

That surprise matters: A founding principle of American privacy law is that government data systems should notify people about how their personal information will be used, and that personal data should not be used outside of the "stated purposes of the [government data] system] as reasonably understood by the individual, unless the informed consent of the individual has been explicitly obtained."[46]

Most critically, however, by using driver's license and ID photo repositories as large-scale, biometric law enforcement databases, law enforcement enters controversial, if not uncharted, territory.

Never before has federal law enforcement built a biometric network primarily composed of law-abiding Americans.

Historically, law enforcement biometric databases have been populated exclusively or primarily by criminal or forensic samples. By federal law, the FBI's national DNA database, also known as the National DNA Index System, or "NDIS," is almost exclusively composed of DNA profiles related to criminal arrests or forensic investigations.[47] Over time, the FBI's fingerprint database has come to include non-criminal records—including the fingerprints of immigrants and civil servants. However, as **Figure TK** shows, 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.

The FBI face recognition unit (FACE Services) shatters this trend. By searching 16 states' driver's license databases, American passport photos, and photos from visa applications, the FBI has created a network of databases that is overwhelmingly made up of non-criminal entries. Never before has federal law enforcement created a biometric database—or network of databases—that is *primarily* made up of law-abiding Americans. Police departments should carefully weigh whether they, too, should cross this threshold.[48]

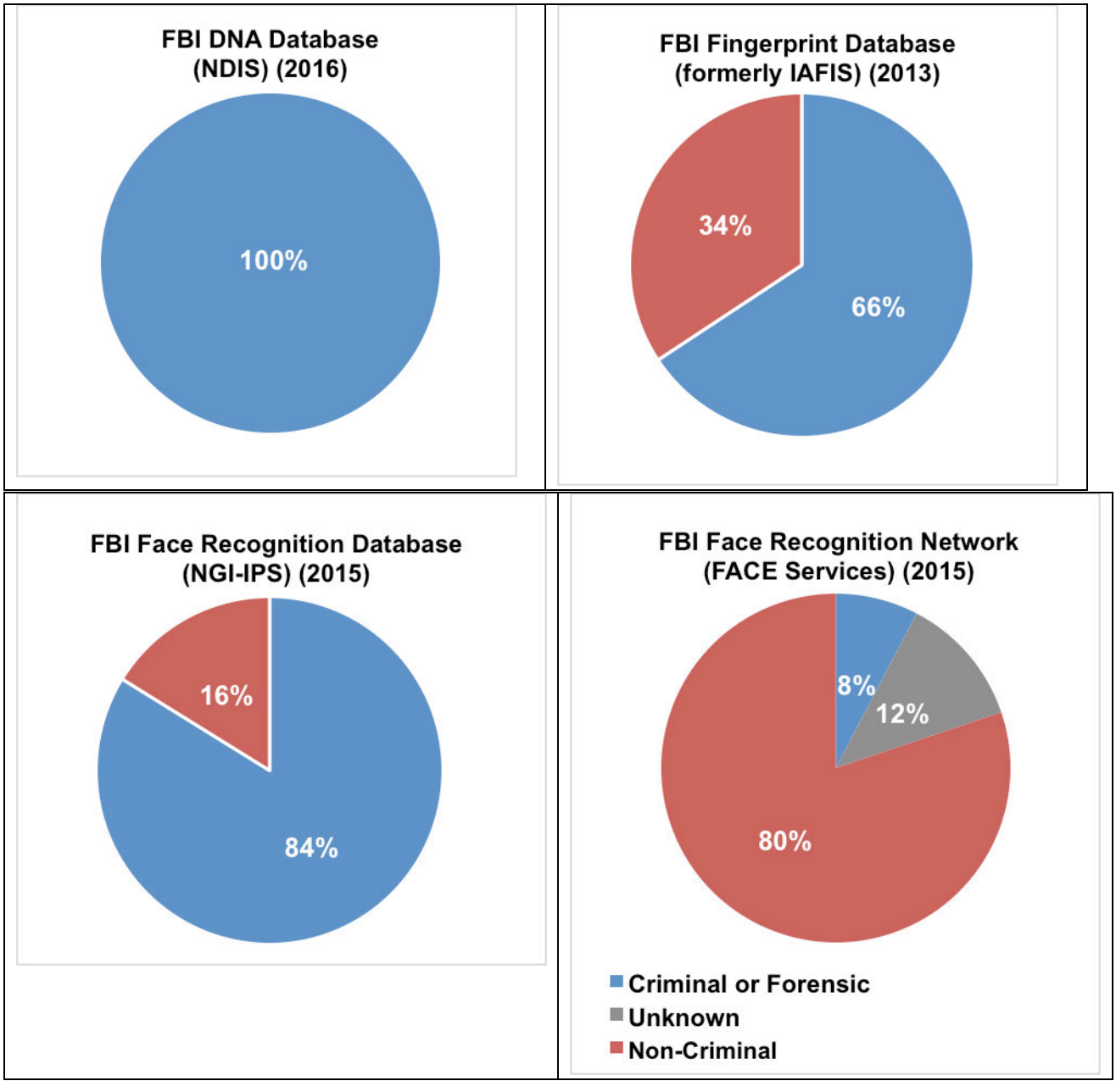
---

[46] *See* Dep't of Health, Education, and Welfare, Records, Computers and the Rights of Citizens 57–58, 61–62 (1973). The HEW committee acknowledged that not all of the FIPPS would apply to criminal intelligence records, but insisted that some of the principles must apply: "We realize that if all of the safeguard requirements were applied to *all* types of intelligence records, the utility of many intelligence-type records . . . might be greatly weakened . . . It does not follow, however, that there is no need for safeguards . . . The risk of abuse of intelligence records is too great to permit their use without *some* safeguards to protect the personal privacy and due process interests of individuals." *Id.* at 74–75.

[47] *See* 42 U.S.C. § 14132(b).

[48] Note that the perceived "risk" of a deployment may vary by jurisdiction. Many states have passed so-called "stop and identify" laws that require the subject of a legal police stop to produce identification, if available, upon request. *See, e.g.*, Colo. Rev. Stat. § 16-3-103. In those states, a Stop and Identify face recognition search run against driver's license photos—which automates a process that residents are legally required to comply with—may be less controversial.

Figure TK. Criminal vs. Non-Criminal Makeup of FBI Biometric Databases & Networks



Sources: FBI, GAO.[49]

3. VERY HIGH RISK DEPLOYMENTS.

Real-time face recognition marks a radical change in American policing—and American conceptions of freedom. With the unfortunate exception of inner-city black communities—where suspicionless police stops are all too common[50]—most Americans have always been able to walk down the street knowing that police officers will not stop them and demand identification. Real-time, continuous video surveillance changes that. And it does so by making those identifications secret, remote, and potentially pervasive. What's more, as this report explains,

[49] The composition of the DNA database (NDIS), the FBI face recognition database (NGI-IPS), and the FBI face recognition unit's network of databases (FBI FACE Services network) are calculated in terms of biometric samples (i.e. DNA samples or photographs), whereas the FBI fingerprint database composition is calculated in terms of individual persons sampled. For DNA, the Criminal or Forensic category includes all offender profiles (convicted offender, detainee, and legal profiles), arrestee profiles, and forensic profiles, as of July 2016. For fingerprints, the criminal category includes fingerprints that are "submitted as a result of an arrest at the local, state, or Federal level," whereas the non-criminal category includes fingerprints "submitted electronically by local, state, or Federal agencies for Federal employment, military service, alien registration and naturalization, and personal identification purposes." For the FBI face recognition database, Criminal or Forensic photos include "photos associated with arrests (i.e. 'mug shots')," whereas Non-Criminal Photos include "photos of applicants, employees, licensees, and those in positions of public trust." Finally, for the FBI face recognition network, the Criminal or Forensic category includes photos of individuals detained by U.S. forces abroad and NGI-IPS criminal photos and Non-Criminal photos include photos from visa applications, driver's licenses, and NGI-IPS civil photos. The Unknown category includes 50 million from four states (Michigan, North Dakota, South Carolina, and Utah) that allow the FACE Services unit to conduct or request searches of driver's license, mug shot, and correctional photos; unfortunately, the GAO did not disaggregate these state databases into their component parts, preventing us from distinguishing between criminal and non-criminal photos. **FBI DNA Database (NDIS) (2016):** Federal Bureau of Investigation, U.S. Department of Justice, *CODIS - NDIS Statistics*, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics (last visited Sept. 22, 2016) (Total: 15,706,103 DNA profiles); **FBI Fingerprint Database (IAFIS) (2013):** Integrated Automated Fingerprint Identification System: Fact Sheet, Fed. Bureau of Investigation (Dec. 5, 2013) (identifying 75.9 million subjects in the National Criminal History Record File and 39.6 million subjects in the automated civil file); Request for Records Disposition Authority, Fed. Bureau of Investigation, https://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-justice/rg-0065/n1-065-04-005_sf115.pdf (clarifying definitions of criminal and civil fingerprint files); **FBI Face Recognition Database (NGI-IPS) (2015):** U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 46, Table 3 (May 2016) (Criminal photos: 24.9 million; Civil photos: 4.8 million); Federal Bureau of Investigation, U.S. Department of Justice, *Privacy Impact Assessment for the Next Generation (NGI) Interstate Photo System*, https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/interstate-photo-system (September 2015) (clarifying composition of the Criminal Identity Group and the Civil Identity Group); **FBI Face Recognition Network (FACE Services) (2015):** U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 47-48, Table 4 (May 2016) (Criminal photos 31.6 million; Civil photos: 330.3 million; Unknown photos: 50 million). Note that the IAFIS system has been integrated into the new Next Generation Identification system. *See* Federal Bureau of Investigation, U.S. Department of Justice, *Next Generation Identification*, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi (last visited Sept. 22, 2016). However, we have been unable to find statistics on the composition of the fingerprint component of NGI.

[50] *See, e.g.*, Michelle Alexander, *The New Jim Crow: Mass Incarceration In The Age Of Colorblindness* 132–133 (2010).

real-time identifications may also be significantly less accurate than identifications in more controlled settings (i.e. Stop and Identify, Arrest and Identify).[51]

In a city equipped with real-time face recognition, every person who walks by a street surveillance camera—or a police-worn body camera—may have her face searched against a watchlist. Right now, technology likely limits those watchlists to a small number of individuals. Future technology will not have such limits, allowing real-time searches to be run against larger databases of mug shots or even driver's license photos.[52]

There is no current analog—in technology or in biometrics—for the kind of surveillance that pervasive, video-based face recognition can provide. Most police geolocation tracking technology tracks a single device, requesting the records for a particular cell phone from a wireless company, or installing a GPS tracking device on a particular car. Exceptions to that trend—like the use of cell-tower "data dumps" and cell-site simulators—generally require either a particularized request to a wireless carrier or the purchase of a special, purpose-built device (i.e., a Stingray). A major city like Chicago may own a handful of Stingrays. It reportedly has access to 10,000 surveillance cameras.[53] If cities like Chicago equip their full camera networks with face recognition, they will be able to track someone's movements retroactively or in real-time, in secret, and by using technology that is *not* covered by the warrant requirements of existing state geolocation privacy laws.[54]

[51] *See* below Section TK Findings: Accuracy.
[52] *Interview with facial recognition company* (June 22, 2016) (notes on file with authors); *Interview with Anil Jain, University Distinguished Professor*, Michigan State University (May 27, 2016) (notes on file with authors).
[53] *See* ACLU of Illinois, *Chicago's Video Surveillance Cameras: A Pervasive and Unregulated Threat to Our Privacy*, 1 (Feb. 2011), http://www.aclu-il.org/wp-content/uploads/2012/06/Surveillance-Camera-Report1.pdf.
[54] Modern state geolocation privacy laws tend to regulate the acquisition of information from electronic devices, e.g. mobile phones and wireless carriers. They do not, on their face, regulate face recognition, which does not require access to any device or company database. *See, e.g.*, Utah Code Ann. § 77-23c-102(1)(a)-(b); Cal. Penal Code § 1546.1(a).

V. FINDINGS

We studied the (1) **Deployment** of face recognition technology—namely how many agencies use face recognition, how often they use it, and the risk level of those uses. We also studied the measures that agencies and other stakeholders apply to protect (2) our **Fourth Amendment** rights and (3) our right to **Free speech**, and evaluated the steps they took to protect against (4) **Accuracy** problems and the potential for (5) **Racial bias** in error rates and in use more generally. Finally, we studied the (6) **Transparency & Accountability** provisions in place at agencies using the technology.

This section outlines our top-level findings in each of these areas. In our **Face Recognition Scorecard**, and in the **City and State Backgrounders** in the **Appendix**, we evaluate how each of 25 specific agencies performs in these same fields.[55] The criteria for the scores are described in their corresponding subsections. Two of the subsections, Deployment and Transparency & Accountability, are measured with two separate scores, whereas one subsection, Racial Bias, is not scored at all. (Our full scorecard methodology can be found in the **Appendix**.)

[INSERT FACE RECOGNITION SCORECARD HERE.]

Before proceeding further, a disclaimer is in order. Our findings are based on 15,000 pages of documents provided in response to over 100 records requests. Many of those records were partial, redacted, or otherwise incomplete. We have made extensive efforts to give state and local police departments the ability to review and correct our conclusions regarding their face recognition systems, but it is inevitable that errors and misunderstandings will occur. We invite agencies to contact the authors with corrections and clarifications—and improvements to their systems—so that this report may be updated accordingly.

[55] We have additionally created a state backgrounder for a 26th jurisdiction, Vermont, detailing that the Vermont DMV face recognition system may conflict with state law. *See* Appendix TK.

Perpetual Lineup Scorecard

Logo →	Mugshots v. Driver's Licenses	CCTV	Scales of Justice	Bullhorn	Target (?)	Shining Sun	Checkmark
Jurisdiction	People in Database	Real-Time Video	4th Amendment	Free Speech	Accuracy	Transparency	Audits
FBI FACE Services	3	0	3	0	1	0	3
Maricopa County	3	0	3	0	2	3	3
Arkansas	2	0	0	0	0	3	0
Los Angeles Region	2	3	0	0	3	3	0
SANDAG	2	1	1	0	3	1	2
San Francisco	2	0	0	0	2	3	0
Florida	3	2	3	0	3	3	3
Hawaii	2	0	2	2	1	2	3
Chicago	2	3	0	0	0	3	0
Iowa	3	0	3	2	0	3	2
Maine	2	0	0	0	0	3	0
Maryland	3	0	2	0	3	3	3
Michigan	3	2	3	0	1	2	1
Minnesota	2	2	3	0	0	3	3
Nebraska	3	2	1	0	0	3	2
Lincoln	3	0	3	0	0	3	2
New Mexico	0	0	0	0	0	3	0
Albuquerque	2	0	2	0	1	3	3
Ohio	3	0	3	1	3	3	2
Pennsylvania	3	0	3	2	3	3	2
Texas	3	0	0	0	0	3	0
Vermont	3	0	3	0	1	0	3
Virginia	2	2	3	0	3	3	3
NOVARIS	2	0	0	0	0	3	0
Seattle Region	2	1	1	2	1	1	2
WV Intelligence Fusion Center	2	3	0	2	0	3	2

A. DEPLOYMENT

Neil Stammer was a fugitive wanted for child abuse and kidnapping who had evaded capture for 14 years after failing to show up for his arraignment. Then, in 2014, a State Department official with the Diplomatic Security Service ran the FBI's wanted posters through a database designed to detect passport fraud—and got a hit for Kevin Hodges, an American living in Nepal. It was Stammer, who'd been living in Nepal for years under a pseudonym. He was arrested and returned to the United States to face charges.[56]

The year before Stammer was caught, on the other side of the world, the Los Angeles Police Department announced the installation of 16 new surveillance cameras in "undisclosed locations" across the San Fernando Valley. The cameras were mobile, wireless, and programmed to support face recognition "at distances of up to 600 feet."[57] *LA Weekly* reported that they fed into the LAPD's Real-time Analysis and Critical Response Center, which would scan the faces in the feed against "hot lists" of wanted criminals or "documented" gang members.[58] It appears that every person who walks by those cameras has her face searched in this way.

What agencies are using face recognition for law enforcement, how often are they using it, and how risky are those deployments?

When proponents of face recognition answer these questions, they often cite cases like Neil Stammer's: A felon, long-wanted for serious crimes, is finally brought to justice through the last-resort use of face recognition by a sophisticated federal law enforcement agency.[59] The LAPD's system suggests a more sobering reality: Police and the FBI use face recognition for routine, day-to-day law enforcement. And state and local police, not the FBI, are leading the way towards the most advanced—and highest risk—deployments.

1. How many law enforcement agencies use face recognition?

---

[56] Federal Bureau of Investigation, U.S. Department of Justice, *Long-Time Fugitive Captured: Juggler Was on the Run for 14 Years* (Aug. 12, 2014), https://www.fbi.gov/news/stories/2014/august/long-time-fugitive-neil-stammer-captured/.

[57] West Valley Community Police Station, *Surveillance Cameras in West San Fernando Valley*, West Valley Police (Jan. 1, 2013), http://www.westvalleypolice.org/index_news_20130120.html.

[58] Darwin Bond-Graham and Ali Winston, *Forget the NSA, the LAPD Spies on Millions of Innocent Folks*, LA Weekly (Feb. 27, 2014), http://www.laweekly.com/news/forget-the-nsa-the-lapd-spies-on-millions-of-innocent-folks-4473467.

[59] *See, e.g., Long-Time Massachusetts Fugitive Arrested in North Carolina*, Federal Bureau of Investigation, U.S. Department of Justice (June 16, 2016), https://www.fbi.gov/boston/press-releases/2016/long-time-massachusetts-fugitive-arrested-in-north-carolina (While this press release does not mention face recognition, a spokesperson for the Pinellas County Sheriff's Office stated that the suspect's identity was confirmed through the use of PCSO's face recognition program. Pinellas County Sheriff's Office, *Email from Jake Ruberto, Technical Support Specialist to Clare Garvie* (Jul. 13, 2016) (on file with authors)); Edward B. Colby, *James Robert Jones, Military Fugitive on the Run Since 1977, Arrested in South Florida: Authorities*, NBC Miami (Mar. 17, 2014), http://www.nbcmiami.com/news/local/James-Robert-Jones-Military-Fugitive-on-the-Run-Since-1977-Arrested-in-South-Florida-Authorities-250247711.html.

We estimate that more than one in four of all American state and local law enforcement agencies can run face recognition searches of their own databases, run those searches on another agency's face recognition system, or have the option to access such a system.[60]

Some of the longest-running and largest systems are found at the state and local level. The Pinellas County Sheriff's Office in Florida, for example, began implementing its current system in 2001.[61] Over 5,300 officials from 242 federal, state, and local agencies have access to the system.[62] In Pennsylvania, officials from over 500 agencies already use the state's face recognition system, which is open to all 1,020 law enforcement agencies in the state.[63]

Many federal agencies access state face recognition systems. While the GAO reports that the FBI face recognition unit (FACE Services) searches 16 state driver's license databases,[64] this is not a complete picture of the FBI's reach into state systems: We found that, after undergoing training, FBI agents in Florida field offices have direct access to the Pinellas County Sheriff's Office system, which can run searches against all of Florida driver's license photos. Notably, the GAO does not identify Florida as forming part of the FACE Services network.[65] It is possible that other field offices can access other state systems, such as those in Pennsylvania and Maryland.[66]

---

[60] The U.S. Department of Justice Bureau of Justice Statistics reports that as of 2013, there were 15,388 state and local law enforcement agencies. Brian A. Reaves, Ph.D., *Local Police Departments, 2013: Personnel, Policies, and Practices*, Bureau of Justice Statistics, Office of Justice Programs, U.S. Department of Justice (May 2015), http://www.bjs.gov/content/pub/pdf/lpd13ppp.pdf. Based on the responses to our survey, we estimate that 3,947 state and local law enforcement agencies (25.6%): (1) currently have the ability to run or request face recognition searches of their own system or that of another agency, or (2) have the option to use face recognition capabilities after requesting access, fulfilling training, or signing an agreement with an agency that has a face recognition system.

[61] *See* Pinellas County Sheriff's Office, *Florida's Facial Recognition Network* (Mar. 26, 2014), Document p. 014722. Other examples include the Los Angeles Police Department, which piloted a face recognition surveillance camera project by 2005. *See LAPD Uses New Technologies to Fight Crime*, Los Angeles Police Department (Feb. 1, 2005), http://www.lapdonline.org/february_2005/news_view/19849; *See* Maricopa County Sheriff's Office, *Computer Server Purchase for Facial Recognition System* (Aug. 28, 2006), Document p. 015026 (indicating that a face recognition program was "being initiated at the Arizona Counterterrorism Information Center (ACTIC)" in conjunction with Hummingbird Defense Systems as early as 2006).

[62] Pinellas County Sheriff's Office, *Florida's Facial Recognition Network, FACES Training 2015*, Document p. 014396; Pinellas County Sheriff's Office, *Interview with Sheriff Bob Gualtieri and Jake Ruberto* (July 26, 2016) (indicating that 242 agencies at the federal, state, and local level have access. Notes on file with authors.).

[63] Pennsylvania JNET, *JNET & PennDOT Facial Recognition Integration* (Dec. 2012), Document p. 013785; Legislative Budget and Finance Committee, Pennsylvania General Assembly, *Police Consolidation in Pennsylvania* (Sept. 2014), http://lbfc.legis.state.pa.us/Resources/Documents/Reports/497.pdf. Similarly, "any officer, deputy, investigator or crime analyst in LA County" is permitted to access the Los Angeles County Sheriff Department's system. Los Angeles County Sheriff's Department, *Facial Identification and the LA Photo Manager* (July 23, 2015), Document p. 000532. Participation in the West Virginia Intelligence Fusion Center "is open to all federal, state, county, and local agencies." West Virginia Intelligence Fusion Center, *Standard Operating Procedures*, Document p. 009944.

[64] U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 51 (May 2016).

[65] Pinellas County Sheriff's Office, *Interview with Sheriff Bob Gualtieri and Technical Support Specialist Jake Ruberto* (July 26, 2016) (notes on file with authors).

[66] Maryland Department of Public Safety and Correctional Services, *PIA Request* (Feb. 2016), Document pp. 008906–008907 (describing that both "internal" users—DPSCS employees, and "external" users—

The Department of Defense, the Drug Enforcement Administration, Immigrations and Customs Enforcement, the Internal Revenue Service, the Social Security Administration, the U.S. Air Force Office of Special Investigations, and the U.S. Marshals Service have all had access to one or more state or local face recognition systems.[67]

2. How often do law enforcement agencies use face recognition?

Face recognition searches are routine at the federal and state level. FBI face recognition searches of state driver's license photos are almost six times more common than federal court-ordered wiretaps.[68] From August 2011 to December 2015, the FBI face recognition unit (FACE Services) ran close to 214,920 face recognition searches, including 118,490 searches of its own database and 36,420 searches against the 16 state driver's license and mug shot databases. The remainder was run against the Department of Defense database and the Department of State's visa and passport photo databases.[69]

In its first eight months of operation, Ohio's system was used 6,618 times by 504 agencies, though its usage rate has since gone down—for the first four months of 2016, the

---

other "law enforcement officers or vetted employees of criminal justice agencies" have access to the face recognition system); Pennsylvania JNET, *JNET & PennDOT Facial Recognition Integration* (Dec. 2012), Document pp. 013785–013787 ("With JFRS deployed on JNET, the system can be made available to any law enforcement agency in Pennsylvania . . . With JFRS available through JNET, this enterprise solution is available at no cost to any municipal, county, state or federal law enforcement agency in the commonwealth.").

[67] Michigan's SNAP database is open to searches from the U.S. Marshals service. Michigan State Police, *Email from Robert Watson to MSPSNAP* (Aug. 17, 2015), Document p. 011113. The Arizona Counterterrorism Information Center, run by the Maricopa County Sheriff's Office, has conducted face recognition searches for federal investigations since 2008. Maricopa County Sheriff's Office, *Letter from Deputy Chief Ray Churay to Deputy Chief David Hendershott* (Apr. 21, 2008), Document p. 015070. The Pinellas County Sheriff's Office has signed MOUs with the U.S. Air Force Office of Special Investigations, the IRS Criminal Investigation Field Office in Tampa, the Social Security Administration, and four other federal agencies with Florida branches. *Memoranda of Understanding between Pinellas County Sheriff's Office and U.S. Air Force Office of Special Investigations Detachment 340* (Jan. 16, 2015), Document p. 013798; *Department of Agriculture and Consumer Services, Office of Agricultural Law Enforcement* (Jul. 9, 2014), Document p. 013901; *Department of Financial Services, Division of Insurance Fraud* (May 14, 2013), Document p. 013906; *Internal Revenue Service, Criminal Investigation, Tampa Field Office* (Aug. 20, 2013), Document p. 014125; *6th Security Forces Squadron* (Jan 21, 2009), Document p. 014208; *Social Security Administration, Office of the Inspector General, Office of Investigations* (Dec. 16, 2014), Document p. 014594; *U.S. Department of Veterans Affairs Police* (Jun. 16, 2014), Document p. 014649. Records indicate that the Department of Defense, the Drug Enforcement Administration, Immigration and Customs Enforcement, the U.S. Marshals Service, and numerous other federal agencies access this system as well. Pinellas County Sheriff's Office, *Florida's Facial Recognition Network, FACES Training 2015*, Document p. 014396.

[68] 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/wiretap-report-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).

[69] *See* U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 49 (May 2016).

system was searched 1,429 times by 104 different agencies.[70] San Diego agencies run an average of around 560 searches of the San Diego Association of Government's system each month.[71] Pinellas County's system may be the most widely used; its users conduct around 8,000 searches per month.[72] This appears to be much more frequent than the searches run by the FBI face recognition unit—almost twice as often, on average.[73]

We have only a partial sense of how effective these searches are. There are no public statistics on the success rate of state face recognition systems. We do know the number of FBI searches that yielded likely candidates—although we do not know how many actual identifications resulted from those potential matches. The statistics are nonetheless striking: Of the FBI's 36,420 searches of state license photo and mug shot databases, only 210 (0.6%) yielded likely candidates for further investigations. Overall, 8,590 (4%) of the FBI's 214,920 searches yielded likely matches.[74]

3. How risky are those deployments?

We found that a large number of police departments are engaging in high risk deployments, and that several of the agencies are actively exploring real-time video surveillance.

a) Moderate Risk Deployments

Of the 52 agencies we surveyed which were now using or had previously used or obtained face recognition technology, we identified 29 that are deploying face recognition under a Moderate Risk model—Stop and Identify, Arrest and Identify, and/or Investigate and Identify off of mug shot databases. Most of the agencies use their systems in a variety of ways. Only one current system, used by the San Diego Association of Governments (SANDAG), is designed to be used only for Stop and Identify searches.[75]

None of the agencies indicated that its mug shot database was limited to individuals arrested for felonies or other serious crimes. Only one agency, the Michigan State Police, deleted mug shots of individuals who are not charged or found innocent.[76] The norm, rather, is

---

[70] *BCI Facial Recognition Video*, YouTube (Mar. 6, 2014), https://www.youtube.com/watch?v=XjvwJlkpFQI at 3:10; *Letter from Gregory Trout, Chief Counsel, Ohio Bureau of Criminal Investigation to Clare Garvie* (Sept. 23, 2016), Document p. 016841.

[71] SANDAG, *Board of Directors Agenda* (Feb. 13, 2015), Document p. 005698 (According to SANDAG estimates from Feb. 13, 2015: "Since August 2012, more than 17,000 image submittals have resulted in approximately 4,700 potential matches.")

[72] Pinellas County Sheriff's Office, *Florida's Facial Recognition Network, FACES Training 2015*, Document p. 014396.

[73] The FBI face recognition unit (FACE Services) has run an average of 4,055 searches per month over the past 4.5 years. U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 49 (May 2016).

[74] *See* U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 49 (May 2016),

[75] SANDAG, *Automated Regional Justice Information System (ARJIS) Acceptable Use Police for Facial Recognition* (Feb. 13, 2015), Document p. 008449.

[76] This is mandated by state law. *See* Mich. Comp. Laws Ann § 28.243. Additionally, members of the Digital Analysis and Identification Division, who are responsible for running most of the Michigan's law enforcement face recognition searches, manually check the potential "match" candidates returned to ensure that information only about pending charges and convictions are disseminated. *Interview with*

reflected in an agency like the Pinellas County Sheriff's Office. Its mug shot database is not scrubbed to eliminate cases that did not result in conviction. To be removed from the database, individuals need to obtain an expungement order—a process that can take months to be resolved.[77]

b) High Risk Deployments

High risk deployments—whether Stop and Identify, Arrest and Identify, or Investigate and Identify—are typified by their access to state driver's license and ID photo databases. Our requests revealed 19 state or local law enforcement agencies in eight states allow face recognition searches of these databases. Combining that with recent information from the GAO, and earlier reporting that we verified against the GAO report or through our own research, we identified 26 states that enroll their residents in a virtual line-up.[78]

In 2014, there were 119,409,269 drivers in these states, of whom 117,673,662 were adults aged 18 or older and 1,736,269 were minors aged 17 or younger.[79] The U.S. Census estimated that in 2014, there were 245,273,438 American adults in the country.[80] This means that, at a minimum, roughly 1 in 2 American adults (48%) have had their photos enrolled in a criminal face recognition network.

The figure is likely larger than that. In 2013, the *Washington Post* and the *Cincinnati Enquirer* conducted similar surveys that flagged four other states—Indiana, Massachusetts, Mississippi and South Dakota—that allowed access but that we were not able to verify.[81] If all four of those states continue to grant access, the total number of licensed drivers in face

---

Peter Langenfeld, Program Manager, Digital Analysis and Identification Section (May 25, 2016) (notes on file with authors).

[77] Pinellas County Sheriff's Office, *Interview with Sheriff Bob Gualtieri and Technical Support Specialist Jake Ruberto* (July 26, 2016) (notes on file with authors). There is currently a five-month backlog for expungement requests in the Florida Department of Law Enforcement (as of Sep. 21, 2016). Florida Department of Law Enforcement, *Seal and Expunge Process*, http://www.fdle.state.fl.us/cms/Seal-and-Expunge-Process/Seal-and-Expunge-home.aspx (last visited Sept. 25, 2016).

[78] *See* U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 51(map). In 2013, the *Washington Post* and the *Cincinnati Enquirer* identified 26 states where law enforcement could run or request face recognition searches of driver's license and ID photo databases. For most of these states, we were able to use calls, document requests, and the 2016 GAO report to determine whether law enforcement access continued or had been discontinued. *See* Craig Timberg and Ellen Nakashima, *State photo ID-databases become troves for police,* Washington Post (June 16, 2013) (state map missing; on file with authors); Chrissie Thompson and Jessie Balmert, *WATCHDOG: Ohio database access rules loosest in U.S.*, Cincinnati Enquirer (Sept. 22, 2013).

[79] *See* Federal Highway Administration, U.S. Department of Transportation, *Highway Statistics 2014* 4-5 (Sept. 2015), http://www.fhwa.dot.gov/policyinformation/statistics/2014/pdf/dl22.pdf.

[80] *See* U.S. Census Bureau, *Annual Estimates of the Resident Population for Selected Age Groups by Sex for the United States, States, Counties, and Puerto Rico Commonwealth and Municipios: April 1, 2010 to July 1, 2014: 2014 Population Estimates*, http://factfinder.census.gov/bkmk/table/1.0/en/PEP/2014/PEPAGESEX.

[81] *See* above note TK.

recognition networks would increase to 131,211,203, of whom 129,280,396 were adults.[82] That comes out to 53% of the adult population.[83]

Figure TK. Drivers and Adults in Law Enforcement Face Recognition Networks (2014)
States and agencies reported to allow or run searches of license and ID photos are in italics.[84]

State License Photo Database	What law enforcement agencies can run or request face recognition searches?	Number of Drivers (2014)
Alabama	FBI	3,881,542
Arizona	Maricopa County Sheriff's Office	4,881,801
Arkansas	FBI	2,111,873
Colorado	Colorado law enforcement	3,883,362
Connecticut	Connecticut law enforcement	2,542,588
Delaware	FBI, *Delaware law enforcement*	732,349
Florida	FBI, Pinellas County Sheriff's Office, 242 other agencies	13,898,347
Georgia	Georgia Bureau of Investigation	6,650,434
Illinois	FBI	8,373,565
Indiana	*Indiana law enforcement*	*4,448,099*
Iowa	FBI, Iowa Department of Public Safety	2,227,950
Kentucky	FBI, *Kentucky State Police*	3,004,919
Maryland	Md. Dep't of Public Safety & Correctional Services, Md. State Police, Baltimore City Police Department, other agencies	4,142,997
Massachusetts	*Massachusetts law enforcement*	*4,765,586*
Michigan	FBI, Michigan State Police, U.S. Dep't of Justice, Detroit Police Department, Mich. Dep't of Corrections, Detroit & Southeast Michigan Information & Intel. Ctr.	7,046,433
Mississippi	*Mississippi Department of Public Safety Criminal Information Center*	*1,977,679*
Nebraska	FBI, Nebraska State Patrol, Lincoln Police Department, *Omaha Police Department*	1,383,693
Nevada	Nevada law enforcement	1,796,443

[82] *See* Federal Highway Administration, U.S. Department of Transportation, *Highway Statistics 2014* 4-5 (Sept. 2015), http://www.fhwa.dot.gov/policyinformation/statistics/2014/pdf/dl22.pdf.
[83] These are 2014 statistics. *See* U.S. Census Bureau, *Annual Estimates of the Resident Population for Selected Age Groups by Sex for the United States, States, Counties, and Puerto Rico Commonwealth and Municipios: April 1, 2010 to July 1, 2014: 2014 Population Estimates*, http://factfinder.census.gov/bkmk/table/1.0/en/PEP/2014/PEPAGESEX.
[84] States or agencies are identified in italics if they were reported to allow or have access to these searches, but we were unable to verify their current access status.

New Mexico	FBI, *New Mexico police*[85]	1,444,857
North Carolina	FBI, *North Carolina law enforcement*	7,025,333
North Dakota	FBI, *Bureau of Criminal Investigation*	527,541
Ohio	Ohio Department of Public Safety, 500+ other agencies	7,915,907
Pennsylvania	Any law enforcement agency in Pennsylvania; 500+ agencies	8,915,641
South Carolina	FBI, *State Police*	3,617,535
South Dakota	*South Dakota law enforcement*	*609,908*
Tennessee	FBI	4,613,166
Texas	FBI, Texas Department of Public Safety	15,648,733
Utah	FBI, *Department of Public Safety*	1,425,703
Vermont	FBI	545,312
West Virginia	West Virginia law enforcement	1,171,907
Drivers in Law Enforcement Face Recognition Networks (Verified states)		119,409,269
Adult Drivers in Law Enforcement Face Recognition Networks (Verified states)		117,673,662
Drivers in Law Enforcement Face Recognition Networks (All reported states)		*131,211,203*
Adult Drivers in Law Enforcement Face Recognition Networks (All reported states)		*129,280,396*
Total Number of Adults in the United States		245,273,438

Note: This is not an exhaustive accounting of law enforcement access to driver's license photo databases. Other states may allow this access that were not identified in our research.

Sources: GAO, FOIA documents, U.S. Dep't of Transportation, Federal Highway Administration, *Washington Post*, *Cincinnati Enquirer*, Police Executive Research Forum

c) Very High Risk Deployments

In May 2016, one of the world's leading face recognition companies reportedly entered into an agreement with the city government of Moscow, Russia. The company, called N-Tech.Lab, would test their software on footage from Moscow's CCTV cameras. "People who pass by the cameras are verified against the connected database of criminals or missing persons," the company's founder said. "If the system signals a high level of likeness, a warning is sent to a police officer near the location." Following the trial, the company will reportedly install its software on Moscow's CCTV system. The city has over 100,000 surveillance cameras.[86]

[85] In 2014, the Police Executive Research Forum reported that New Mexico allowed police to run face recognition searches on the state's driver's license database. Police Executive Research Forum, *Future Trends in Policing* (2014), http://www.policeforum.org/assets/docs/Free_Online_Documents/Leadership/future%20trends%20in%20policing%202014.pdf.

[86] Daniil Turovsky, *The end of privacy: 'Meduza' takes a hard look at FindFace and the looming prospect of total surveillance*, Medusa (July 14, 2016), https://meduza.io/en/feature/2016/07/14/the-end-of-privacy.

Is real-time video surveillance like that seen in Moscow coming to major American cities? The answer to this question is likely "yes."

In the U.S., no police department other than the LAPD openly claims to use real-time face recognition. But our review of contract documents and other reports suggests that at least four other major police departments have bought or expressed plans to buy real-time systems.

- In 2012, the West Virginia Intelligence Fusion Center purchased a system with the ability to "automatically monitor video surveillance footage and other video for instances of persons of interest."[87]

- In a 2012 grant application, the Chicago Police Department requested funds for high-end video processing servers "configured to process video analytics and facial recognition… to allow for real-time analysis of simultaneous high quality video streams."[88]

- In 2012, South Sound 911 in Washington state wrote in its Request for Proposals for face recognition capabilities: "The system should have the ability to do facial recognition searches against live-feed video."[89] However, the final manual for the face recognition system, which was adopted by the Seattle Police Department, states that it "may not be used to connect with 'live' camera systems."[90]

- The Dallas Area Rapid Transit police announced plans to deploy real-time face recognition software throughout its system sometime in 2016.[91]

---

[87] Tygart Technology, *MXSERVER™ Overview*, www.tygart.com/products/mxserver (last visited Sept. 22, 2016). In its "Statement of Need" and sole source purchase justification for face recognition, the West Virginia Intelligence Fusion Center listed real-time capabilities as one of the system's minimum requirements. West Virginia Intelligence Fusion Center, *WV Intelligence Fusion Center Statement of Need*, Document pp. 009971–009973.

[88] Chicago Police Department, *FY09 Transit Security Grant Program: CTA's Regional Transit Terrorism Prevention and Response System (T-CLEAR)* (Sept. 12, 2012), Document p. 008725. The grant narrative also detailed the Department's plan to purchase video processing software that "will efficiently and in real-time compare the face [captured through a video stream] to the set of faces in the data structure." Chicago Police Department, *FY09 Transit Security Grant Program: CTA's Regional Transit Terrorism Prevention and Response System (T-CLEAR)* (Sept. 12, 2012), Document p. 008726.

[89] Law Enforcement Support Agency (South Sound 911), *Mug shot Booking Photo Capture Solution: Section II Project Background*, Document p. 012048.

[90] Seattle Police Department, *Seattle Police Manual: Booking Photo Comparison Software*, Document p. 009907. The Seattle Police Department adopted the contract between Dynamic Imaging, the face recognition vendor company, and South Sound 911, which explains why the initial RFP was issued by South Sound 911, but the use policy was drafted by the Seattle Police Department. Seattle Police Department, *City Purchasing Current Contract Information: Regional Booking Photo Comparison System*, Document p. 011066; *Interview with Sean Whitcomb, Seattle Police Department* (Sept. 13, 2016) (notes on file with authors).

[91] *See* Brandon Formby, *DART addresses 'Big Brother' fears over facial recognition software,* Dallas Morning News (Feb 17, 2016), http://transportationblog.dallasnews.com/2016/02/dart-eyeing-facial-recognition-software-for-its-buses-trains-and-stations.html/. The DART General Counsel's office was unable to locate records in response to our request for information on this system; however, officials confirmed in a phone interview that negotiations were underway to secure funding for the system. *Interview with DART General Counsel's Office* (notes on file with authors).

This means that five major American police departments either claim to use real-time video surveillance, have bought the necessary hardware and software, or have expressed a written interest in buying it.

The supply exists to meet this demand. Almost all major face recognition companies advertise real-time face recognition systems. Specifically:

- NEC, the top performer in NIST accuracy tests,[92] advertises that "[f]ace recognition can do far more than is generally understood," and offers an "application for real-time video surveillance" that can "[d]etect[] subjects in a crowd in real time."[93]

- Cognitec advertises its "FaceVACS—VideoScan" solution to "instantly detect, track, recognize and analyze people in live video streams or video footage." [94]

- 3M Cogent recently introduced a new "3M Live Face Identification System" that "uses live video to match identities in real time . . . The system automatically recognizes multiple faces . . . to identify individual people from dynamic, uncontrolled environments."[95]

- Safran Identity & Security offers Morpho Argus, a "real-time video screening system, processing faces captured within live or pre-recorded video streams."[96]

- Dynamic Imaging has advertised a system add-on that would "support the ability to perform facial recognition searches against live-feed video."[97]

- DataWorks Plus claims to be able to "[r]apidly detect faces in live video surveillance monitoring for face recognition."[98]

---

[92] Patrick Grother and Mei Ngan, *Face Recognition Vendor Test: Performance of Face Identification Algorithms*, NIST Interagency Report 8009 (May 26, 2014), http://biometrics.nist.gov/cs_links/face/frvt/frvt2013/NIST_8009.pdf ("As in the 2010 test, the algorithms from the NEC corporation give broadly the lowest error rates on all datasets").

[93] *NeoFace Watch: High performance face recognition*, NEC Global Safety Division (Sept. 2014), http://www.nec.com/en/global/solutions/safety/face_recognition/PDF/Face_Recognition_NeoFace_Watch_Brochure.pdf (last visited Sept. 23, 2016).

[94] *See* Business Wire, *3M Live Face Identification System Takes Security Solutions from Reactive to Proactive* (Sept. 20, 2016), http://www.businesswire.com/news/home/20160920006378/en/3M-Live-Face-Identification-System-Takes-Security.

[95] *FaceVACS-VideoScan*, Cognitec Systems (June 2016), http://www.cognitec.com/files/layout/downloads/FaceVACS-VideoScan-5-3-flyer.pdf (last visited Sept. 23, 2016).

[96] *Real-time video screening system: Morpho Argus*, Safran (June 3, 2015), http://www.morpho.com/en/video/605 (last visited Sept. 23, 2016).

[97] South Sound 911, *Scope of Work, Dynamic Imaging Systems, Inc.*, (Feb. 20, 2013), Document p. 009582.

[98] *FACE Watch Plus Real Time Screening*, DataWorks Plus, http://www.dataworksplus.com/rts.html (last visited Sept. 23, 2016).

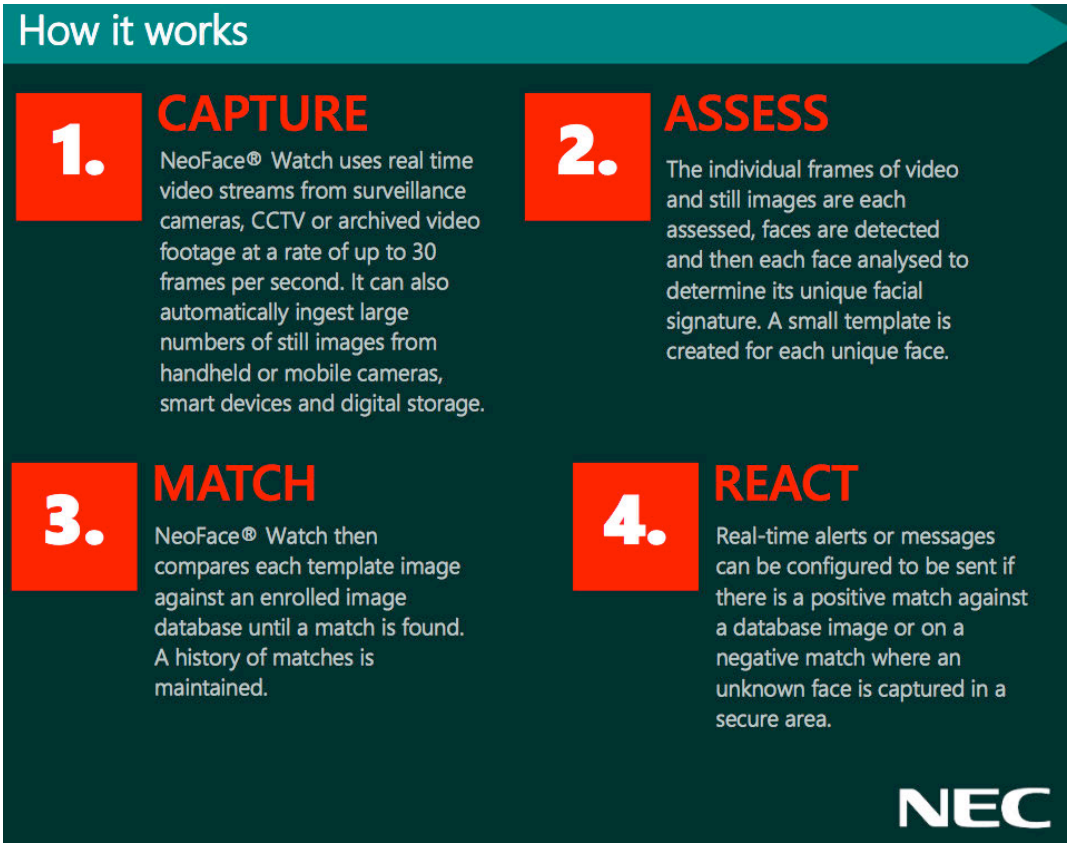


Figure TK. Excerpts from an NEC brochure for the NeoFace Watch real-time face recognition system.

The proliferation of police body-worn cameras presents another opportunity for real-time face recognition. Rick Smith, the CEO of Taser, the leading manufacturer of body cameras, recently told *Bloomberg Businessweek* that he expects real-time face recognition off of live streams from body cameras to eventually become a reality.[99] In a recent interview with *Vocativ*, the director of the West Virginia Intelligence Fusion Center, Thomas Kirk, had a similar vision: "Everyone refers to the *Minority Report*… about how they use facial recognition and iris recognition. I actually think that that is the way of the future."[100]

We anticipate that real-time face recognition systems will become commonplace.

Researchers and industry experts we interviewed agreed that real-time face recognition is becoming technologically feasible, but that computational limitations, video quality, and poor camera angles constrain its effectiveness and sharply limit its accuracy. NIST is currently running the first ever test for face recognition in video, which should shed light on the accuracy and performance of these algorithms in real-time.[101]

---

[99] *See* Karen Weise, *Will a Camera on Every Cop Make Everyone Safer? Taser Thinks So*, Bloomberg BusinessWeek (July 12, 2016), http://www.bloomberg.com/news/articles/2016-07-12/will-a-camera-on-every-cop-make-everyone-safer-taser-thinks-so.
[100] *See* Kevin Collier, *Inside the Government Centers Where the FBI Shares Intel with the Police*, Vocativ (Aug. 8, 2016), http://www.vocativ.com/347400/fusion-center-cops-fbi-share-data/.
[101] *See Face in Video Evaluation (FIVE),* National Institute of Standards and Technology, U.S. Department of Commerce, http://www.nist.gov/itl/iad/ig/five.cfm (last visited Sept. 23, 2016).

Real-time video surveillance appears to be a simple question of supply and demand. As the technology improves, we anticipate that real-time face recognition systems will become commonplace.

SIDEBAR 2: Scoring Agency Deployment

We developed two scores to measure the risk level of an agency's deployment. The first focuses on the main differentiator between moderate and high risk systems—the people enrolled in the system's face recognition database. The second focuses on how the agency has addressed real-time or historical video surveillance.

- **People in the Database.** Who is enrolled in the face recognition database or network of databases available to the law enforcement agency?
    - Green: Mug shots of individuals arrested, with enrollment limited based on the underlying offense, and/or with mug shots affirmatively "scrubbed" by police to eliminate no-charge arrests or not-guilty verdicts.
    - Yellow: Mug shots of individuals arrested, with no limits or rules to limit which mug shots are enrolled, or where mug shots are removed only after the individual applies for, and is granted, expungement.
    - Red: Driver's license photos in addition to mug shots of individuals arrested.
- **Real-Time Video Surveillance.** How has the agency addressed the risks of real-time or historical video surveillance?
    - Green: Written policy (1) prohibiting the use of face recognition for real-time video or historical video surveillance, or (2) that restricts its use only to life threatening public emergencies and requires a time-limited warrant.
    - Yellow: No written policy addressing real-time or historical video surveillance, but agency has affirmatively stated that it does not use face recognition in this manner.
    - Red: Agency has deployed, purchased, or indicated a written interest in purchasing face recognition for real-time or historical video surveillance but has not developed a written policy or affirmatively disclaimed these practices.

B. FOURTH AMENDMENT

The two district courthouses serving Cheltenham Township, Pennsylvania, adjudicate landlord-tenant disputes and municipal ordinance violations and also hold preliminary hearings and arraignments on more serious criminal charges.[102] Several years ago, the Cheltenham Township Police Department stationed officers outside a courthouse parking lot to "perform counter-surveillance"—taking photos of people attending the court hearing of an alleged gang

[102] Magisterial District Courts of Pennsylvania are courts of limited jurisdiction that handle landlord-tenant disputes, small claims of up to $12,000, summary offenses, municipal code violations, and preliminary hearings and arraignments in misdemeanor and felony offenses that will be tried in higher courts. *Magisterial District Courts*, County of Montgomery Magisterial District Courts, Montgomery County, http://www.montcopa.org/300/Magisterial-District-Courts (last visited Aug. 18, 2016). Cheltenham Township is served by Magisterial District Court 38-1-02 and 38-1-03. *Magisterial District Courts*, County of Montgomery Magisterial District Courts, Montgomery County, (Sept. 19, 2016), http://www.montcopa.org/DocumentCenter/View/10059 (last visited Aug. 18, 2016).

member. These photos were then run through Pennsylvania's face recognition system, which searches state mug shots and, beginning in 2012, all 34 million Pennsylvania driver's license photos.[103] We do not know if the photos were taken of suspected criminals—or if they were just people who happened to be in the courthouse parking lot.

This may seem unremarkable: Surreptitious police photography is an established policing technique. While the Fourth Amendment protects us against "unreasonable searches and seizures," it is unclear whether face recognition constitutes a "search." (See **Sidebar 3**.)

Protections from "unreasonable searches and seizures" can originate in any of the three branches of government: the judiciary, the legislature, or the executive, which includes law enforcement. Instead of allowing those protections to grow old and out of date, however, legislatures across the country are passing dozens of laws restricting the use of 21st century tracking technology to monitor public conduct. When legislators have hesitated, state and federal courts have stepped in and interpreted the Fourth Amendment to require warrants and other protections.

Unfortunately, courts and legislatures by and large have not applied these protections to face recognition technology. In the absence of guidance from legislatures and courts, police departments have created systems that often fall short of the protections offered against other tracking technology.

SIDEBAR 3: Face recognition and the Fourth Amendment.

Before 1967, the Supreme Court generally adhered to a property-based view of the Fourth Amendment. Judges' rulings on whether or not a Fourth Amendment "search" occurred largely turned on the existence of trespass.[104] In 1967, however, the Court declared in *Katz v. U.S.* that "the Fourth Amendment protects people, not places."[105] In a concurrence, Justice Harlan set forward a test, additional to trespass, to determine whether or not a Fourth Amendment "search" had occurred: Has the government infringed on an expectation of privacy that "society is prepared to recognize as 'reasonable'"?[106] This became known as the "reasonable expectation of privacy" test.

The Supreme Court has never formally recognized a reasonable expectation of privacy in public conduct. In the 1983 case of *U.S. v. Knotts*, the Supreme Court found that the use of technology to track a person's public movements—movements otherwise visible to the naked eye—did not infringe a reasonable expectation of privacy.[107] In *U.S. v. Jones* (2012), the Court reiterated that it had not "deviated from the understanding that mere visual observation does not constitute a search."[108]

---

[103] *See* Pennsylvania JNET, *Pennsylvania Justice Network 2012–2013 Annual Report*, Document p. 016738; *Welcome to the JNET Facial Recognition System Slides*, (May 5, 2014) Document p. 010750.
[104] *See* Olmstead v. United States, 277 U.S. 438, 473–75 (1928).
[105] *See* Katz v. United States, 389 U.S. 347, 351 (1967).
[106] *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
[107] See United States v. Knotts, 460 U.S. 276, 282 (1983) (finding that a criminal defendant lacked a reasonable expectation of privacy in his movements on public roads where those movements were visually observable to the public, and that police use of a beeper to track those movements "does not alter the situation").
[108] 132 S. Ct. 945 at 953 (2012).

Nevertheless, in *Jones*, a "shadow majority" of five justices expressed a willingness to reevaluate the contours of the reasonable expectation of privacy test to encompass some forms of geolocation tracking of public movements.[109] In later cases, the Supreme Court highlighted the transformational nature of 21st century surveillance technology—and rejected simplistic comparisons of modern technology to older policing practices. In *Riley v. California* (2014), for example, the Court ridiculed the government's contention that a search of an arrestee's smartphone was "materially indistinguishable" from a search of a person's pockets upon arrest. "That is like saying a ride on horseback is materially indistinguishable from a flight to the moon," Justice Roberts wrote.[110]

At publication, no cases in any state or federal court—let alone the Supreme Court—have addressed whether any form of law enforcement face recognition constitutes a Fourth Amendment search. It is unclear whether the Court would treat face recognition as being tantamount to "mere visual observation"—or if the Court would analogize it to space travel.

1. Courts have limited geolocation tracking—but not face recognition.

Except for forensic analysis of latent fingerprints and DNA, law enforcement collection of biometric information has typically required a physical search or handling of a suspect—e.g., reaching into their mouth for a buccal swab, or rolling their fingers on an inkpad. The physical nature of these searches or seizures may seem like a small detail, but it has major consequences for the Fourth Amendment: Namely, it means that judges have felt comfortable regulating that conduct under the Fourth Amendment.[111]

Face recognition changes the equation by allowing tracking and identification outside of a traditional Fourth Amendment search or seizure. The Pinellas County Sheriff's Office's use policy for mobile biometric identification (**Figure TK** below) illustrates this powerfully.

3. Individuals will not be physically detained for the purpose of taking a biometric sample for identification. Deputies should ask for consent; however this does not preclude a deputy taking the photograph of a person in a public place provided the deputy has not hindered the movement of the person.

   a. Physical force shall not be used for the purpose of taking a photograph or fingerprint.

   b. An individual in public shall **not** be stopped or told to pose for a photograph when it is not being done for a law enforcement investigation, i.e., a person in a motor vehicle shall not be required to roll down tinted windows or uncover their face just for the purpose of taking their photograph.

4. All biometric and search activity are logged and subject to audit.

5. Deputies are encouraged to use biometric identification whenever practical.

Figure TK. Pinellas County Sheriff's Office, Standard Operating Procedure: Mobile Biometric Usage.[112]

[109] *See* United States v. Jones ,132 S. Ct. 945 at 954 (Sotomayor, J., concurring); 132 S. Ct. 945 at 957–58 (Alito, J., concurring) (2012).
[110] *See* Riley v. California, 134 S.Ct. 2473, 2488 (2014).
[111] *See* Maryland v. King, 133 S.Ct. 1958, 1968–1969 (2013) ("It can be agreed that using a buccal swab on the inner tissues of a person's cheek in order to obtain DNA samples is a search."); Florida v. Hayes, 470 U.S. 811, 816 (1985) (finding that a Fourth Amendment seizure has clearly occurred where the police "forcibly remove a person from his home or other place in which he is entitled to be and transport him to the police station").
[112] Pinellas County Sheriff's Office, *Standard Operating Procedure POB 52: Mobile Biometric Usage* (Jan. 12, 2016), Document p. 014375.

PCSO bars officers from physically detaining individuals, and stresses that the absence of consent should not preclude officers from taking a photograph in a public place. Rather, if someone is in public, officers are encouraged to photograph that person and use biometric identification "whenever practical."[113]

In this respect, face recognition is not alone—geolocation tracking via cell-site location information, automated license plate readers (ALPRs), and drones also allow tracking through non-invasive observation. Thus, as **Sidebar 3** suggests, *all* of these tracking technologies would seem to fall into a constitutional grey area.[114]

And yet a growing number of state supreme courts and lower federal courts *are* interpreting the Fourth Amendment to limit public surveillance. This is clearest with geolocation tracking. Federal district courts in California and New York have found that individuals do have a reasonable expectation of privacy in the extended records of their movements revealed by cell-site location information—and that the Fourth Amendment requires police to get a warrant to obtain this information.[115] The highest courts of Massachusetts and New Jersey have done the same, although each state reached this conclusion by interpreting their state constitutions, rather than the Fourth Amendment.[116] In these cases, the courts recognized that dragnet-style surveillance raises serious and novel privacy concerns—and that those concerns are not extinguished by the fact that the behavior tracked occurs in public.[117]

To date, however, not a single state or federal court has considered the question of whether a face recognition search constitutes a search for the purposes of the Fourth Amendment, or an analogous provision in a state constitution. As a result, the Fourth Amendment implications of face recognition technology remain an open question.

2. Legislatures have not placed meaningful limits on law enforcement face recognition.

---

[113] Pinellas County Sheriff's Office, *Mobile Biometric Usage Policy* (Apr. 26, 2016), Document p. 014375.
[114] Cell-site location tracking—tracking a suspect's smartphone by getting location information from his wireless carrier—hits another Fourth Amendment hurdle: The idea that we have no reasonable expectation of privacy in information we volunteer to a third party—in the present case, our phone company. *See*, *e.g.*, Smith v. Maryland, 442 U.S. 735, 746–47 (1979); United States v. Graham, 824 F.3d 421, 437-38 (4th Cir. 2016) (en banc).
[115] *See* In re Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1023 (N.D. Cal. 2015), *appeal dismissed* (Feb. 5, 2016) (finding that "individuals have an expectation of privacy in the historical CSLI associated with their cell phones, and that such an expectation is one that society is willing to recognize as reasonable"); *id* at 1039 (requiring a warrant for historical cell-site location information); In re U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 119–20 (E.D.N.Y. 2011) (finding that "cell-phone users maintain a reasonable expectation of privacy in long-term cell-site-location records"); *id* at 127 (requiring a search warrant for historical cell-site location information).
[116] *See* Commonwealth v. Augustine, 4 N.E.3d 846, 865-66 (Mass., 2014), *State v. Earls*, 70 A.3d 630, 644 (N.J., 2013). Separately, *see* Tracey v. State, 152 So. 3d 504, 526 (Fla. 2014), *reh'g denied* (Dec. 8, 2014) (imposing a probable cause requirement for obtaining real-time cell-site location data in Florida);
[117] *See e.g.*, In re Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1020–21 (discussing the *Knotts* court's indication that dragnet-style surveillance would raise issues distinct from those presented in the instant case); Tracey v. State, 152 So. 3d at 513 (discussing the *Knotts* court's indication that dragnet-style surveillance would raise issues distinct from those presented in the instant case).

The Fourth Amendment acts as a floor, not a ceiling, for the protections the government can extend to its citizens against a particular police practice. This means that legislatures are free to create more privacy protections and safeguards than the minimum that courts believe the Fourth Amendment requires.

Legislators across the country have eagerly passed laws expanding the privacy rights of citizens against a range of 21st century public tracking technology. A total of 17 states have passed laws regulating law enforcement geolocation tracking, and 13 states have passed laws regulating law enforcement's use of drones; these laws generally require that police obtain warrants, supported by probable cause, before engaging in tracking.[118] Another 9 states have passed laws regulating police use of automated license plate readers (ALPRs).[119] Although most of these laws do not generally require warrants, they do generally limit when ALPRs can be deployed, how the data they collect can be used and shared, and how long that data can be kept.

Number of states that regulate police use of…

13
Drones

9
Automated license plate readers

17
Geolocation tracking

5
Face recognition

Not a single state has passed a law that places comprehensive limits on law enforcement use of face recognition technology. Five states have passed laws that limit some discrete aspect of police face recognition use.

- **Police Body Worn Camera Footage.** In 2015, Oregon passed a law barring face recognition searches of recordings from police body-worn cameras, but leaving open the possibility that face recognition may be used on live videos rather than recordings.[120]

[118] *See generally* Cal. Penal Code §§ 1546 *et seq.*; Colo. Rev. Stat. Ann. § 16-3-303.5; 724 Ill. Comp. Stat. Ann. 168/1 *et seq.*; Ind. Code Ann. §§ 35-33-5-15; Me. Rev. Stat. tit. 16, §§ 647 *et seq.*; Md. Code Ann. Crim. Proc. §1-203.1; Minn. Stat. § 626A.42; Mont. Code Ann. § 46-5-110; N.H. Rev. Stat. Ann. §§ 644-A:1 *et seq.*; R.I. Gen Laws Ann. §§ 12-32-1 *et seq.*; Tenn. Code Ann. § 39-13-610; Utah Code Ann. §§ 77-23c-101 *et seq.*; Va. Code Ann. § 19.2-70.3; 13 V.S.A. § 8102; Wash. Rev. Code Ann. §§ 9.73.260 *et seq.*; Wis. Stat. Ann. § 968.373; Alaska Stat. Ann. §§ 18.65.900 *et seq.*; Ind. Code Ann. 35-33-5-9; Fla. Stat. Ann. § 934.50; Ind. Code Ann. 35-33-5-9; 725 Ill. Comp. Stat. Ann. 167/1 *et seq.*; Me. Rev. Stat. tit. 25, § 4501; 2015 Nev. Rev. Stat. Ann. §493.112(2)-(4); N.C. Gen. Stat. Ann. §§ 15A-300.1 *et seq.*; N.D. Cent. Code Ann. §§ 29-29.4-01 *et seq.*; Or. Rev. Stat. §§ 837.310 *et seq.*; Tenn. Code Ann. §§ 39-13-609, 39-13-902; Utah Code Ann. §§ 63G-18-101 *et seq.*; Vt. Stat. Ann. Tit. 20, § 4622; Va. Code Ann. § 19.2-60.1.

[119] Cal. Veh. Code § 2413; Cal. Civ. Code §§ 1798.29, 1798.90.5; Colo. Rev. Stat. Ann. § 24-72-113; Me. Rev. Stat. tit. 29-a, § 2117-A; Md. Code Ann., Pub. Safety § 3-509; Minn. Stat. §§ 13.82, 13.824, 626.847; N.H. Rev. Stat. Ann. §§ 261.75-b, 236.130; N.C. Gen. Stat. Ann. §§ 20-183.30 *et seq.*; Utah Code Ann. §§ 41-6a-2001 *et seq.*; Vt. Stat. Ann. tit. 23, §§ 1607 *et seq.*

[120] *See* Or. Rev. Stat. § 133.741(1)(b)(D).

Recently, New Hampshire passed a similar law, which will take effect in 2017.[121] (Below the level of state law, the city of Cincinnati adopted a similar regulation, and six local police departments have adopted use policies roughly to this effect.)[122]

- **Police Drone Footage.** Two states, Maine and Vermont, have passed laws restricting the use of face recognition on footage collected by police drones. The Vermont law states that face recognition shall not be used on any data that a drone collects "on any person, home, or area other than the target of the surveillance."[123]The Maine law is more ambiguous, requiring state officials to issue rules for drones that will restrict the use of face recognition.[124]

- **Destruction of Records.** Michigan law requires the destruction of biometric data, including the fingerprint and face recognition data from people who are arrested but never charged or who are found innocent.[125] The law provides little else by way of protection, however. Instead, it expressly authorizes the collection of biometric data for almost all crimes, and expressly allows non-criminal biometric information—for example, face recognition data derived from a driver's license photo—to be used for criminal purposes.[126]

---

[121] *See* N.H. Rev. Stat. Ann. § 105-D:2(XII) (effective Jan. 1, 2017).

[122] The city of Cincinnati and police departments in five other localities bar searches of body-worn camera recordings, but allow analysis of footage from particular incidents. *See* Cincinnati Police Department, *Body Worn Camera System* (July 14, 2016), https://www.bwcscorecard.org/static/policies/2016-07-14 Cincinnati - BWC Policy.pdf ("Stored video and audio from a BWC shall not . . . Be searched using facial recognition software. [. . .] This does not prohibit CPD from using recognition software to analyze the recording of a particular incident when reasonable suspicion exists that a specific suspect or person in need of assistance may be a subject of a particular recording."); Baltimore Police Department, Policy 824: Body Worn Cameras Pilot Program (Oct. 26, 2015), https://www.bwcscorecard.org/static/policies/2015-10-26%20Baltimore%20-%20BWC%20Policy.pdf ("Stored video and audio data from a BWC shall not … be searched using facial recognition software" but same exception); Baltimore County Police Department, *BCoPD Body-Worn Camera Use Policy* at "System Recordings", https://www.bwcscorecard.org/static/policies/2016-07-14%20Baltimore%20County%20-%20BWC%20Policy.pdf ("System records … may not be … searched using facial recognition software" but same exception); Montgomery County Police Department, Body *Worn Camera System* (Apr. 20, 2016), https://www.bja.gov/bwc/pdfs/MCPD-BWCS-Pilot-Program-Summary-Report.pdf ("The stored video and audio data from a BWCS recording may not … be searched using facial or voice recognition software" but same exception); Parker Police Department, *Parker Police Department Policy and Procedures Manual: Recording Devices and Imaging Equipment* (May 6, 2016),, https://www.bwcscorecard.org/static/policies/2016-05-06 Parker - BWC Policy.pdf ("The Department shall not utilize any biometric technology, such as facial recognition, to conduct searches of video files. Stored video and audio data from a BWC shall not … be searched using facial recognition software" with same exception). The Boston police adopted a policy that appears to bar real-time face recognition. *See* Boston Police Department, *Body-Worn Camera Pilot Program Policy* (July 12, 2016), https://www.bwcscorecard.org/static/policies/2016-07-12 Boston - BWC Policy.pdf ("BWC's will not include technological enhancements including, but not limited to, facial recognition or night-vision capabilities.").

[123] Vt. Stat. Ann tit. 20 § 4622(d)(2) ("Facial recognition or any other biometric matching technology shall not be used on any data that a drone collects on any person, home, or area other than the target of the surveillance.").

[124] Me. Rev. Stat. Ann. tit. 25 § 4501(5)(D) ("Restrictions on the use of … facial recognition technology, thermal imaging and other such enhancement technology").

[125] *See* Mich. Comp. Laws Ann. § 28.243(7)-(8).

[126] Mich. Comp. Laws Ann. § 28.243 at (1), (2), (4), (5); Mich. Comp. Laws Ann. § 28.248.

Given their limited scope, none of these laws provide the range of protections afforded by most state laws governing geolocation tracking, drones, or automated license plate readers.

Apart from regulating police face recognition systems, seven states directly or indirectly curb law enforcement access to state department of motor vehicle face recognition systems, which are typically designed to detect identity fraud. Maine, Missouri, New Hampshire and Vermont have blanket bans on their DMVs using biometric technology or collecting biometric data.[127] Washington stipulates that the DMV can use biometric technology only to verify the identity of a license or ID card holder.[128] Both Washington and Oregon prohibit disclosure of biometric data to law enforcement, although Washington allows disclosure for identity theft crimes.[129] Hawaii's regulations do not expressly address face recognition, but nonetheless block law enforcement access to license photos outside of investigations into identity theft.[130]

The few, discrete protections that these laws do provide may be easily evaded. Vermont law, for example, expressly prohibits its Department of Motor Vehicles from implementing "any procedures or processes for identifying applicants for licenses, learner permits, or non-driver identification cards that involve the use of biometric identifiers."[131] Somehow, however, Vermont has interpreted this provision to allow the FBI to request—and obtain—face recognition searches of 1.8 million Vermont driver's license and ID photos.[132] Given that they do not directly constrain law enforcement, other states' DMV provisions could be read in a similarly narrow manner.

3. Most police departments place few constraints on face recognition.

In September 2015, the Department of Justice announced a new policy for federal law enforcement's use of cell-site simulators. Up until that point, the Department had obtained what

[127] *See* Me. Rev. Stat. Ann. tit. 29-A, § 1401 ("9. Use of biometric technology. The Secretary of State may not use biometric technology, including, but not limited to, retinal scanning, facial recognition or fingerprint technology, to produce a license or nondriver identification card."); Mo. Ann. Stat. § 302.189 ("The department of revenue shall not use, collect, obtain, share, or retain biometric data nor shall the department use biometric technology, including, but not limited to, retinal scanning, facial recognition or fingerprint technology, to produce a driver's license or nondriver's license or to uniquely identify licensees or license applicants for whatever purpose."); N.H. Rev. Stat. Ann. § 260:10-b ("The state shall not collect, obtain, or retain any biometric data in connection with motor vehicle registration or operation, or in connection with driver licensing.") and N.H. Rev. Stat. Ann. § 263:40-b ("The department is prohibited from using any facial recognition technology in connection with taking or retaining any photograph or digital image for purposes of this chapter."); Vt. Stat. Ann. tit. 23, § 634(c) ("The Department of Motor Vehicles shall not implement any procedures or processes for identifying applicants for licenses, learner permits, or nondriver identification cards that involve the use of biometric identifiers.")

[128] *See* Wash. Rev. Code Ann. § 46.20.037(1) (stipulating that DMV may use its face recognition system "only to verify" applicants identities and prevent identity fraud).

[129] *See* Wash. Rev. Code Ann. § 46.20.037(4)(d); Or. Rev. Stat. Ann. § 807.026 ("biometric data may not be made available to anyone other than employees of the [Department of Transportation] acting in an official capacity").

[130] Haw. Code R. § 19-122-1(g) ("Except as may be required by law, the examiner of drivers shall not permit a digital image or personal information obtained from a state of record to be accessed or used by a law enforcement agency or personnel of such agency for any other purpose.")

[131] *See* Vt. Stat. Ann. tit. 23, § 634(c).

[132] *See* U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 47 (May 2016).

it viewed as "appropriate legal authorization" before using the devices.[133] The authorization was less than a warrant; rather, the Department had merely certified to a judge that the information being obtained was "relevant to an ongoing criminal investigation."[134] Now, however, the Department announced that, not as a matter of law, but "as a matter of policy," federal law enforcement would seek a warrant before using a cell-site simulator.[135]

The Department of Justice's announcement illustrates an important and often overlooked principle: Law enforcement agencies are free to voluntarily adopt restrictions on tracking technology that go above and beyond their view of what current statutes or case law requires.

While some agencies have exercised that authority, a surprising number of police departments appear to have not taken basic steps to limit use of face recognition. We can evaluate these agencies on three simple metrics:

- Have they adopted a use policy telling officers when it is appropriate to use face recognition, and how they should and should not use it?
- What degree of individual suspicion do they require prior to running a search?
- Do they limit the use of face recognition to certain serious offenses?

a) A surprising number of agencies have not adopted use policies.

Of 52 agencies, at least 24 either did not provide a face recognition use policy in response to our document requests, or were clearly covered by another agency's use policy.[136] At least five of those agencies—the Daytona Beach Police Department, the Jacksonville Sheriff's Office, the Nebraska State Patrol, the Kansas City Police Department (former program), and the Iowa Department of Public Safety—expressly acknowledged that they did not

[133] *See* Office of Public Affairs, Department of Justice, *Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators (*Sept. 3, 2015), https://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators.
[134] U.S. Department of Justice, D*epartment of Justice Policy Guidance: Use of Cell-Site Simulator Technology (*Sept. 3, 2015) at 4*,* https://www.justice.gov/opa/file/767321/download.
[135] *See* Department of Justice, *Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology (*Sept. 3, 2015) at 3, https://www.justice.gov/opa/file/767321/download ("While the Department has, in the past, appropriately obtained authorization to use a cell-site simulator by seeking an order pursuant to the Pen Register Statute [*sic*], *as a matter of policy*, law enforcement agencies must now obtain a search warrant supported by probable cause…") (emphasis added); *see also* 18 U.S.C. § 3122(b)(2) (pen register statute requiring "a certification… that the information obtained is relevant to an ongoing criminal investigation being conducted by that agency").
[136] These agencies are: Baltimore Police Department; Chicago Police Department; Daytona Beach Police Department; Iowa Department of Public Safety; Jacksonville Sheriff's Office; Los Angeles County Sheriff's Department; Los Angeles Police Department; Maryland Department of Public Safety and Correctional Services; Maryland State Police; Miami Police Department; Minnesota Department of Public Safety; Montgomery County Police; Nebraska State Patrol; San Francisco Police Department; Tampa Police Department; Texas Department of Public Safety; Virginia State Police; Arizona Department of Public Safety; Auburn Police Department; Illinois State Police; Kansas City Police Department; New Bedford Police Department; Plymouth County Sheriff's Department; and the San Jose Police Department.

have a use policy (or, in the case of Iowa, a "finalized" use policy) for law enforcement face recognition.[137]

b) A minority of agencies clearly require individualized suspicion prior to search.

Even though several agencies provided contract documents for real-time face recognition systems, not a single agency provided documents suggesting that they require a warrant—or judicial approval of any kind—prior to any face recognition search.

The agencies did, however, impose different kinds of legal restrictions that do not require judicial approval. Some agencies require officers to have an individualized suspicion that the individual whose photo is being submitted for a search be involved in a crime, but they vary in the degree of suspicion required. The agencies may require that officers have **probable cause** to believe that the individual search for was involved in a crime, or the agencies may merely require that an officer have **reasonable suspicion** to that effect.

Other agencies do not require any degree of individualized suspicion and instead only stipulate that face recognition searches must be conducted for **criminal justice or law enforcement purposes**. In these jurisdictions, anyone's face can be searched in their face recognition database, so long as this is done in furtherance of a law enforcement mission.

Overall, of the 52 agencies, plus the FBI face recognition unit (FACE Services), we were able to determine the legal standard that applied to face recognition for only 24 of them, plus the FBI. Of those agencies, three required probable cause, and 10 required reasonable suspicion. The remainder either required a criminal justice purpose or provided no documentation to suggest a legal standard of any kind. Putting it differently, only 13 of 52 agencies (25%) clearly required *any* degree of individualized suspicion (e.g. reasonable suspicion or probable cause) prior to a face recognition search.

[137] *See* Daytona Beach Police Department, *Interview with Jimmy Flynt* (Jan. 19, 2016) Document p. 000107; Jacksonville Sheriff's Department, *Interview with Crime Analysis Unit Manager Celbrica Tenah* (Feb. 17, 2016) Document p. 010709; Nebraska State Patrol, *Letter from Agency Legal Counsel Wendy Wussow* (Feb. 16, 2016), Document p. 009181; Kansas City Police Department, *Interview with Sgt. Jake Becchina* (Jan. 28, 2016), Document p. 010191; Iowa Department of Public Safety, *Letter from Commissioner Roxann M. Ryan to Clare Garvie* (Apr. 1, 2016), Document p. 011911 ("Our Department has not yet adopted a final policy."). Note that while the Daytona Beach and Jacksonville jurisdictions access the Pinellas County Sheriff's Department face recognition system, they do not appear to be required to follow the Pinellas County use policy.

Figure TK. Legal Standards for Face Recognition Search, by Jurisdiction
Agencies reporting discontinued face recognition programs are in italics.

		All Agencies	Moderate Risk Deployments	High Risk Deployments
Individualized Suspicion Required	**Probable Cause**	Maryland DPS Michigan State PD Albuquerque PD, NM	Albuquerque PD, NM	Maryland DPS Michigan State Police[138]
	Reasonable Suspicion	Carlsbad PD, CA Chula Vista PD, CA SANDAG, CA San Diego PD, CA Honolulu PD, HI Iowa DPS *Cumberland Co., ME* King County SO, WA Seattle PD, WA South Sound 911	Carlsbad PD, CA Chula Vista PD, CA SANDAG, CA San Diego PD, CA Honolulu PD, HI *Cumberland Co. SO, ME* King County SO, WA Seattle PD, WA South Sound 911	Iowa DPS
Individualized Suspicion Not Required	**Criminal Justice or Law Enforcement Purpose**	FBI FACE Services Pinellas Co. SO, FL Chicago PD, IL *Illinois State PD* Prince George's Co., MD Michigan State Police Minnesota DPS Lincoln PD, NE Ohio BCI Virginia State PD NOVARIS, VA WVI/FC	Chicago PD, IL Prince George's Co., MD Minnesota DPS Virginia State PD NOVARIS, VA WVI/FC	FBI FACE Services Michigan State Police Pinellas Co. SO, FL *Illinois State PD* Lincoln PD, NE Ohio BCI
Unknown		Maricopa Co. SO, AZ *Arizona DPS* LA Co. SO, CA Los Angeles PD, CA San Diego Co. SO, CA San Francisco PD, CA *San Jose PD, CA* Daytona Beach PD, FL Jacksonville SO, FL Miami PD, FL Palm Beach Co. SO, FL Tampa PD, FL Hawaii CJDC	LA Co. SO, CA San Diego Co. SO, CA San Francisco PD, CA *San Jose PD, CA* Hawaii CJDC *Auburn PD, MA* *New Bedford PD, MA* *Plymouth Co. SD, MA* Kansas City PD, MO Texas DPS Fairfax Co. PD, VA *Pierce County SO, WA* Snohomish Co. SO, WA	Maricopa Co. SO, AZ *Arizona DPS* Los Angeles PD, CA Daytona Beach PD, FL Jacksonville SO, FL Miami PD, FL Palm Beach Co. SO, FL Tampa PD, FL Maryland State PD Baltimore PD, MD Montgomery Co. PD, MD Nebraska State PD Pennsylvania JNET

[138] The Michigan State Police requires probable cause, or that a subject is unable to provide identification due to incapacitation, for the use of face recognition on mobile devices. *See* Michigan State Police, *SNAP Acceptable Use Policy*, Document pp. 011436–011439 (Michigan Department of State images encompass driver's license photographs). It is unclear from the use policy what the standard is for desktop searches, but in correspondence the Department indicated that a "law enforcement reason" is required. Michigan State Police, *Letter to Clare Garvie on state one-page feedback,* Document p. 016824. Both mobile and desktop systems can run searches against Michigan's driver's license photo database. Michigan State Police therefore is listed both in Probable Cause : High Risk Deployment and Unknown : High Risk Deployment.

	Auburn PD, MA *New Bedford PD, MA* *Plymouth Co. SO, MA* Maryland State PD Baltimore PD, MD Montgomery Co. PD, MD Kansas City PD, MO Nebraska State PD Pennsylvania JNET Pennsylvania State PD Carlisle Borough PD, PA Philadelphia PD, PA Texas DPS Fairfax Co. PD, VA *Pierce County SO, WA* Snohomish Co. SO, WA		Pennsylvania State PD Carlisle Borough PD, PA Philadelphia PD, PA

Perversely, as **Figure TK** shows, the agencies engaging in higher risk deployments appear less likely to require individualized suspicion. Of the 29 agencies that have used face recognition under a Moderate Risk deployment model—either Stop and Identify or Arrest and Identify using a mug shot database—10 of them (34.5%) required some form of individualized suspicion. Meanwhile, of the 24 agencies (including the FBI) that have used a High Risk deployment—Stop and Identify or Arrest and Identify using a driver's license database—only three (12.5%) require individualized suspicion.

Agencies engaging in higher risk deployments appear *less* likely to require individualized suspicion for a search.

The absence of an individualized suspicion requirement means that face recognition may be used on effectively anyone—e.g., a pedestrian anywhere near a crime—so long as some criminal justice purpose can be cited for the search. At least three agencies—including the FBI face recognition unit (FACE Services)—expressly allow face recognition searches to identify witnesses to a crime, not just criminal suspects.[139]

c) Only one agency limits face recognition use to certain crimes.

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 federal wiretaps of

[139] The other agencies are the Michigan State Police and the Pennsylvania Justice Network. Federal Bureau of Investigation, Department of Justice, *Privacy Impact Assessment for the FACE Services Unit*, at 10–11 (May 1, 2015), https://www.fbi.gov/services/records-management/foia/privacy-impact-assessments/facial-analysis-comparison-and-evaluation-face-services-unit ("Probe photos are potential subjects, victims, or witnesses of/to federal crimes that have been collected pursuant to authorized FBI investigations."). Michigan State Police, *Interview with Peter Langenfeld, Program Manager, Digital Analysis and Identification Section* (Mar. 23, 2016), Document pp. 010928 (MSP allows face recognition searches to identify witnesses to a crime, not just criminal suspects) Michigan State Police, *Mobile Facial Recognition, Web Application Instructions*, Document p. 011345 (The image of "capture" drop-down includes the categories: insufficient ID, warrant, criminal suspect, witness, victim, other as categories under which an officer can add a probe on a mobile device.). Pennsylvania Justice Network, *JNET Facial Recognition User Guide*, Document p. 010845 ("Facial recognition is used primarily with images of suspects or witnesses from surveillance or CCTV cameras, but can also be used with photos from other sources, such as social media sites or still photos.")

those communications to investigations of certain serious federal offenses. Congress gave even narrower authority to state law enforcement, allowing wiretaps only for certain felonies.[140]

There are echoes of this trend in modern law enforcement biometrics. Jurisdictions may search the FBI face recognition database (NGI-IPS) for investigations of *any* crime—regardless of the nature or the severity of the offense.[141] But in order to be enrolled in that database's "unsolved photo file"—a photo file of unidentified individuals that is compared to every new photo enrolled in the database—a photograph must pertain to an investigation of a felony offense for criminal homicide, forcible rape, robbery, or aggravated assault.[142]

Likewise, in *Maryland v. King*, the Supreme Court upheld a Maryland law requiring the collection of DNA from all individuals charged with violent crimes, burglary, or attempted burglary, and the search of their DNA against the federal DNA database, which includes forensic DNA samples from unsolved crimes.[143] In upholding that program and differentiating it from a generalized search, however, the Court cited the "fundamental" distinction that Maryland's DNA searches were limited to individuals arrested, detained, and charged with a serious criminal offense.[144]

None of the 52 responsive agencies clearly restricted face recognition use to more serious crimes. Only one, the Nebraska State Patrol, limited its use to a certain kind of offense—identity theft.[145]

SIDEBAR 4: Scoring Fourth Amendment Protections

Our score for Fourth Amendment protections turns on the level of individualized suspicion required prior to running a face recognition search. Where a jurisdiction relies on a driver's license rather than a mug shot database, however, the score takes into account proportionality (i.e., Does the jurisdiction restrict the use of dragnet-style driver's license photo databases to the investigation of serious offenses or identity crimes?). In other words, our score uses a bifurcated standard. If the agency uses face recognition on databases that include only mug shots, the first standard is used. If the agency uses face recognition on databases that include driver's license photos, the second standard is used.

- **Targeted database—mug shots only.**

---

[140] *See* The Omnibus Crime Control and Safe Streets Act of 1968 (Pub.L. 90–351, 82 Stat. 197, enacted June 19, 1968, codified at 42 U.S.C. § 3711); 18 U.S.C. § 2516(1)-(2).
[141] *See* Criminal Justice Information Services Division, Federal Bureau of Investigation, U.S. Department of Justice, *Interstate Photo System (IPS) Policy and Implementation Guide (Version 1.2)* (Sept. 3, 2014) Document p. 009325 (not establishing any crime-based limitation on searches and stating that "[i]t is the responsibility of the user agency to develop appropriate usage policies for the IPS component…").
[142] *See* Criminal Justice Information Services Division, Federal Bureau of Investigation, U.S. Department of Justice, *Interstate Photo System (IPS) Policy and Implementation Guide (Version 1.2)* (Sept. 3, 2014) at 3, Document p. 009320) (specifying that such photos must be "lawfully obtained pursuant to an authorized criminal investigation and meeting a felony crimes against persons Uniform Crime Report coding definition").
[143] *Maryland v. King*, 133 S.Ct. 1958, 1979-80 (2013); Md. Code Ann., Pub. Safety 2-504(d)(1).
[144] *Maryland v. King*, 133 S.Ct. 1958, 1977-78 (2013).
[145] *See* Nebraska State Patrol, *Memorandum of Understanding between the Nebraska State Patrol and the Nebraska DMV* , Document p. 009190 (restricting Nebraska State Patrol's access to the Nebraska DMV's photo repository for the purpose of "enhanc[ing] the ID Theft Task Force Working Relationship between the NSP and the DMV").

- Green: Reasonable suspicion of the subject to be searched, and at least one of the following: (1) searches are limited to suspects and victims of crimes; and (2) Investigate and Identify searches are limited to felonies only.
- Yellow: Reasonable suspicion of the subject to be searched but the standard has exceptions or allows for searches for bystanders or witnesses as well.
- Red: No legal standard stated, or a statement that face recognition may be used for any "law enforcement" or "criminal justice" purpose.

- **Dragnet database—license and ID photos.**
  - Green: (1) Searches are limited to investigations of serious offenses *and* require a warrant or court order supported by probable cause; or (2) searches are limited to identity-related crimes.
  - Yellow: Probable cause searches are limited to investigations of serious offenses (for non-identity-related crimes).
  - Red: Anything less than probable cause (for non-identity crimes).

C. FREE SPEECH

J. Edgar Hoover kept track of his opponents. Hoover's FBI conducted surveillance on Martin Luther King, Jr., Fannie Lou Hamer, Cesar Chavez, Marcus Garvey, and many other civil rights leaders.[146] Public protests were seen as a threat. FBI agents, disguised as freelance photographers, were sent to photograph them. According to a candid memoir from an FBI undercover photographer, Richard Coffman:

> Following Martin Luther K.'s 'I Have a Dream Speech' it was discovered that some of our 'Most Wanted' and several subjects of our Domestic Security investigations liked to participate or show up at the various demonstrations. Many of them mostly attracted by the anonymity, opportunity of free drugs and easy available sex. On some of the really large demonstrations I would recruit a dozen or so fellow Agents, instruct them how to not look like FBI Agents and how to mingle among the 'Hippies' and other protest types and see and report what was going on.[147]

Coffman took special interest in surreptitious photographs of interracial couples and nude or partially nude female protesters, which he shared with other law enforcement officials.[148]

Today's FBI is a different place. In training, every FBI agent learns about the agency's surveillance of Dr. King.[149] But the specter of political surveillance survives. In a 2012 Senate

---

[146] *See* Alvaro Bedoya, *The Color of Surveillance*, *Slate* (Jan. 18, 2016), http://www.slate.com/articles/technology/future_tense/2016/01/what_the_fbi_s_surveillance_of_martin_luther_king_says_about_modern_spying.html.

[147] Richard C. Coffman, Eyewitness to J. Edgar Hoover's FBI 423 (2014).

[148] Coffman held weeklong photography courses for law enforcement officials, multiple times a year, to train them in remote photographic surveillance of demonstrations. At those trainings, "[t]o keep the classes awake," he would distribute albums of photos he deemed "attention getters" to "pep up" his class. These included photos of "sexually enthusiastic students cavorting nude in the Reflecting Pool;" a "shot of a minor movie starlet smiling[], but panty-less"; a "'sneak shot' of an 'Oreo-cookie couple's 'making-out'; and a "surreptitious. . . 'close-up' shot of a top-lessly attired hippie teen-age girl." Richard C. Coffman, Eyewitness to J. Edgar Hoover's FBI 425-26 (2014).

[149] *See* Federal Bureau of Investigation Director James Comey, *Hard Truths: Law Enforcement and Race*, Remarks at Georgetown University (Feb. 12, 2015), https://www.fbi.gov/news/speeches/hard-truths-law-enforcement-and-race ("There is a reason that I require all new agents and analysts to study the FBI's

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.[150] In 2015, the FBI admitted that it conducted surveillance flights over Ferguson and Baltimore during protests of police use of force.[151] The Department of Homeland Security has monitored Black Lives Matter protests.[152] And footage of Chris Wilson's protest shows an officer videotaping the event.[153]

What if every time an FBI special agent pointed his camera at a protester, the FBI could use face recognition to identify her?

Figure TK: Police videotape a 2010 Los Angeles protest. (Photo: Rogan Ferguson)

The First Amendment protects our freedom of speech and our right to "peaceably assemble, and [] petition the [g]overnment for a redress of grievances." Unfortunately, the Supreme Court's interpretation of the First Amendment may provide little protection against the use of face recognition to identify peaceful protesters. Despite the fact that leading law enforcement agencies—including the FBI and the Department of Homeland Security (DHS)—have explicitly recognized the potential chilling effect of face recognition on free speech, we

---

interaction with Dr. Martin Luther King, Jr., and to visit his memorial in Washington as part of their training … to ensure that we remember our mistakes and that we learn from them.")

[150] *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..

[151] *See* Eric Tucker, *Comey: FBI used aerial surveillance above Ferguson,* Associated Press (Oct. 22, 2015), http://www.salon.com/2015/10/22/comey_fbi_used_aerial_surveillance_above_ferguson/.

[152] *See* George Joseph, *Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson*, The Intercept (June 24, 2015), https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/.

[153] *See* WFTS Webteam, *Black Lives Matter protesters arrested at Florida State Fair*, WFTS Tampa Bay (Feb. 8, 2016), http://www.abcactionnews.com/news/local-news/black-lives-matter-protesters-arrested-at-state-fair.

found that almost none of the agencies using face recognition have adopted express prohibitions against using the technology to track political or other First Amendment activity.

1. First Amendment case law is unclear on face recognition.

First Amendment case law offers mixed guidance on whether face recognition would impermissibly chill free speech and association.[154] The Supreme Court has held that the First Amendment protects the right to *anonymous* speech and association. But the Court has also held that the mere surveillance of speech is insufficient grounds for a First Amendment violation.

a) The right to anonymous speech and association.

Face recognition, at its core, is a means of identification. In 1958, the Supreme Court held in *NAACP v. Alabama* that the NAACP could not be compelled by state law to disclose the identities—the names and addresses—of its members, on the grounds that disclosure would likely hinder the ability of those members collectively to advocate their beliefs.[155] The Court noted that there existed a "vital relationship between freedom to associate and privacy in one's associations," particularly in instances where a group advocates minority or unpopular beliefs.[156]

Talley v. California in 1960, and *McIntyre v. Ohio Elections Commission* in 1995, reaffirmed the protection of anonymous speech. In *Talley,* the Court held that a law prohibiting the distribution of anonymous pamphlets violated the First Amendment. The Court reasoned that "[t]here can be no doubt that such an identification requirement would tend to restrict freedom to distribute information and thereby freedom of expression."[157] "Anonymity," the Court said 35 years later in *McIntyre*, "is the shield from the tyranny of the majority."[158]

b) The right of the police to investigate demonstrations.

The right to free speech and association does not amount to a right to be free from surveillance, however.[159] In *Laird v. Tatum* in 1972, the Supreme Court considered whether military surveillance of public meetings and demonstrations had an "inhibiting effect" on the expression of First Amendment rights. The Court held that without a showing of past or immediate danger of direct injury, it does not. Since then, two lower federal courts have applied *Tatum* to permit police photography of public demonstrations.[160]

---

[154] *See* Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 Minn. L. Rev. 407, 543–551 (2012).
[155] 357 U.S. 449, 1174 (1958).
[156] 357 U.S. at 462.
[157] Talley v. California, 362 U.S. 60, 63 (1960).
[158] McIntyre v. Ohio Elections Com'n, 514 U.S. 334, 357 (1995).
[159] For a more in-depth analysis of case precedent in the field of Remote Biometric Identification, *see* Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 Minn. L. Rev. 407, 543–551 (2012).
[160] In 1972, the Fourth Circuit in *Donohoe v. Duling* considered whether the Richmond Police Department had infringed on people's freedom of speech and association by photographing public demonstrations, meetings, and vigils. In concluding that *Tatum* controlled, the court held that the attendees were not "chilled" by the photographic surveillance or deterred from participating in future public gatherings. Donohoe v. Duling, 465 F.2d 196, 202 (4th Cir. 1972). In *Philadelphia Yearly Meeting of Religious Society of Friends v. Tate,* the Third Circuit in 1975 considered whether the Philadelphia Police Department had violated the First Amendment by attending public meetings, photographing those in attendance, and

But there are limits to this doctrine. In *Hassan v. City of New York*, a 2015 case challenging the NYPD's pervasive video, photographic, and undercover surveillance of Muslim Americans following 9/11,[161] the Third Circuit agreed with the plaintiffs—the victims of surveillance—that the manner by which the program was administered—specifically targeting a group of people for their beliefs and religious affiliations—may have caused them "direct, ongoing, and immediate harm."[162]

While photography is a first step in face recognition, face recognition is more than photography; it is identification. As a result, we do not know what courts will say about the integration of face recognition into photographic surveillance of protests.[163]

2. Legislators and police forces could fix this problem. They haven't.

In the absence of clear protections afforded by the courts, it is critically important that legislators and police forces consider the implications of face recognition on free speech.

"Surveillance has the potential to make people feel extremely uncomfortable, cause people to alter their behavior, and lead to self-censorship and inhibition."

- The International Justice and Public Safety Network

Legislators have yet to step up to this task. As noted above, not a single state has passed legislation to comprehensively rein in face recognition—and none of the laws that have been passed address the specific risks that face recognition poses to free speech and expression. The federal Privacy Act generally prohibits the government from keeping records "describing how any individual exercises rights guaranteed by the First Amendment."[164] But the FBI is now petitioning for its face recognition system to be exempt from the enforcement of this provision.[165]

Major federal and state law enforcement agencies have recognized the threat that face recognition presents to free speech. A Privacy Impact Assessment drafted in 2011 by DHS, the FBI, and a number of state police agencies, considered the effects of law enforcement face

---

compiling and sharing those photographs and other information on attendees with other law enforcement agencies and private entities. The court found that "mere police photographing and data gathering at public meetings" is "legally unobjectionable and creates at best a so-called subjective chill" insufficient to form the basis of a First Amendment claim. Phila. Yearly Meeting of Religious Soc'y of Friends v. Tate, 519 F.2d 1335, 1137–38 (3d Cir. 1975).

[161] Hassan v. City of New York, 804 F.3d 277, 285 (3d Cir. 2015).

[162] Hassan v. City of New York, 804 F.3d 277, 292 (3d Cir. 2015).

[163] As Professor Donohue points out, in his dissent in *Donohoe* Judge Harrison Winter found the idea of the photographs being used to identify unknown meeting-goers to be a different—and distant—proposition. "I cannot suppose that every time a picture is taken of an unknown person it is sent to the FBI in order to determine whether that person is dangerous." Donohoe v. Duling, 465 F.2d 196, 206 (4th Cir. 1972) (Winter, dissenting). Yet that is precisely what advanced face recognition would allow.

[164] 5 U.S.C. § 552a(e)(7) (2014).

[165] *See* Privacy Act of 1974; Implementation, 81 Fed. Reg. 27288, 27289 (proposed May 5, 2016) (to be codified at 28 C.F.R. pt. 16).

recognition on the "erosion or compromise of anonymity."[166] 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."[167]

To address this concern, the Assessment encourages that law enforcement use policies include express 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."[168] In such circumstances, "the collection of long range lens photographs should be limited to instances directly related to criminal conduct or activity."[169]

We surveyed many of the state law enforcement agencies that helped write the Assessment.[170] But only one agency that provided responsive records expressly addressed the use of face recognition on First Amendment activities in its policy.[171] Ohio's newly implemented rule on face recognition 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

[166] 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, 016648–016649 .
[167] 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 p. 016632.
[168] 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 p. 016649.
[169] 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 p. 016649.
[170] The NIets Facial Recognition Workgroup included officials from the FBI, New Jersey State Police, Illinois State Police, Pinellas County Sheriff's Office, Delaware State Police, SANDAG ARJIS, and the Oregon State Police. 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 p. 016627.
[171] Other agencies, including the Seattle Police Department, West Virginia Intelligence Fusion Center, and Pennsylvania JNET, have general policies or procedural orders that limit what and how information about a person's religious, political, or other affiliation may be gathered and retained by the agency. Seattle Police Department, *Email from Karim Miller to Clare Garvie* (Sept. 13, 2016), Document p. 016829 ("Information will be gathered and recorded in a manner that does not unreasonably infringe upon: individual rights, liberties, and freedoms guaranteed by the Constitution of the United States and the State of Washington, including freedom of speech, press, association, and assembly . . ."); West Virginia Intelligence Fusion Center, *Privacy Policy*, Document p. 009926 ("The WVI/FC will not seek or retain information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event"); Pennsylvania JNET, *Pennsylvania JNET Privacy Policy*, Document p. 016804 ("JNET . . . does not seek and/or retain information about individuals solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event . . . "). The PIA articulates the importance of expressly prohibiting the use of face recognition specifically on protected activities—face recognition is an identification tool, and "[t]he potential harm of identification is that it increases the government's power to control individuals through the chilling effects." 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 p. 016648.

> 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.[172]

The FBI appears to be implementing the PIA's recommendations by directing users of its face recognition systems to adopt similar rules. The FBI face recognition database Policy and Implementation Guide states: "All appropriate use policies must protect the constitutional rights of all persons and should expressly prohibit collection of photos in violation of an individual's 1st and 4th Amendment rights."[173] However, of the four state law enforcement agencies that provided their face recognition use policy and can submit searches to the FBI face recognition database, not one included this express prohibition.[174]

SIDEBAR 4: Scoring Free Speech Protections

Given the potential chilling effect of face recognition on protected First Amendment activities, we award the highest score on free speech protections only to agencies that expressly address—and enumerate—activities that may chill free speech in a face recognition use policy, not just a general manual or procedural order.

- Green: Express statement in a face recognition use policy prohibiting the use of face recognition to target or collect information on individuals on the basis of their race, religion, or other bases that may stifle speech.
- Yellow: (1) A statement in a face recognition use policy prohibiting the use of face recognition in violation of state or federal law, including the First Amendment; or (2) a statement in a *general* policy or police manual prohibiting the targeting or collection of information on individuals on the basis of their race, religion, or other bases that may stifle speech.
- Red: No statements outlined in either section above.

D. ACCURACY

"With an identification rate above 95% as measured by U.S. government-sponsored Face Recognition Vendor Tests, our technology is the industry's finest."

- FaceFirst website

[172] Ohio Bureau of Criminal Investigation, *To Be Added 2016 Date TBD*, Document p. 009218 (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).
[173] Criminal Justice Information Services Division, Federal Bureau of Investigation, U.S. Department of Justice, *Interstate Photo System (IPS) Policy and Implementation Guide (Version 1.2)* (Sept. 3, 2014), Document p. 009325.
[174] The following states have access to the FBI face recognition database (NGI-IPS) and provided us with their use policy: Hawaii; Maryland; Michigan; and Florida.

"FaceFirst makes no representations or warranties as to the accuracy and reliability of the product in the performance of its facial recognition capabilities."

- FaceFirst contract with the San Diego Association of Governments

In police face recognition, there are high stakes to accuracy. An accurate algorithm correctly identifies a face in an ATM photo and leads police to a robber's door. An inaccurate algorithm sends them to the wrong house—and could send an innocent person to jail.[175]

Face recognition companies understand this, and promise police departments seemingly sky-high accuracy standards. The website of FaceFirst, which uses Cognitec's algorithm in face recognition software that it sells to police, states that "[w]ith an identification rate above 95% as measured by U.S. government-sponsored Face Recognition Vendor Tests, our technology is the industry's finest."[176] This is misleading: the 95% figure is a decade old and vastly oversimplifies the nuances of accuracy into a single number from a single test.[177] Since 2006, Cognitec's algorithm has doubtlessly changed dramatically—and the tests have certainly gotten harder too.[178]

In fact, FaceFirst has made sure that it will not be held to this high standard. A 2015 contract with one of the largest police face recognition systems in the country, the San Diego Association of Governments, includes the following disclaimer: "FaceFirst makes no representations or warranties as to the accuracy and reliability of the product in the performance of its facial recognition capabilities."[179]

Compared to fingerprinting, state-of-the-art face recognition is far less reliable and well-tested. Yet other than instructing the recipients of potential face recognition matches that search results are only investigative leads—not conclusive evidence—jurisdictions and other stakeholders take too few steps to protect against false positives and other errors.

---

[175] *See* Simson Garfinkle, Future Tech, Discover, 23.9 (2002): 17–20 (reporting false positive error generated by face recognition technology in use at the Fresno Yosemite International Airport), http://simson.net/clips/2002/2002.Discover.09.FaceID.pdf; *Cf.* Eric Licthblau, *U.S. Will Pay $2 Million to Lawyer Wrongly Jailed*, N.Y. Times (Nov. 30, 2006) (describing the case of Brandon Mayfield, who was wrongly linked to the 2004 Madrid train bombings as the result of a faulty fingerprint identification); Office of the Inspector General, U.S. Department of Justice, *A Review of the FBI's Handling of the Brandon Mayfield Case* (Jan. 2006) at 1, https://oig.justice.gov/special/s0601/exec.pdf (describing process by which automated fingerprint matching system and FBI human examiner incorrectly matched Mayfield's prints to Madrid bomber's).

[176] FaceFirst, *Frequently Asked Questions*, http://www.facefirst.com/faq (last visited Sept. 1, 2016).

[177] *See* FaceFirst, *Frequently Asked Questions*, http://www.facefirst.com/faq (last visited Sept. 1, 2016) (archived copy available at https://web.archive.org/web/20160119232512/http://www.facefirst.com/faq and on file with authors) (acknowledging 95% figure is drawn from a 2006 accuracy test).

[178] *See* Patrick Grother and Mei Ngan, *Face Recognition Vendor Test: Performance of Face Identification Algorithms*, NIST Interagency Report 8009 (May 26, 2014), http://biometrics.nist.gov/cs_links/face/frvt/frvt2013/NIST_8009.pdf.

[179] SANDAG, *Arjis Contract with Facefirst, LLC*, Document p. 008358.

1. Accuracy remains a work in progress. Real-time systems and systems with large databases are especially error-prone.

Face recognition is widely considered to be less accurate than fingerprint identification.[180] Age changes faces, as do cosmetics, inebriation, and obstructions like glasses or hair.[181] Fingerprints, in contrast, are relatively consistent over time, although they can be altered by accidents or prolonged, manual labor.[182] Fingerprinting has over a century-long track record in law enforcement. The first, primitive face recognition algorithms were developed in the early 1990s.[183]

When face recognition is run on photos captured at a distance, it is often subject to a wider range of environments. 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.[184]

Real-time, continuous video surveillance systems tend to combine the worst of these traits, rendering them less accurate than many other deployments. Unlike mug shot-based systems, which use photos captured in controlled settings according to strict standards,[185] real-time systems must contend with people going about their daily lives. Subjects rarely face the camera straight on, and video stills are often poorly or unevenly lit. The security cameras themselves vary in quality and are often mounted on ceilings. They often capture only the tops of people's heads.

In a real-time experiment set in a train station in Mainz, Germany from 2006 to 2007, lighting was a major problem. Accuracy was at 60% during the day but 10–20% at night.[186] A report on the experiment notes the challenge of uncontrolled image capture: "cooperative

---

[180] *See, e.g.,* Patrick J. Grother, et. al., *Multiple-Biometric Evaluation, Report on the Evaluation of 2D Stll-Image Face Recognition Algorithms*, NIST Interagency Report 7709 at 2, National Institute of Standards and Technology (Aug. 24, 2011), http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=905968 ("Face images have been collected in law enforcement for more than a century, but their value for automated identification remains secondary to fingerprints.").

[181] *See* Anil Jain & Brendan Klare, *Face Matching and Retrieval in Forensics Applications*, 19 IEEE MultiMedia 1, 20 ("The face recognition community has recognized four key factors that significantly compromise recognition accuracy: pose, illumination, expression, and aging.").

[182] *See* Mark Hawthorne, *Fingerprints: Analysis and Understanding* 21 (2008) ("Friction skin is Permanent. That is, the skin does not change under normal conditions from the time of formation until decomposition after death. . . Friction skin will deteriorate with age as well as all skin, but classification and identification normally will not be affected.").

[183] *See* Turk & Pentland, *Eigenfaces for Recognition*, 3 J. Cognitive Neurosci. 1, 71 (1991).

[184] *See* Patrick Grother & Mei Ngan, *Face Recognition Vendor Test: Performance of Face Identification Algorithms*, NIST Interagency Report 8009, 25 (May 26, 2014), http://biometrics.nist.gov/cs_links/face/frvt/frvt2013/NIST_8009.pdf.

[185] *See* National Institute of Standards and Technology, U.S. Department of Commerce, *American National Standard for Information Systems: Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information*, ANSI/NIST-ITL 1-2011 (Dec. 2013), http://biometrics.nist.gov/cs_links/standard/ansi_2012/Update-Final_Approved_Version.pdf.

[186] *See* Federal Criminal Police Office of Germany, Federal Ministry of the Interior, *Face recognition as a search tool—foto-fahndung*, https://www.bka.de/SharedDocs/Downloads/EN/Research/PhotographBasedSearches/fotofahndungAbschlussberichtEnglisch.pdf;jsessionid=8A41E1E76C3A9180114D9669DE618B34.live0612?__blob=publicationFile&v=1 (English version).

behavior must be attained from the wanted person."[187] Overall recognition rates averaged between 17% and 29%.[188]

Accuracy also drops as databases become larger.[189] Larger databases are more likely to contain lookalikes that mislead face recognition algorithms into picking the wrong matches. As a database size rises to a national scale, an algorithm will inevitably encounter highly similar faces. Larger databases may also be more likely to contain older images, which can drive down accuracy.[190] (See **Sidebar 5** for an explanation of accuracy measurements.)

SIDEBAR 5: Understanding Face Recognition Accuracy

The accuracy of a face recognition algorithm cannot be reduced to a single number. Algorithms make mistakes in a variety of different ways, some of which are more problematic than others. Algorithms use a photo of a subject (a *probe photo*) to search for matching faces in a database of identified face images. An algorithm can return one of two responses: an accept—a photo that it thinks is a possible match, or a reject—a concession that no matching photos were found.

- If the algorithm finds a match that indeed contains the subject, it has achieved a *true accept*—it correctly made a match.
- If the subject isn't in the database of images and the algorithm correctly returns nothing, it has achieved a *true reject*—it correctly found that there was no match.
- If the subject isn't in the database of images but the algorithm mistakenly suggests a match with the image of someone else, it has produced a *false accept*—it matched to the wrong person.
- If the subject is in the image database, but the algorithm fails to find a match or mistakenly suggests a match containing someone else, it has produced a *false reject*—it should have found the right person but didn't.[191]

In figuring out how to handle false accepts and rejects, a law enforcement agency has to make a difficult choice. If the goal is to identify as many leads as possible, it might prefer to be over-inclusive and err on the side of false accepts, giving more possible leads from which to choose (assuming the correct lead could eventually be identified from this set).

---

[187] *See* Federal Criminal Police Office of Germany, Federal Ministry of the Interior, *Face recognition as a search tool—foto-fahndung* at 6.
[188] *See* Federal Criminal Police Office of Germany, Federal Ministry of the Interior, *Face recognition as a search tool—foto-fahndung* at 25.
[189] Patrick J. Grother, et. al., *Multiple-Biometric Evaluation, Report on the Evaluation of 2D Still-Image Face Recognition Algorithms*, NIST Interagency Report 7709, 2, National Institute of Standards and Technology (Aug. 24, 2011), http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=905968; Patrick Grother & Mei Ngan, *Face Recognition Vendor Test: Performance of Face Identification Algorithms*, NIST Interagency Report 8009, 58 (May 26, 2014), http://biometrics.nist.gov/cs_links/face/frvt/frvt2013/NIST_8009.pdf.
[190] *See generally* Lacey Best-Rowden & Anil Jain, *A Longitudinal Study of Automatic Face Recognition*, Proc. of the IEEE International Conference on Biometrics (May 19-22, 2015), http://www.cse.msu.edu/rgroups/biometrics/Publications/Face/BestRowdenJain_LongitudinalStudyFaceRecognition_ICB15.pdf.
[191] *See* MBE 2010 at Patrick J. Grother, et. al., *Multiple-Biometric Evaluation, Report on the Evaluation of 2D Still-Image Face Recognition Algorithms*, NIST Interagency Report 7709 at 15, National Institute of Standards and Technology (Aug. 24, 2011), http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=905968.

This is the approach of the FBI face recognition database (NGI-IPS), which returns between two and 50 candidate mug shots for any given search—most of which necessarily will be false accepts.[192] Yet a false accept could be devastating to someone mistakenly implicated by face recognition. To avoid these errors, an agency might prefer false *rejects* instead, and stipulate that searches will return a small number of candidate images. Doing so, however, risks failing to find the right person at all.

2. Law enforcement agencies use too few protections for accuracy.

Most agencies that provided a face recognition use policy included some form of disclaimer stating that potential matches were investigative leads only and could not form the sole basis for arrest. Beyond this, however, agencies appear to take remarkably few steps to protect against errors in their face recognition systems.

a) Agencies do not consistently consider accuracy when purchasing systems.

The contracting process gives agencies a chance to ensure system accuracy by requiring certain accuracy thresholds, or that algorithms be submitted to accuracy tests, both before and after purchase.

Few agencies provided a full set of contracting documents in response to our records requests. Of the nine contract-related responses we did receive, four were sole source contracts, meaning that there was no competitive process for selecting or upgrading the face recognition system.[193] The other agencies providing responses demonstrated very different approaches to face recognition accuracy.

On one end of the spectrum, the Los Angeles County Sheriff's Department and Ohio Bureau of Criminal Investigation did not require any demonstration or testing for face recognition accuracy. When one company asked whether there were accuracy expectations for face and iris recognition, L.A. County responded: "There are no expectations, as we are requesting vendors to enlighten us as to [the] accuracy capability for standalone face and iris."[194] These vague standards contrast sharply with both agencies' strong accuracy requirements for fingerprint algorithms.[195]

---

[192] U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 14 (May 2016).

[193] The nine agencies that provided contract documents, including RFPs, responses to RFPs, sole source purchasing documents, and contracts, are: Maricopa County Sheriff's Office; Los Angeles County Sheriff's Department; SANDAG; San Francisco Police Department; Pinellas County Sheriff's Office; Michigan State Police; Virginia State Police; South Sound 911; and the West Virginia Intelligence Fusion Center (WVI/FC). Agencies with sole source contracts, either for the initial system purchase or for the latest system upgrade are: Maricopa County Sheriff's Office; Pinellas County Sheriff's Office; Virginia State Police; and WVI/FC.

[194] *See* Los Angeles County Sheriff's Office, *Bulletin Number 1: Questions and Responses Release, Multi-Biometric Identification System (MBIS) Request for Information Number 414-SH* (Feb. 2, 2010), Document p. 000205.

[195] Both agencies required specific accuracy rates for the systems' fingerprint algorithms, broken down by true match rates, failure to match rates, and by probe image type such as mobile searches and latent-to-criminal comparisons (analogous to the remote biometric identification application of face recognition). *See* LA County Sheriff's Office, *Request for Proposals for Multimodal Biometric Identification System*

"[W]e are requesting vendors to enlighten us as to [the] accuracy capability for standalone face and iris."

- L.A. County Contracting Bulletin

On the other end, for the face recognition component to its multi-biometric system, the San Francisco Police Department required that bidding companies:

- Meet specific target accuracy levels—an error rate of 1% or better;
- Provide copies of the results from all prior accuracy tests conducted by NIST in which their algorithm was evaluated;
- Upon acceptance, submit to verification tests to ensure the system "achieves the same or better accuracies than what has been achieved by relevant NIST and/or other independent and authoritative 3rd party testing;" and
- Submit to regular future accuracy testing "to reconfirm system performance and detect any degradation."[196]

South Sound 911 also considered accuracy in its request for face recognition proposals, requiring that: "The search results must meet a match rate of a 96% confidence rating," and "[t]he system must have high threshold facial recognition search capability for both in-car and booking officer queries."[197]

b) Few agencies used trained human reviewers to bolster accuracy.

Since face recognition accuracy remains far from perfect, experts agree that a human must double-check the results of face recognition searches to ensure that they are correct. As the architect of a leading face recognition algorithm put it, "I wouldn't like my algorithm to take someone to jail as a single source" of identifying evidence.[198]

Simple human review of results is not enough, however. Without specialized training, human reviewers make so many mistakes that overall face recognition accuracy could actually drop when their input is taken into account. Humans instinctively match faces using a number of psychological heuristics that can become liabilities for police deployments of face recognition.

(MBIS) Solution (July 2013), Document pp. 000935–000937; Ohio Bureau of Criminal Investigation, *Response to Ohio Attorney General's Office Request for Proposals No. RFP-BCI-ITS-AB01 from 3M Cogent*, Document p. 016396.

[196] *See* San Francisco Police Department, *SFPD Request for Proposal, Automated Biometric Identification System Section 02—Technical Specifications* (Mar. 31, 2009), Document pp. 005555–005558.

[197] Law Enforcement Support Agency (South Sound 911), *Request for Proposal: Mug Shot Booking Capture Solution, Specification No. 3002-12-05* (2012), Document p. 009432.

[198] *See Interview with anonymous engineer* (Mar. 9, 2016) (notes on file with authors).

For example, studies show that humans are better at recognizing people they already know[199] and people of the same race.[200]

As evidence of the benefits of training, one study tested the performance of Australian passport personnel, who use Cognitec's algorithm to check for duplicate passport applications.[201] Facial *reviewers*, who receive limited instruction in face matching, identified the correct match or correctly concluded there was no match only half the time; they did no better than college students. Specially trained facial *examiners*, however, did about 20% better.

Unfortunately, while other agencies may do this training, documents we received identified only eight systems that employed human gatekeepers to systematically review matches before forwarding them to officers: the FBI face recognition unit (FACE Services), the Albuquerque Police Department, the Honolulu Police Department, the Maricopa County Sheriff's Office, the Michigan State Police, the Palm Beach County Sheriff's Office, the Seattle Police Department, and the West Virginia Intelligence Fusion Center.[202]

Even these systems are still not ideal. For all but two of these systems—the FBI face recognition unit and the Michigan State Police—the level of training required for these human gatekeepers is unclear. Some searches evade review altogether. When a Michigan State Police

---

[199] *See* Ritchie, et al., *Viewers base estimates of face matching accuracy on their own familiarity: Explaining the photo-ID paradox*, 141 Cognition 161–169 (2015).

[200] *See* Christian Meissner & John Brigham, *Thirty Years of Investigating the Own-race Bias in Memory for Faces: A meta-analytic review*, 7 Psychology, Public Policy, and Law 3–35 (2001).

[201] *See* White, et al., *Error Rates in Users of Automatic Face Recognition Software*, PLoS ONE 10(10) (2015). The study presented the images to subjects for only 18 seconds, however, so it is possible that results might have improved if the subjects had more time. Documents from the Facial Identification Scientific Working Group suggest that "review" should take 45 sections and "examination" longer than two hours. *See* Facial Identification Scientific Working Group, *Guidelines for Facial Comparison Models, Version 1.0* (Feb. 2, 2012), https://www.fiswg.org/document/viewDocument?id=25.

[202] FBI Face Services, U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 17 (May 2016) (searches are manually reviewed and only "the top one or two" candidates are returned to the FBI agent); Albuquerque Police Department, *Procedural Order – Facial Recognition Technology*, Document p. 009203 ("When trained RTCC personnel identify a possible match, they will notify the officer or case agent and supply them with possible names and images of known offenders."); Honolulu Police Department, *Policy: Facial Recognition Program* (Sept. 14, 2015), Document p. 014705 ("If the facial recognition system detects a viable candidate, the CAU shall complete a follow-up report for the assigned detective. The CAU analyst's follow-up report shall contain the steps taken to compare the known and unknown photographs and how the CAU analyst came to his or her conclusion(s)."); Maricopa County Sheriff's Office, *MCSO/ACTIC Facial Recognition Procedures: Image Records Request*, Document p. 014963–014965 (describing a process where searches are reviewed and approved by facial recognition supervisors twice, and results are accompanied by an explanatory narrative); Michigan State Police, *Statewide Network of Agency Photos (SNAP) Unit: Overview and Workflow*, Document p. 011467–11468 (latent (investigate and identify) searches go through a team of trained examiners who narrow down candidates to a single match or none at all, which are peer reviewed by a second examiner to confirm the result.); Palm Beach County Sheriff's Office, *SOPICS Facial Recognition Program Policy*, Document p. 008651 (at least two analysts review candidate lists before the search results are returned to the requestor); Seattle Police Department, *Booking Photo Comparison Software Manual* (Feb. 19, 2014), Document p. 009907 ("Only Department-Trained Photo Personnel Will Use BPCS"); West Virginia Intelligence Fusion Center, *Letter from Thomas Kirk, General Counsel for the Office of the Secretary, West Virginia Department of Military Affairs and Public Safety, to Clare Garvie* (Jan. 25, 2016), Document p. 009911 ("When an image has been checked against the facial recognition database and results are shown, a visual check by the analyst is performed to check the probability of the match against the target image.").

officer conducts a face recognition search from a mobile phone (such as for a field identification during a traffic stop), the algorithms' results are forwarded directly to the officer without any human review.[203] Similarly, while the FBI subjects its own searches of its database to trained human review, states requesting FBI searches of that same database are returned up to 50 candidate images without any kind of human review.[204]

c) Human reviewer training regimes are still in their infancy.

Agencies that are eager to implement human training may encounter yet another difficulty: the techniques for manually comparing photos of faces for similarity—techniques that would inform this sort of training—are still in their infancy. The FBI's Facial Identification Scientific Working Group (FISWG), whose members include academic institutions and law enforcement agencies at all levels of government, has developed training and standardization materials for human facial comparison.

"It's not science at this point—it's more of an art."

Its preferred approach is "morphological comparison," which examines the similarity of different facial features depending on their "permanence." However, the science behind this approach is murky—as FISWG's materials report, "only limited studies have been done on accuracy or reproducibility."[205] An engineer at one company was more direct: "it's not science at this point—it's more of an art."[206]

3. Testing regimes are voluntary, sporadic, and resource-limited.

There is only one public, independent benchmark for comparing the accuracy of these algorithms—a face recognition competition offered by the National Institute of Standards and Technology (NIST) every three or four years. All leading manufacturers currently submit to these tests, but participation in the competition is entirely voluntary, and manufacturers are under no obligation to submit to NIST tests before selling their algorithms to law enforcement agencies.

In 2010, NIST observed that accuracy had improved by "an order of magnitude in each four-year period" between tests, a dramatic pace of technological innovation.[207] However, the last round of testing was in 2013, a lifetime ago at the pace that face recognition technology moves. Thus, state and local law enforcement agencies seeking to purchase face recognition in

---

[203] *Interview with Peter Langenfeld, Program Manager, Digital Analysis and Identification Section* (May 25, 2016) (notes on file with authors).
[204] *See* U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 14 (May 2016) ("The search of NGI-IPS is a completely automated process…").
[205] *See* Facial Identification Scientific Working Group, *Guidelines for Facial Comparison Models, Version 1.0* at 5 (Feb. 2, 2012), https://www.fiswg.org/document/viewDocuments;jsessionid=6A11990853BB99B8EBA42E6C03883543.
[206] *Personal interview with an engineer (anonymous)* (June 22, 2016) (notes on file with authors?).
[207] *See* Patrick J. Grother, et. al., *Multiple-Biometric Evaluation (MBE) 2010, Report on the Evaluation of 2D Still-Image Face Recognition Algorithms*, NIST Interagency Report 7709 at 3, National Institute of Standards and Technology (Aug. 24, 2011), http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=905968

2016 would have less reliable information to go on when contracting with face recognition vendors given the time that has passed since the last test.

4. Publicly available photo sets do not reflect the size or diversity of the human population.

Outside of NIST's accuracy tests, several publicly available, academic collections of facial photos provide a limited basis for making independent accuracy comparisons between algorithms. The most prominent of the collections is called "Labeled Faces in the Wild" and dates to 2007.[208] These datasets typically feature celebrities. This makes it easier to label thousands of individual faces, but fails to capture the full range of human diversity.

These datasets are also small, on the order of a few thousand photos. By contrast, a single state may have millions of photos in its face recognition databases. (For example, Pennsylvania has over 34 million and Michigan has over 40 million.)[209] The difference in size matters: as explained above, as a dataset grows in size, the likelihood of similar faces increases, challenging accuracy.[210]

A public dataset becomes less useful over time as researchers calibrate their design decisions to the specific photos it contains rather than to face recognition in general. As a consequence, it is common to see algorithms that perform flawlessly on one dataset but struggle in other contexts.[211] The Intelligence Advanced Research Projects Activity (IARPA), a U.S. intelligence organization that funds intelligence-related research,[212] is sponsoring an initiative called the Janus project that will generate a wave of new, more difficult datasets.[213]

SIDEBAR 6: Scoring Accuracy Protections

As this section explains, an agency can take a variety of steps to safeguard against errors into their face recognition system. Our accuracy score considers a range of different measures, with particular weight given to the use of trained human examiners as a backstop to accuracy.

- Green: Agency demonstrates **four** or **five** criteria listed below.
- Yellow: Agency demonstrates **three** of the criteria.
- Red: Agency demonstrates **two** or fewer of the criteria.

---

[208] *See* University of Massachusetts — Amherst, *Labeled Faces in the Wild*, http://vis-www.cs.umass.edu/lfw/ (last visited Sept. 22, 2016).
[209] Pennsylvania JNET, *JNET Facial Recognition Presentation Slides* (2014), Document p. 010750; Michigan State Police, *Interview with Peter Langenfeld, Program Manager, Digital Analysis and Identification Section* (May 25, 2016) (notes on file with authors).
[210] *See above* Section 1: Accuracy remains a work in progress. Real-time systems and systems with large databases are especially error-prone.
[211] Brendan F. Klare et al., *Pushing the Frontiers of Unconstrained Face Detection and Recognition: IARPA Janus Benchmark A*, 28 IEEE Conference on Computer Vision and Pattern Recognition 1 (June 2015) (" . . . performance has begun to saturate on LFW, YTW, and other unconstrained datasets. At the same time, unconstrained face recognition is hardly considered a solved problem.").
[212] Office of the Director of National Intelligence, https://www.iarpa.gov/ (last visited Sept. 22, 2016).
[213] Brendan F. Klare et al., *Pushing the Frontiers of Unconstrained Face Detection and Recognition: IARPA Janus Benchmark A*, 28 IEEE Conference on Computer Vision and Pattern Recognition (June 2015); Office of the Director of National Intelligence, *Janus*, https://www.iarpa.gov/index.php/research-programs/janus/baa?highlight=WyJqYW51cyJd (last visited Sept. 22, 2016).

- The criteria are:
    - Algorithms have been tested by the National Institute of Standards and Technology;
    - Contract with vendor company contains provisions that require face recognition algorithms to have been tested for accuracy and will be tested at all future opportunities;
    - Most or all face recognition queries are validated by trained human examiners or agencies have a unit or designated personnel that perform a review and screening function of the candidate lists (weighted as two criteria);
    - Face recognition results or candidate lists are treated as investigative leads only.

E. RACIAL BIAS

"Q: Is the Booking Photo Comparison System biased against minorities[?]"

"A: No… it does not see race, sex, orientation or age. The software is matching distance and patterns only, not skin color, age or sex of an individual."

- Frequently Asked Questions, Seattle Police Department

Human vision is biased: We are good at identifying members of our own race or ethnicity, and by comparison, bad at identifying almost everyone else.[214] Yet many agencies using face recognition believe that machine vision is immune to human bias. In the words of one Washington police department, face recognition simply "does not see race."[215]

The reality is far more complicated. Studies of racial bias in face recognition algorithms are few and far between. The research that has been done, however, suggests that these

[214] *See, e.g.*, Gustave A. Feingold, *The Influence of Environment on Identification of Persons and Things*, 5 *J. of the Am. Inst. of Crim. L. & Criminology* 39, 50 (May 1914-March 1915) ("Now it is well known that, other things being equal, individuals of a given race are distinguishable from each other in proportion to our familiarity, to our contact with the race as a whole."); Luca Vizioli, Guillaume A. Rousselet, Roberto Caldara, *Neural Repetition Suppression to Identity is Abolished by Other-Race Faces*, 107 Proc. of the Nat'l Acad. of Sci. of the U.S., 20081, 20081 (2010), http://www.pnas.org/content/107/46/20081.abstract. This problem is known as the "other-race" effect. *Id*. Humans are more accurate at identifying people they know. See supra note TK.

[215] *See* Seattle Police Department, *Booking Photo Comparison System FAQs*, Document p. 009377. 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, http://www.tampabay.com/news/publicsafety/crime/facial-recognition-technology-proving-effective-for-pinellas-deputies/1019492.

systems do, in fact, show signs of bias. The most prominent 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.[216] In interviews, we were surprised to find that two major face recognition companies did not test their algorithms for racial bias.[217]

Racial bias intrinsic to an algorithm may be compounded by outside factors. African Americans are disproportionately likely to come into contact with—and be arrested by—law enforcement.[218] This means that police face recognition may be overused on the segment of the population on which it underperforms. It also means that African Americans will likely be overrepresented in mug shot-based face recognition databases. Finally, when algorithms search these databases, the task of selecting a final match is often left to humans, even though this may only add human bias back into the system.

1. Face recognition algorithms exhibit racial bias.

Despite the lack of extensive public and independent testing, several studies have uncovered racial bias in face recognition algorithms. In 2011, researchers used the algorithms and images from a 2006 NIST competition to compare accuracy on subjects of East Asian and Caucasian descent.[219] They found that algorithms developed in East Asia performed better on East Asians, while algorithms developed in Western Europe and the U.S. performed better on Caucasians. This result suggests that algorithms may be most accurate on the populations who developed them—a concerning effect given that software engineers in the United States are predominately Caucasian males.[220]

The 2012 FBI-coauthored study tested three commercial algorithms on mug shots from Pinellas County, Florida.[221] The companies tested include the suppliers of algorithms to the Los Angeles County Sheriff, the Maryland Department of Public Safety, the Michigan State Police, the Pennsylvania Justice Network, and the San Diego Association of Governments (SANDAG), which runs a system used by 28 law enforcement agencies within San Diego County.[222]

All three of the algorithms were 5 to 10% less accurate on African Americans than Caucasians. To be more precise, African Americans were less likely to be successfully identified

---

[216] *See* Brendan F. Klare et al., *Face Recognition Performance: Role of Demographic Information*, 7 *IEEE Transactions on Information Forensics and Security* 1789, 1797 (2012) (hereinafter "Klare et al.").
[217] *See Interview with Face Recognition Company* (Mar. 3, 2016) (notes on file with authors); *Interview with Face Recognition Company* (Mar. 16, 2016) (notes on file with authors).
[218] *See, e.g.*, Brad Heath, *Racial Gap in U.S. Arrest Rates: 'Staggering Disparity'*, USA Today, Nov. 19, 2014, http://www.usatoday.com/story/news/nation/2014/11/18/ferguson-black-arrest-rates/19043207.
[219] *See* P. Jonathon Phillips et al., *An Other-Race Effect for Face Recognition Algorithms*, 8 ACM Transactions on Applied Perception 14:1, 14:5 (2011).
[220] *See*, *e.g.*, Google Diversity, *Our Workforce: Tech*, https://www.google.com/diversity/ (last visited Sept. 22, 2016) (showing the 2015 tech workforce to be 81% male and 57% white); Maxine Williams, *Facebook Diversity Update: Positive Hiring Trends Show Progress,* Facebook (July 14, 2016), http://newsroom.fb.com/news/2016/07/facebook-diversity-update-positive-hiring-trends-show-progress/ (showing that the tech workforce is currently 83% male and 48% white—a plurality).
[221] *See* Klare et al., *above* note TK, at 1789.
[222] As of Feb. 13, 2015, there were approximately 800 registered users of TACIDS from 28 law enforcement agencies in the San Diego area. SANDAG, *Board of Directors Agenda Item 2* (Feb. 13, 2015), Document p. 005699.

—i.e., more likely to be falsely rejected—than other demographic groups.[223] A similar decline surfaced for females as compared to males[224] and younger subjects as compared to older subjects.[225]

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. To put this in more concrete terms, if the perpetrator of the 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 lead the police to misidentify the perpetrator and investigate the wrong person. Many systems, including the FBI's, return the top few matches for a given probe photo no matter how bad the matches themselves are. If the photo's subject is African American and the system erroneously fails to identify the right person, innocent people are more likely to be bumped up the list—and potentially investigated. Even if the perpetrator is simply knocked a few spots lower on the list, it means that, according to the facial recognition system, innocent people will look like better matches.

5–10%
Lower accuracy rates for African Americans and women, as measured in an FBI co-authored 2012 study.

There are various explanations for this bias. The simplest is that training is destiny; the faces that an algorithm practices on are the faces it will be best at recognizing. When those

---

[223] *See* Klare et al., *above* note TK, at 1797. A few studies have contradicted this result. G. H. Givens et al., *How Features of the Human Face Affect Recognition: A statistical comparison of three face recognition algorithm,* Computer Vision and Pattern Recognition (2004) found that African American and Asian subjects were easier to recognize, but did so using primitive academic algorithms that are a decade older than those from the 2012 study. They were trained and tested on images collected for the FERET dataset in 1993-96. Patrick J. Grother, et al., *Multiple-Biometric Evaluation (MBE) 2010, Report on the Evaluation of 2D Still-Image Face Recognition Algorithms*, NIST Interagency Report 7709 at 55-56, National Institute of Standards and Technology (Aug. 24, 2011), http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=905968 also found that "blacks were easier to recognize than whites for 5 of the 6 algorithms" tested in the study, three of which were the same commercial algorithms as those tested by Klare et al. However, the MBE 2010 study provides only a single graph and a paragraph of analysis to support this finding. We rely on the analysis by Klare et al., which was more systematic, comprehensive, and thorough in the way it presented its findings.

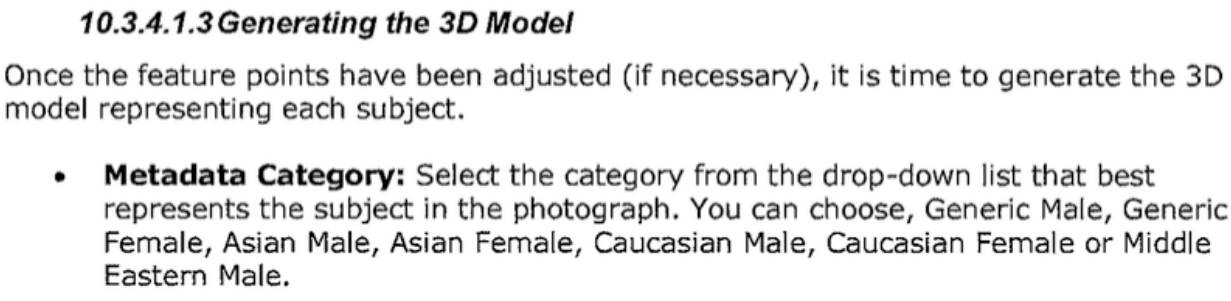
[224] *See* Klare et al., *above* note TK, at 1797. This finding is also supported by P. Jonathon Phillips, et al., *Face Recognition Vendor Test 2002: Evaluation Report* (Mar. 2003) at 26–28, http://www.face-rec.org/vendors/FRVT_2002_Evaluation_Report.pdf and Patrick J. Grother, et al., *Multiple-Biometric Evaluation (MBE) 2010, Report on the Evaluation of 2D Still-Image Face Recognition Algorithms*, NIST Interagency Report 7709 at 51, National Institute of Standards and Technology (Aug. 24, 2011), http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=905968.

[225] *See* Klare et al., *Face Recognition Performance: Role of Demographic Information*, 7 I*EEE Transactions on Information Forensics and Security* 1790, 1798 (2012). This finding is also supported by Phillips, et. al., *Face Recognition Vendor Test 2002: Evaluation Report* (Mar. 2003) at 29, http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50767. This result is contradicted by Patrick J. Grother, et. al., *Multiple-Biometric Evaluation, Report on the Evaluation of 2D Stll-Image Face Recognition Algorithms*, NIST Interagency Report 7709 at 51-52, National Institute of Standards and Technology (Aug. 24, 2011), http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=905968 which found no prevailing effect.

faces disproportionately represent one race, an algorithm will optimize its accuracy for that group at the expense of others. Notably, in addition to testing three commercial algorithms, the 2012 study also tested an academic algorithm that was trained three separate times exclusively on Caucasians, African Americans, and Latinos; it consistently performed best on the race on which it was trained.[226]

The authors of the 2012 study suggest another contributing factor: Some demographics may be inherently more difficult to recognize than others. For example, they hypothesize that cosmetics could make it harder to match photos of women.[227] In interviews, several experts noted that individuals with darker skin tones are more difficult to identify because face recognition relies on color contrast to characterize facial features.[228]

Finally, bias may be the inadvertent result of intentional design decisions. Engineers designing an algorithm may purposefully design it to perform on certain demographics, potentially at the expense of others.



10.3.4.1.3 Generating the 3D Model

Once the feature points have been adjusted (if necessary), it is time to generate the 3D model representing each subject.

- **Metadata Category:** Select the category from the drop-down list that best represents the subject in the photograph. You can choose, Generic Male, Generic Female, Asian Male, Asian Female, Caucasian Male, Caucasian Female or Middle Eastern Male.

Figure TK. Pennsylvania Justice Network, "JNET Facial Recognition User Guide Version 1.8" (Dec. 4, 2014)

As an example of a design choice that may result in bias, a 2014 handbook for users of the Pennsylvania Justice Network (JNET) face recognition system instructs users on how to generate a three-dimensional model of a face by using software from a company called Animetrics. In order to generate the model, users are instructed to enter the race or ethnicity of the subject. But as described in the handbook, the JNET system's only options are "Generic Male, Generic Female, Asian Male, Asian Female, Caucasian Male, Caucasian Female or Middle Eastern Male."[229] As of 2015, African Americans and Latinos comprised 11.7% and 6.8% of Pennsylvanians, respectively.[230] While this is only one of many tools used in Pennsylvania's face recognition software suite, it excludes a significant portion of the state's population—and, potentially, the communities most likely to encounter law enforcement.

---

[226] *See* Klare et al., *Face Recognition Performance: Role of Demographic Information*, 7 I*EEE Transactions on Information Forensics and Security* 1790, 1800 (2012) ("Face recognition performance on race/ethnicity…generally improves when training exclusively on that same cohort.").

[227] *See* Klare et al., *Face Recognition Performance: Role of Demographic Information*, 7 I*EEE Transactions on Information Forensics and Security* 1790, 1797 (2012) ("These results strongly suggest that the female cohort is inherently more difficult to recognize.")

[228] *Interview with anonymous company engineer* (Mar. 9, 2016) ("when you have people with very dark skin, you have a lower dynamic range, which means that it's much harder to capture high-quality images. . . This is one reason why the performance on black subjects has typically been worse") (notes on file with authors).

[229] *See* Pennsylvania JNET, *JNET Facial Recognition User Guide Version 1.8* (Dec. 4, 2014), Document p. 010879–010883.

[230] *See* U.S. Census, *Quick Facts: Pennsylvania*, http://www.census.gov/quickfacts/table/PST045215/42#headnote-js-b (last accessed July 24, 2016).

2. Face recognition algorithms are not being tested for racial bias.

The scientific literature on racial bias of face recognition is sparse. The two studies discussed in this section represent some of the only lines of work to investigate this phenomenon. NIST, which has run a face recognition competition every three to four years since the mid-1990s, has tested for racial bias just once.[231] The problem may be related to demand: Even jurisdictions like the San Francisco Police Department—which required prospective face recognition vendors to demonstrate a target accuracy levels, provide documentation of performance on all applicable accuracy tests, and submit to regular future accuracy tests—did not ask companies to test for racially biased error rates.[232]

This state of affairs is not limited to the government or academia. In the spring of 2016, we conducted interviews with two of the nation's leading face recognition vendors for law enforcement to ask them how they identify and seek to correct racially disparate error rates. At that time, engineers at neither company could point to tests that explicitly checked for racial bias. Instead, they explained that they use diverse training data and assume that this produces unbiased algorithms.[233]

Engineers at two of the nation's leading face recognition companies indicated that they did not explicitly test their systems for racial bias.

This problem may trace, in part, to a lack of diverse photo datasets that could be used to test for racially biased errors. The 2011 study, for example, was likely tested only on Caucasians and East Asians because its database was composed of photos of undergraduate volunteers who were 77% Caucasian, 14% Asian, and 9% "other or unknown."[234] Likewise, the 2012 study also tested the algorithms on Hispanics, but the results were erratic due to "the insufficient number of training samples available."[235] This situation is the norm in face recognition—diverse collections of photos that accurately capture communities of interest to law enforcement are in short supply. This deficiency reduces the reliability of testing regimes for existing systems and makes it more difficult to train new algorithms.

3. African Americans are disproportionately likely to be subject to police face recognition.

---

[231] See Patrick J. Grother, et. al., *Multiple-Biometric Evaluation, Report on the Evaluation of 2D Stll-Image Face Recognition Algorithms*, NIST Interagency Report 7709, National Institute of Standards and Technology 55-56 (Aug. 24, 2011), http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=905968.
[232] San Francisco Police Department, *Request for Proposal—Automated Biometric Identification System, Section 02: Technical Specifications* (Mar. 31, 2009), Document pp. 005555–005557.
[233] *Interview with anonymous engineer* (Mar. 9, 2016) (notes on file with authors); *Interview with anonymous engineer* (Mar. 16, 2016) (notes on file with authors). In order to obtain candid responses, we assured employees at these companies that their answers would be reported anonymously. A third company declined to be interviewed without a non-disclosure agreement that would prohibit publication of their responses.
[234] Flynn et al., *Lessons from Collecting a Million Biometric Samples*, University of Notre Dame/National Institute of Standards and Technology, https://www3.nd.edu/~kwb/Flynn_Phillips_Bowyer_FG_2015.pdf.
[235] *See* Klare et al., *Face Recognition Performance: Role of Demographic Information*, 7 I*EEE Transactions on Information Forensics and Security* 1790, 1798.

A face recognition system can only "find" people who are in its database; in systems that rely on mug shot databases, racial disparities in arrest rates will make African Americans much more "findable" than others—even though those identifications may themselves be more likely to be erroneous.

Ratio of African American arrest rates to population share in select jurisdictions

3:1	2:1	3:1	2:1
Arizona	Hawaii	L.A. County	Michigan
5:1	**3:1**	**3:1**	**2:1**
Minnesota	Pennsylvania	San Diego County	Virginia

Sources: U.S. Census, Minnesota Department of Public Safety, King County Department of Adult and Juvenile Detention, Pennsylvania Uniform Crime Reporting System, State of California Department of Justice Office of the Attorney General, Virginia State Police, Arizona Department of Public Safety[236]

[236] All arrest ratios have been rounded to the nearest whole number. Arizona Department of Public Safety, Crime in Arizona (2014), http://www.azdps.gov/about/reports/docs/crime_in_arizona_report_2014.pdf (11.34% of adult arrests were of African Americans in Arizona); U.S. Census Bureau, *2010-2014 American Community Survey 5-Year Estimates Arizona*, https://factfinder.census.gov/bkmk/table/1.0/en/ACS/14_5YR/DP05/0400000US04 (African Americans comprised 4.2% of the population of Arizona); California Department of Justice, Office of the Attorney General, *CJSC Statistics: Arrests*, https://oag.ca.gov/crime/cjsc/stats/arrests (last visited Sept. 22, 2016) (22.94% of arrests in Los Angeles were of African Americans); U.S. Census Bureau, *2010-2014 American Community Survey 5-Year Estimates Los Angeles*, https://factfinder.census.gov/bkmk/table/1.0/en/ACS/14_5YR/DP05/0500000US06037 (African Americans comprised 8.34% of the population of Los Angeles); Minnesota Department of Public Safety, *Uniform Crime Report* (2014), https://dps.mn.gov/divisions/bca/bca-divisions/mnjis/Documents/2014-MN-Crime-Book.pdf (24.50% of arrests were of African Americans in Minnesota); U.S. Census Bureau, *2010-2014 American Community Survey 5-Year Estimates Minnesota*, https://factfinder.census.gov/bkmk/table/1.0/en/ACS/14_5YR/DP05/0400000US277 (African Americans comprised 5.4% of the population of Minnesota); Pennsylvania Uniform Crime Reporting System, Crime in Pennsylvania: Annual Uniform Crime Report (2014), http://www.paucrs.pa.gov/UCR/Reporting/Annual/AnnualFrames.asp?year=2014 (31.8% of arrests in Pennsylvania were of African Americans); U.S. Census Bureau, *2010-2014 American Community Survey 5-Year Estimates Pennsylvania*, https://factfinder.census.gov/bkmk/table/1.0/en/ACS/14_5YR/DP05/0400000US42 (African Americans comprised 10.4% of the population of Pennsylvania); California Department of Justice, Office of the Attorney General, *CJSC Statistics: Arrests*, https://oag.ca.gov/crime/cjsc/stats/arrests (last visited Sept. 22, 2016) (15.12% of those arrested in San Diego County were of African Americans), U.S. Census Bureau, 2010-2014 American Community Survey 5-Year Estimates San Diego County, https://factfinder.census.gov/bkmk/table/1.0/en/ACS/14_5YR/DP05/0500000US06073 (African Americans comprised 5.0% of the population of San Diego County); Uniform Crime Reporting Section, Department of State Police, Crime in Virginia (2014), http://www.vsp.state.va.us/downloads/Crime_in_Virginia/Crime_in_Virginia_2014.pdf (44.73% of those arrested in Virginia were African American); U.S. Census Bureau, 2010-2014 American Community Survey 5-Year Estimates Virginia,

Many agencies that reported using mug shot databases (alone or in conjunction with driver's license and ID photos) experience dramatic racial disparities in arrest rates. For example, in 2014, African Americans represented 5.4% of Minnesota's population but 24.50% of those arrested. In contrast, Caucasians were 82.1% of the population but 57.0% of those arrested.[237] A Center on Juvenile and Criminal Justice fact sheet notes that "African American women, 5.8 percent of San Francisco's total female population, constituted 45.5 percent of all female arrests in 2013."[238]

These statistics do not just speak to arrests. They reflect the fact that African Americans are not just more likely to be arrested: they are also more likely to be stopped, interrogated, or otherwise investigated by law enforcement. Police face recognition systems do not only perform worse on African Americans; African Americans also more likely to be enrolled in those systems *and* be subject to their processing.

A natural response to the enrollment problem might be to move away from mug shot databases and instead use driver's license and ID photo databases, which may better reflect the overall population in a jurisdiction. As this report explains, however, this results in the creation of a dragnet biometric database of law-abiding citizens—a shift that is unprecedented in the history of federal law enforcement and raises profound privacy issues. Face recognition presents some problems for which there are no easy answers.

SIDEBAR 7: Scoring Protections Against Racial Bias

There was too little information available to score individual agencies on their efforts to combat racial bias in their face recognition system. The main factor in this decision was the absence of regular accuracy tests for racially biased error rates. (Many jurisdictions also failed to disaggregate arrest rates along the lines of race and ethnicity.) If NIST institutes regular accuracy tests for racial bias, however, police departments and the communities they serve should condition system purchases on an algorithm's performance in bias tests.

F. TRANSPARENCY & ACCOUNTABILITY

In 2014, Victor Manuel Torres, a civil rights attorney in San Diego, began receiving complaints—about one a day over the course of a few months. Each caller had been stopped by the police for a different reason, but after that each story was the same: Sometime during questioning, the officer had pulled out a tablet and taken their photo, without asking for consent or providing an explanation. The callers were indignant and confused. Why would the police need my photo? How were they going to use it? Was this even legal?[239]

---

https://factfinder.census.gov/bkmk/table/1.0/en/ACS/14_5YR/DP05/0400000US51 (African Americans comprised 19.3% of the population of Virginia).

[237] Minnesota Department of Public Safety, *Uniform Crime Report* (2014), https://dps.mn.gov/divisions/bca/bca-divisions/mnjis/Documents/2014-MN-Crime-Book.pdf (24.50% of arrests were of African Americans in Minnesota); U.S. Census Bureau, *2010-2014 American Community Survey 5-Year Estimates Minnesota*, https://factfinder.census.gov/bkmk/table/1.0/en/ACS/14_5YR/DP05/0400000US277 (African Americans comprised 5.4% of the population of Minnesota).

[238] Michael Males, *San Francisco's Disproportionate Arrest of African American Women Persists* (Apr. 2015) at 1, http://www.cjcj.org/uploads/cjcj/documents/disproportionate_arrests_in_san_francisco.pdf.

[239] *Interview with Victor Manuel Torres, San Diego Criminal Attorney* (Mar. 8, 2016) (notes on file with authors).

Police in San Diego County, California, began using face recognition to identify subjects in the field in 2012. Two years later, there were over 800 officers using the mobile systems from 28 different law enforcement agencies in the region.[240] Yet it wasn't until three years after it was deployed, in April 2015, that a face recognition use policy was put in place. Once that policy was made public, Torres noted, the complaints virtually stopped.

What's unusual about the San Diego case is not the police's use of face recognition without consent or notice—it's that a use policy was eventually approved by an advisory board and then made available to the public.

Most law enforcement agencies have deployed face recognition with minimum levels of transparency and internal accountability. Four of the 52 responsive agencies—or less than 8%—have a face recognition use policy that is publicly available. For 24 jurisdictions that use or formerly used face recognition, no use policy whatsoever was provided in response to our survey. Just one jurisdiction received legislative approval for their policy, and one policy received formal review by an outside privacy or civil liberties organization. Compounding this lack of oversight, almost none of the jurisdictions we surveyed—including the FBI—have a functional internal audit regime to prevent misuse or document when it occurs.

1. Law enforcement agencies are not transparent about using face recognition.

Police departments generally tell the public very little about their use of face recognition. When the existence of these systems comes to light, it is often due to the work of investigative journalists and privacy organizations.

The agencies with the most advanced face recognition systems are often the least transparent.

Ohio's face recognition system remained almost entirely unknown to the public for five years—until an investigation conducted by the Cincinnati Enquirer uncovered that the Ohio's Bureau of Criminal Investigation had enrolled all Ohio state driver's license photos in the system two months prior, with no notice provided to current or future license holders.[241] The Sheriff's Department in Hennepin County, Minnesota, acquired face recognition in 2013. Yet it only released information about its system in 2016 after a court ordered it to disclose that information to an investigative journalist.[242]

Some of the largest law enforcement agencies—and those who may have the most advanced face recognition systems—are the least transparent. The New York Police Department's use of face recognition has been described in numerous news articles; NYPD spokespersons admit that it exists.[243] Yet the NYPD denied our records request entirely, arguing

[240] SANDAG, *SANDAG Public Safety Committee Agenda* (Dec. 12, 2014), Document p. 008309.
[241] Chrissie Thompson, *Ohio residents not told how license photos used*, Cincinnati Enquirer (Aug. 26, 2013); Chrissie Thompson, *A year later, how secure is Ohio's facial ID system?* Cincinnati Enquirer (Aug. 15, 2014), http://www.cincinnati.com/story/news/politics/2014/08/14/ohio-facial-recognition/14090601/.
[242] Tony Webster, *Hennepin County Sheriff circumvents state to expand facial recognition database*, Tonywebster.com (Jun. 3, 2016), https://tonywebster.com/2016/06/hennepin-sheriff-facial-recognition/.
[243] *See, e.g.*, Pei-Sze-Cheng, *I-Team: Use of Facial Recognition Technology Expands as Some Question Whether Rules are Keeping Up*, NBC New York (Jun. 23, 2015),

that the responsive records fall under the "non-routine techniques and procedures" exemption in New York's Freedom of Information Law.[244] The Chicago Police Department provided responsive records to a small fraction of our request. These documents suggested that the department had purchased of a large-scale system in 2009, but provided no information about how such a system is used or what policies are in place governing such use, except that such policies were to be developed in the future.[245]

The Los Angeles Police Department is the only American police department to openly claim to use real-time, continuous face recognition. Curiously, the LAPD found "no records responsive to [our] request"[246] for information about this or any other face recognition system, despite ten years' of LAPD news releases and annual reports that document at least three separate police face recognition initiatives.[247]

Unfortunately, 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.[248] The Pinellas County Sheriff's Office system has been operational for almost 15 years. The Pinellas County Public Defender, Bob Dillinger, reports that in that time, his office has never received any face recognition information as part of a *Brady* disclosure.[249] In an interview, he suggested that if the PCSO face recognition system ever identifies someone other than a criminal defendant as a potential suspect in that defendant's case, public defenders have a right to know.[250]

---

http://www.nbcnewyork.com/news/local/Facial-Recognition-NYPD-Technology-Video-Camera-Police-Arrest-Surveillance-309359581.html; Peter B. Counter, *Government Use of Facial Recognition Deepens in New York*, FindBiometrics (Jun. 24, 2015), http://findbiometrics.com/government-use-of-facial-recognition-new-york-26244/; New York Post, *NYPD uses high-tech facial-recognition software to nab barbershop shooting suspect* (Mar. 16, 2012), http://nypost.com/2012/03/16/nypd-uses-high-tech-facial-recognition-software-to-nab-barbershop-shooting-suspect/.

[244] New York City Police Department, *Letter from Records Access Officer Lieutenant Richard Mantellino to Clare Garvie* (Mar. 30, 2016), Document p. 016726 (letter denying New York State Freedom of Information Law Request # 2016-PL-337, denial appealed and determination pending as of September 2016).

[245] Chicago Police Department, *Letter from Chicago Police Department Freedom of Information Officer K. Tierny to Djana Martin* (Sept. 29, 2015), Document p. 008726, 008729, and 008686.

[246] Los Angeles Police Department, *Letter from Senior Management Analyst Martin Bland to Clare Garvie* (Feb. 25, 2016), Document p. 000102; *Phone messages and conversations between Mary Taylor, Management Analyst, Discovery Section and Clare Garvie* (Feb. 17, Mar. 22, and April 34, 2016) (notes on file with authors).

[247] West Valley Community Police Station, *Surveillance Cameras in West San Fernando Valley*, West Valley Police (Jan. 1, 2013), http://www.westvalleypolice.org/index_news_20130120.html; Office of the Chief of Police, Los Angeles Police Department, LIII The Beat 10 (Oct. 2007), http://assets.lapdonline.org/assets/pdf/october_07_beat_9%20-%20OK.pdf (detailing deployment of prototype Smart Car with face recognition software); Los Angeles Police Department, *LAPD Uses New Technologies to Fight Crime* (Feb. 1, 2005), http://www.lapdonline.org/february_2005/news_view/19849 (describing face recognition as "major technological innovation" of Rampart Division of LAPD, contributing to 19 arrests).

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

[249] *Email from Bob Dillinger, Pinellas County Public Defender, to Clare Garvie* (Aug. 8, 2016) (on file with authors).

[250] *Interview with Public Defender Bob Dillinger* (July 27, 2016) (notes on file with authors).

2. Agencies are even less transparent about how—or how frequently—they use face recognition.

While a limited number of agencies inform the public about the existence of face recognition, even fewer disclose how officers use it. 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.[251] We are also aware of just one agency that regularly reports to the public how frequently face recognition is used.[252]

The FBI, for its part, has consistently failed to comply with the transparency requirements of the E-Government Act and the Privacy Act, which 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 Next Generation Identification system.[253] 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 this year.[254]

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, 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.[255]

---

[251] ARJIS Facial Recognition Acceptable Use Policy, http://www.arjis.org/SitePages/Policies.aspx (last visited Sept. 22, 2016); Honolulu Police Department, *Policy: Facial Recognition Program*, http://honolulupd.org/information/index.php?page=viewPolicies (last visited Sept. 22, 2016); Michigan State Police*, SNAP Acceptable Use Policy*, http://www.michigan.gov/msp/0,4643,7-123-72297_64747_64749-357133--,00.html (last visited Sept. 23, 2016); Seattle Police Department, *Manual: Booking Photo Comparison Software*, http://www.seattle.gov/police-manual/title-12---department-information-systems/12045---booking-photo-comparison-software (last visited Sept. 23, 2016).

[252] Upon request and on an annual basis, SANDAG holds open Public Safety Committee meetings during which member agencies provide information about the use of face recognition pursuant to the requirements provided in SANDAG's Face Recognition Acceptable Use Policy. *See* SANDAG, *ARJIS Acceptable Use Policy for Facial Recognition* (Feb. 13, 2015), Document p. 008453.

[253] *See* S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 21–22 (May 2016), *See* S. Gov't Accountability Office, GAO/AIMD-00-21.3.1, Standards for Internal Control in the Federal Government 13 (Nov. 1999); 44 U.S.C. § 101; 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).

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

[255] *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=DOJ-OPCL-2016-0008-0114 (explaining impact of proposed exemption of FBI's NGI System from key Privacy Act accountability provisions).

3. Police policies are not subject to legislative or public review.

Very few agencies require or obtain legislative approval of a police face recognition use policy, or mandate review of that policy by privacy and civil liberties organizations.

Of the 52 responsive agencies, only SANDAG appears to have a system in place where elected officials review and approve the agency's face recognition use policy.[256] The Acceptable Use Policy for face recognition requires annual review by SANDAG's Board of Directors, which is mostly comprised of local elected officials. SANDAG's Board of Directors meetings are also open to the public.[257]

We found only one agency that submits its face recognition use policy for legislative approval.

The Seattle regional system appears to be the only one with a policy formally reviewed by an outside organization. The Seattle City Council approved funds for the program on condition that the ACLU of Washington was consulted on and approved the final policy.[258] The Michigan State Police also initiated informal review of their face recognition use policy by a state legislator and a contact at the ACLU.[259] No other jurisdiction we surveyed had any formal or informal external mechanism in place for review or approval of their system's use policy, either by the legislature or privacy and civil liberties organizations.

4. Few agencies have robust internal audits to prevent misuse.

Few police departments seem to have implemented robust internal accountability measures. Many agencies, including the Maricopa County Sheriff's Office, the Carlsbad Police Department, the Maryland Department of Public Safety, and the Albuquerque Police Department expressly stated that they had not audited face recognition use.[260] Only nine of the

---

[256] SANDAG, *Automated Regional Justice Information System (ARJIS) Acceptable Use Policy for Facial Recognition,* (Feb. 13, 2015), Document p. 008453 ("The Acceptable Use Policy for Facial Recognition will be brought to the SANDAG Public Safety Committee and the SANDAG Board of Directors at least once per year for review and determination regarding the need for amendments."); The SANDAG Board of Directors "is composed of mayors, councilmembers, and a county supervisor from each of the region's 19 local governments." SANDAG, Board of Directors, http://www.sandag.org/index.asp?committeeid=31&fuseaction=committees.detail (last visited Sept. 22, 2016).

[257] SANDAG, *Board of Directors Agenda,* (Feb. 13, 2015) Document p. 005696 ("Members of the public may speak to the Board of Directors on any item at the time the Board is considering the item.")

[258] South Sound 911, *Interview with Staff Attorney Peter Beckwith and Facial Recognition Technology Program Manager Matt Johnson*, (Feb. 9, 2016), Document p. 011899; *Interview with Doug Klunder, ACLU Privacy Counsel* (May 6, 2016) (notes on file with authors) Document p. 012666. The ACLU provided extensive review and feedback over the course of a year prior to the adoption of the policy. Note however that it is not clear whether this was a written requirement; if the system were to be changed or enhanced in the future, it would not necessarily receive the same scrutiny.

[259] Michigan State Police, *Interview with Peter Langenfeld, Program Manager, Digital Analysis and Identification Section*, (March 23, 2016) Document p. 010928. We reached out to the ACLU of Michigan for more information on this process and they could not corroborate this consultation.

[260] Maricopa County Sheriff's Office, *Letter to requestor*, Document p. 014949; Carlsbad Police Department, *Letter to requestor*, Document p. 000149 (note that SANDAG states that it conducts audits, but also places the responsibility on agencies accessing face recognition to conduct their own audits as well. SANDAG, *Automated Regional Justice Information System (ARJIS) Acceptable Use Policy for*

52 responsive agencies (17%), plus the FBI face recognition unit (FACE Services), expressly indicated that they audit their employees' use of the face recognition system for improper use.[261]

Of these 10 regimes, however, some are non-operational. The Pinellas County Sheriff's Office, for example, does not audit system use—despite policies that suggest otherwise. The Standard Operating Procedure for mobile biometrics states that "[a]ll [mobile] biometric and search activity are logged and subject to audit."[262] The Palm Beach County Sheriff's Office, an agency that uses the Pinellas County system, also said that audits are "done by Pinellas."[263] Nonetheless, Sheriff Gualtieri acknowledged in an interview that internal audits are not conducted. "We don't police our users," he said.[264] The Pinellas County face recognition system—which appears to be the most frequently used face recognition system in the country—may therefore lack any internal oversight or accountability mechanism to protect against, or even to detect, misuse.

Only one responsive agency—the Michigan State Police—actually provided evidence of routine audits in response to our request for such records.[265]

SIDEBAR 8: Scoring Transparency & Accountability Protections

We developed one score focused on public transparency and oversight by legislatures or privacy and civil liberties groups (Public Transparency), and another focused on internal oversight measures (Internal Audits). The Public Transparency score was based on information provided in response to document requests and publicly available records, whereas the Accountability score was based on documents provided by agencies.

- **Public Transparency.** Has the agency publicly posted its face recognition use policy, and has it been reviewed or approved by a legislature or privacy and civil liberties groups?
    - Green: Agency has a public face recognition use policy that has been reviewed or approved by a legislature and/or privacy and civil liberties groups.

Facial Recognition, (Feb. 13, 2015) Document p. 008452 ("Identifying and addressing intentional misconduct is the responsibility of the individual agency."); Maryland DPSCS, *Response to requestor*, Document p. 008906; Albuquerque Police Department, *Letter to requestor*, Document p. 009204 ("Does not exist" in response to the request for audits of the FRT system).

[261] These agencies include: FBI FACE Services, *PIA for FACE Services Unit* (May 1, 2015), https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/facial-analysis-comparison-and-evaluation-face-services-unit; Pinellas County Sheriff's Office, *Mobile Biometric Usage*, Document p. 014375; Iowa Department of Public Safety, *Letter from Public Information Officer Alex Murphy to Clare Garvie*, (Jan. 29, 2016), Document p. 008658; Michigan State Police, *SNAP Acceptable Use Policy*, Document p. 011439; Pennsylvania JNET, *End User Agreement*, Document p. 010945; SANDAG, *ARJIS Facial Recognition Acceptable Use Policy*, Document p. 008452; Seattle Police Department, *BPCS Manual*, Document p. 009909; West Virginia Intelligence Fusion Center, *General WVI/FC Privacy Policy*, Document p. 009939.

[262] *See* PCSO, *General Order 12-14: Sheriff's Office Biometric Identification Program*, Document p. 013982; PCSO, *Standard Operating Procedure POB 52: Mobile Biometric Usage*, Document p. 014375.

[263] Palm Beach Sheriff's Office, *Interview with Fusion Center Director Scott Nugent* (Jan. 15, 2016), Document p. 008649.

[264] *Interview with Sheriff Bob Gualtieri and Technical Support Specialist Jake Ruberto* (July 26, 2016) (notes on file with authors).

[265] Michigan State Police, *Various audit records*, Document pp. 011107–011145.

  - Yellow: Agency has a public use policy, but there is no evidence that the policy received external review or approval.
  - Red: Agency has not made its use policy public, or has no use policy.

- **Internal Audits.** Does the agency monitor and conduct audits of face recognition use by its officers and other accessing agencies? (Since our records request specifically asked for records pertaining to audits, when an agency did not provide audit records or sample audit forms and did not deny this request, it was assumed that no audits were conducted.)

  - Green: Formal audit procedure is in place and there is evidence that audits are indeed conducted.
  - Yellow: Audit procedure in place but it is unclear if audits are conducted.
  - Red: No audit procedure in place and/or no audits are conducted.

VI. RECOMMENDATIONS

A. LEGISLATURES

A core recommendation of this report is that Congress and state legislatures pass commonsense legislation, comparable to the Wiretap Act and its state analogs, to comprehensively regulate law enforcement face recognition. This legislation should implement the following recommendations, each of which is featured in the **Model Face Recognition Act** in the **Appendix**.

- **Recommendation TK. Law enforcement face recognition searches should be conditioned on an individualized suspicion of criminal conduct.**

For over two centuries, American law enforcement has been constrained by a basic standard: The police cannot search anyone they please. Rather, before law enforcement officials infringe on an individual's liberty, they generally must have an individualized suspicion that the individual is engaged in criminal conduct.

At a minimum, legislatures should require that face recognition searches be conditioned on an officer's reasonable suspicion that an individual is engaged in criminal conduct. This standard currently applies to police investigatory stops.[266] While some states require that people identify themselves at the request of police, the Supreme Court has ensured that those laws require a predicate of reasonable suspicion.[267] Face recognition allows law enforcement to identify someone *without* stopping or even talking to her. Our proposal ensures that the old standard survives new technology.

A reasonable suspicion standard should apply to all Stop and Identify, Arrest and Identify, and Investigate and Identify searches that run on mug shot databases. Higher standards should apply to riskier deployments, such as systems that rely on driver's license databases or real-time, continuous video surveillance.

- **Recommendation TK: Mug shot databases used for face recognition should exclude people who were found innocent or who had charges against them dropped or dismissed.**

Mug shot databases used for face recognition include countless individuals who have interacted with law enforcement but who have never been convicted of a crime.[268] This is particularly problematic in cases like Chris Wilson's: A single act of peaceful civil disobedience should not result in a lifetime in a criminal face recognition database.

---

[266] *See* Terry v. Ohio, 392 U.S. 1 (1968) (requiring police officers to have a reasonable suspicion that a person is involved in criminal activity prior to an investigatory stop).

[267] *See* Brown v. Texas, 443 U.S. 47, 53 (1979) (finding that a Texas statute's application was unconstitutional because it required individuals to identify themselves to police even if the police officer lacked reasonable suspicion); Hiibel v. Sixth Judicial Dist. of Nev., Humboldt Cty., 542 U.S. 177, at *5 (2004) (recognizing the "constitutional limitation" established in *Brown*, but upholding a Nevada Stop and Identify statute partly because the statute required that a field stop "be justified at its inception").

[268] *See* Ellen Nakashima, *FBI wants to exempt its huge fingerprint and photo database from privacy protections*, Washington Post (June 1, 2016) (51 percent of all arrests in the FBI's face and fingerprint database "lack final dispositions, such as whether a person has been convicted or even charged").

A single act of peaceful civil disobedience should not result in a lifetime in a criminal face recognition database.

Congress and states that rely on mug shot databases for face recognition should follow the lead of Michigan, which requires the destruction of biometric data from people who are arrested but have been found innocent, or who have had the charges against them dropped or dismissed.[269] The FBI should do this voluntarily, whether or not Congress commands it to do so.

- **Recommendation TK. Searches of license photos should only occur if state legislatures vote to allow them. States that allow access should notify the public.**

Unless and until state legislatures openly debate this access and affirmatively vote to grant it, law enforcement face recognition systems should constrain themselves to mug shot databases. Even if state legislatures *do* approve searches of license and ID photos, many citizens may remain unaware of this practice. Therefore, these states should implement a notice requirement similar to that of Washington State, which requires special notices to driver's license applicants, online postings, and "notices in conspicuous locations" in the Department of Licensing's physical offices.[270]

- **Recommendation TK: Searches of driver's license and ID photos should occur only under a court order issued upon a showing of probable cause.**

States that allow searches of driver's license and ID photos should require a higher level of individualized suspicion, preferably probable cause, for those searches. If a state scans all of its drivers' faces as part of criminal investigations, it should, at a minimum, ensure that those searches are based on reasonably trustworthy information.[271]

The determination of probable cause should not be in the hands of the police or the FBI. It should be in the hands of a state judge or a federal judge with jurisdiction over the state. As with the Wiretap Act, this judicial oversight requirement should not be total. In true emergencies, searches should initially proceed without judicial approval (but require a follow-up application). Other scenarios should not require judicial approval at all. These include searches to identify missing children, deceased victims, and lawfully arrested people during the booking process.

We also believe that judicial approval should not be required for police searches that are narrowly designed to detect identity theft and fraud. These searches parallel departments of motor vehicles' longstanding practice of "de-duping" ID photos to detect fraud.

- **Recommendation TK. Limit searches of license photos—and after-the-fact investigative searches—to investigations of serious offenses.**

---

[269] *See* Mich. Comp. Laws § 28.243(7)-(8); see also above notes TK-TK and accompanying text.
[270] Wash. Rev. Code § 46.20.037(3).
[271] *See* Brinegar v. United States, 338 U.S. 160, 175-176 (1949) ("[P]robable cause exists where 'the facts and circumstances within their [the officers'] knowledge and of which they had reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that' an offense has been or is being committed.") (citations omitted).

There is a tradition in American law enforcement of limiting the most controversial investigative techniques to the most serious crimes.[272] That principle should apply to face recognition: If a state decides to allow law enforcement to conduct face recognition searches of its driver's license and other ID photos, it should limit those searches to serious offenses, preferably those identified in the oral and wire provisions of the Wiretap Act, and identity theft and fraud.[273]

This principle should also apply to Moderate Risk deployments, which involve face recognition against a mug shot database. In a Stop and Identify deployment, where a police officer encounters someone in person, takes her photo, and uses that photo to run a face recognition search, the use of the technology is at least somewhat transparent to the search subject. In a lawfully initiated officer encounter, that officer's safety is also in play; he has a need to know whether he is interacting with a law-abiding citizen or a wanted felon.[274]

In an Arrest and Identify search, where someone is arrested and her mug shot is simultaneously enrolled and run against a mug shot database, use of face recognition may or may not be transparent—but the Supreme Court has recognized a strong state interest in the reliable identification of suspects in government custody.[275]

In an Investigate and Identify search, where a suspect is identified after the commission of the offense from a video still or surreptitious photograph, none of these interests are at play. The search is entirely invisible to the subject and the public at large. Outside of the public eye, there is a risk that some officials may use a minor offense, like jaywalking, as a pretext to justify a search to identify a peaceful protester—or an attractive member of the opposite sex.[276] For this reason, we believe that Investigate and Identify searches—even those limited to mug shot databases—should be limited to investigations of felonies.

- **Recommendation TK. Real-time video surveillance should only occur in life-threatening public emergencies under a court order backed by probable cause.**

When operating through a large network of street surveillance footage—or, potentially, police-worn body cameras—real-time, continuous face recognition would allow law enforcement to secretly locate people and track their movements. Real-time video surveillance offers police the same abilities as do real-time GPS tracking or access to cell-site location information, techniques that require court-issued warrants in a growing number of jurisdictions.[277]

---

[272] See above section TK, subsection TK (Fourth Amendment).
[273] *See* 18 U.S.C. § 2516 (1)-(2) (limiting federal interception of wire and oral communications to investigations of certain federal offenses and state wire and oral interceptions to a narrow category of felonies).
[274] *See* Terry v. Ohio, 392 U.S. 1, 30 (1968) (recognizing a state interest in officer safety during police investigative stops).
[275] *See* Maryland v. King, 133 S. Ct. 1958, 1980 (2013) (identifying "significant state interests" in identifying suspect in custody "so that the criminal justice system can make informed decisions concerning pretrial custody).
[276] *See Police across US misuse databases to look up celebrities, romantic partners and others*, Associated Press (Sept. 28, 2016), http://www.nola.com/crime/index.ssf/2016/09/police_across_us_misuse_databa.html.
[277] *See, e.g.*, Cal. Penal Code § 1546 et seq.; 725 Ill. Comp. Stat. act 168/1 et seq.; Md. Code Ann. Crim. Proc. § 1-203.1; see above notes TK, TK and accompanying text.

A simple warrant is not enough, however. If deployed pervasively, real-time video surveillance threatens to create a world where, once you set foot outside, the government can track your every move.

Some communities may conclude that real-time video surveillance is too inaccurate, or too threatening to civil liberties. Communities that decide to allow real-time video surveillance under a probable cause-backed court order should issue those orders only:

- in life-threatening public emergencies;
- in specific locations for a limited period of time; and
- upon a showing that law enforcement has exhausted other means to investigate the crime.

Most of these restrictions have direct analogs in the Wiretap Act.[278] Also like the Wiretap Act, if law enforcement is forced to use real-time video surveillance without a court order, it should file a prompt follow-up application to a court.[279]

- **Recommendation TK. Use of face recognition to track people on the basis of their race, ethnicity, religious or political views should be prohibited.**

A statute regulating law enforcement face recognition should prohibit the use of the technology to track individuals solely on the basis of their political or religious beliefs, or any other conduct protected by the First Amendment, and prohibit tracking of individuals solely on the basis of their race, ethnicity, or other protected status. Without these prohibitions, there is a real danger that face recognition could chill free speech or endanger access to education or public health.

- **Recommendation TK. All law enforcement use of face recognition should be subject to public reporting requirements and internal audits.**

Face recognition is too powerful to be secret. 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.[280] This would include:

(1) the number of face recognition searches run;

(2) the nature of those searches (i.e. Stop and Identify, Arrest and Identify, Investigate and Identify);

(3) the crimes that those searches were used to investigate;

---

[278] *See* 18 U.S.C. § 2516(1)-(2) (limiting federal interception of wire and oral communications to investigations of certain federal offenses); 18 U.S.C. § 2518(1)(c) (requiring a statement that other investigative techniques have been attempted, are unlikely to succeed, or are too dangerous); 18 U.S.C. § 2518(5) (capping wiretap authorizations to an extendable thirty-day period).

[279] *See* 18 U.S.C. § 2518(7) (allowing warrantless wiretaps in certain emergency situations, if the procedure is followed by an application within 48 hours after the wiretap has begun).

[280] *See* 18 U.S.C. § 2519.

(4) the arrests and convictions that resulted from those searches;

(5) the databases that those searches accessed;

(6) for real-time video surveillance, the duration and approximate location of those searches; and

(7) any other information that the jurisdiction deems appropriate.

These transparency measures should be coupled with the logging of all searches and rigorous audits to prevent and identify misuse.

Face recognition is too powerful to be secret.

Recommendation TK. Congress should provide funding to increase the frequency and scope of accuracy tests and create more diverse photo datasets for training.

The National Institute of Standards and Technology will need new funding to expand the frequency and scope of its accuracy tests—particularly to create new testing programs to prevent algorithmic bias and deepen testing of real-time face recognition systems. NIST can also play a role in helping face recognition companies prevent bias—not just test for it. With increased funding, NIST may be able to develop more diverse photo datasets that companies can use to improve the accuracy of their algorithms across racial, ethnic, and age groups.

Recommendation TK. State and federal financial assistance for face recognition should be conditioned on transparency, oversight, and accountability.

Many state and local face recognition systems receive federal financial assistance.[281] Congress should use its power of the purse to promote transparency, public accountability, internal audits, and accuracy. Federal financial assistance should be restricted to federal, state and local agencies that:

- publicly report use statistics;
- publicly post use manuals and obtain approval for those manuals from elected officials;
- certify that internal audits are in place; and

[281] *See, e.g.,* Pinellas County Sheriff's Office, *Request for Proposal: On-line User Training Program* (May 27, 2011), Document p. 014451 ("In 2001, PCSO initiated a law enforcement facial recognition program from grants awarded by the U.S. Department of Justice, Office of Community Oriented Policing Services (COPS)."); Seattle Police Department, *Mugshot Booking Photo Comparison DRAFT - Project Documents,* Document p. 012489 ("The Mugshot Booking Photo [face recognition] comparison project . . . is a result of funding from a Department of Homeland Security (DHS) grant under the Urban Area Security Initiative (UASI) . . ."); SANDAG, *Proposed FY 2015 Program Budget Amendment: Urban Area Security Initiative Tactical Identification System Project* (Feb. 13, 2015), Document p. 005716 (describing an award of $99,000 from the DHS Urban Area Security Initiative to continue maintaining the Tactical Identification System, which includes face recognition); Chicago Police Department, *CTA's Regional Transit Terrorism Prevention and Response System (T-CLEAR)* (Sept. 12, 2012), Document p. 008725–008729 (a grant proposal to the DHS FY09 Transit Security Grant Program outlining a video security system that includes face recognition).

- participate in NIST accuracy tests, and, when they are available, tests for racially biased error rates.

State legislatures can institute similar measures.

B. LAW ENFORCEMENT

Regardless of when legislatures act, there are a number of steps that federal and state law enforcement can take to address the problems presented in this report.

1. FEDERAL BUREAU OF INVESTIGATION & DEPARTMENT OF JUSTICE

- **Recommendation TK: Require probable cause for and restrict searches of driver's license and ID photo databases to serious, enumerated offenses.**

The FBI should voluntarily refrain from searching driver's license and ID photos in states that have not passed legislation expressly authorizing criminal face recognition searches of those databases. If the FBI decides to proceed with these searches, it should voluntarily restrict them to investigations of serious offenses enumerated in the oral and wire provisions of the Wiretap Act.[282]

In addition, these searches should be limited to instances in which the FBI has probable cause to believe that the subject of the search committed the offense in question. While a probable cause standard is not common for systems that rely on driver's license databases, some major jurisdictions have adopted it without apparent impediments to their law enforcement mission.[283]

- **Recommendation TK: Leverage police access to the FBI face recognition database (NGI-IPS) to promote best practices for face recognition.**

At the moment, seven states have the ability to search the FBI face recognition database, which is populated by 24.9 million mug shots. Over time, that number will grow, giving the FBI an even greater opportunity to promote best practices for state and local police. In line with the recommendations set out for legislatures, officers should be allowed to search the database only after certifying that they have a reasonable suspicion that the suspect in question committed a felony offense. The FBI should itself adopt this policy for all mug shot searches.

More broadly, access to the FBI face recognition database should be conditioned on an agency's adoption of a face recognition use policy, public posting of that policy, and its approval by a city council or local legislature. They should also be contingent on audits.

- **Recommendation TK: Audit police and FBI searches of the FBI face recognition database and FBI searches of state driver's license and ID photo databases.**

In a 2012 Senate hearing on FBI use of face recognition, then Deputy Assistant Director of FBI Criminal Justice Information Services (CJIS), Jerome Pender, assured the public that

[282] *See* 18 U.S.C. §§ 2516 (1)–(2).
[283] *See above* Figure TK Legal Standards for Face Recognition Search, by Jurisdiction.

state agencies' use of the FBI's face recognition database would be audited—both by the FBI and the state agency in accordance with agreements signed with those agencies.[284] The Privacy Impact Assessment for the FBI's face recognition database also says that "robust audit processes [are] already present," and that agencies requesting searches "will be subject to training and audit requirements by the applicable CJIS Systems Agency (CSA) and periodic FBI audits."[285] The 2016 GAO report revealed, however, that the FBI had never audited state agency searches of the FBI's face recognition database—nor had the FBI audited its own use of state databases.[286] Going forward, these audits should be conducted.

Despite the FBI's assurances in the 2012 hearing, the signed agreements that have been made public do not require that states annually audit their own use of the FBI face recognition database.[287] If it is not now in place, this requirement should be added to all MOUs between state agencies and the FBI.

- **Recommendation TK: The FBI should test its face recognition system for accuracy and racially biased error rates, and make the results public.**

The last public accuracy statistics for the FBI face recognition database suggest that it successfully includes the correct candidate in a list of 50 potential matches only 86% of the time.[288] In other words, in this test, one out of every seven searches returned a list of 50 "innocent" candidates. This test was run on a database 25 times *smaller* than the current FBI face recognition database; generally, errors increase with database size.

This is not acceptable. The FBI should regularly test its system for accuracy and make those results public. It should do the same for racially biased error rates.

- **Recommendation TK: Investigate state and local agencies' use of face recognition for potential disparate impact.**

The Department of Justice Civil Rights Division regularly investigates state and local police practices. They should extend those investigations to explore face recognition, as the

---

[284] *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.").

[285] Federal Bureau of Investigation, U.S. Department of Justice, *Privacy Impact Assessment for the Next Generation Identification (NGI) Interstate Photo System*, (Sept. 2015), https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/interstate-photo-system.

[286] *See* U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 25–32 (May 2016) (audits "have not yet assessed the use of face recognition searches of NGI-IPS").

[287] *See, e.g.* Michigan State Police, *MOU between the FBI and The Michigan State Police for the Interstate Photo System Facial Recognition Pilot (IPSFRP)* (Apr. 8, 2011), Document pp. 011304–011309; Nebraska State Patrol, *MOU between the FBI and Nebraska State Patrol for the IPSFRP* (Oct. 2012), Document pp. 009183–009189.

[288] *See* U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 49, 26 (May 2016) (describing test results on a dataset of 926,000 photos.

systems used by a number of agencies under recent investigation may produce a disparate impact on minority communities.

In Maricopa County, Arizona, for example—the subject of a recently settled DOJ civil rights lawsuit[289]—the Maricopa County Sheriff's Office (MCSO) enrolled all of Honduras' driver's license photos into its face recognition system as part of an effort to combat Mara Salvatrucha, a Central and North American gang.[290] African Americans are themselves likely overenrolled in the system, which also searches mug shots. In Arizona, African Americans are arrested at a rate close to three times that of their share of the population.[291]

- **Recommendation TK: Develop procurement guidance for state and local agencies purchasing face recognition programs with DOJ funding.**

DOJ can support state and local accountability efforts by providing procurement guidance for agencies receiving DOJ funding. This guidance should discourage the use of sole source contracting for initial purchases or heighten sole source justification requirements. It could also encourage: (1) including specific target accuracy levels in agency Requests for Proposals (RFPs); (2) requiring proof of participation in NIST accuracy tests; (3) accuracy verification testing during the system acceptance process; and (4) regular independent accuracy tests during the contract period, including internal tests and submission to all applicable NIST tests during that period.

- **Recommendation TK: Reverse the current proposal to exempt the FBI's face recognition system from key Privacy Act requirements.**

If promulgated, this rule would eliminate key mechanisms for public transparency and accountability over a database already operating largely in the dark. This report strongly suggests that we need more transparency over face recognition, not less. The DOJ and FBI should reverse this proposal.[292]

- **Recommendation TK: Voluntarily release detailed public reports on the FBI's face recognition programs.**

These reports would detail the databases that the FBI searches, the number and nature of face recognition searches conducted by the FBI and states accessing the FBI system, arrests and convictions stemming from those searches, and the types of crimes investigated. The annual release of this information would add a layer of public transparency and accountability to

[289] U.S. Department of Justice, *Justice Department Reaches Settlement in Civil Rights Lawsuit Against Maricopa County, Arizona, and Maricopa County Sheriff*, https://www.justice.gov/opa/pr/justice-department-reaches-settlement-civil-rights-lawsuit-against-maricopa-county-arizona (last visited Oct. 2, 2016).
[290] *See* Maricopa County Sheriff's Office, *Purchase of Equipment to Enhance the MCSO Facial Recognition Unit at the ACTIC* (Aug. 20, 2007), Document p. 015058.
[291] *See above* note TK.
[292] For more information, see the Center's filing on the proposed exemptions. Center on Privacy & Technology et. al., Comment on Proposed Rule to Exempt Next Generation Identification System from Provisions of the Privacy Act and the Modified System of Records Notice for that System (July 6, 2016), https://www.regulations.gov/document?D=DOJ-OPCL-2016-0008-0114 (explaining the impact of the proposed exemptions).

complement internal audits. These reports could be modeled after the annual reports required under the Wiretap Act.[293]

2. STATE & LOCAL LAW ENFORCEMENT

- **Recommendation TK: Impose a moratorium on face recognition searches of state driver's license and ID photos until state legislatures regulate that access.**

Many states have driver's privacy laws that allow law enforcement to access driver's license and ID photos; we identified only two, however, that expressly allow law enforcement to run *face recognition* searches of those photos.[294] State and local law enforcement should impose a moratorium on these searches until state legislatures have the opportunity to debate and regulate them through legislation.

- **Recommendation TK: Adopt public face recognition use policies that have received legislative review and approval.**

All agencies, including those that access another agency's system, should adopt a face recognition use policy, preferably in line with the recommendations set out above. Policies should be developed simultaneous to—if not before—the implementation of a face recognition system or upon gaining access to another agency's system. Most importantly, they should be made public and submitted for approval by city councils or other local legislative bodies.

A **Model Police Face Recognition Use Policy**, based on best practices in existing polices around the country, is included in the **Appendix**.

- **Recommendation TK: Use contracts and the contracting process to maximize accuracy.**

Agencies should avoid sole source contracting for initial purchases. In a competitive RFP, agencies should require vendor companies to demonstrate target accuracy levels and prove an algorithm's submission to NIST accuracy tests. The system acceptance process should include accuracy verification testing on searches that mimic the agency's actual use of face recognition—such as on probe images that are of lower quality or feature a partially obscured face. Final contracts should require continued internal accuracy testing in operational settings and submission to all applicable NIST tests. Finally, agencies should avoid contracts where the vendor has disclaimed responsibility for the accuracy of the algorithm, even when the vendor uses a third-party algorithm.

- **Recommendation TK: Implement internal audits, tests for accuracy and racial bias, and the use of trained face examiners.**

Law enforcement agencies should audit their officers' use of face recognition, regardless of whether the agency runs its own system or accesses another's. They should regularly test their systems for accuracy and, when the tests become available, racial bias. Each search

[293] *See* 18 U.S.C. § 2519.

[294] *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").

should be conducted or reviewed by trained facial examiners to minimize algorithm error and possible bias in the search results.

C. NATIONAL INSTITUTE OF STANDARDS & TECHNOLOGY

- **Recommendation TK: Regularly include tests for algorithmic bias along the lines of race, gender, and age in face recognition competitions.**

NIST's assessments are widely considered to be the gold standard in face recognition testing, yet NIST has checked for racial bias only once despite holding Face Recognition Vendor Test (FRVT) competitions for more than a decade. This information would be of immense value to law enforcement agencies that look to acquire face recognition technology.

- **Recommendation TK: Increase the frequency of face recognition competitions, ideally testing on an annual or biennial basis.**

New innovations, such as deep learning or drastic reductions in template sizes, can reshape the technological landscape seemingly overnight. NIST's current testing regime, which offers a competition every three to four years, is too infrequent to keep up with the pace of innovation. Acknowledging resource limitations, NIST should ideally hold its competition every one to two years.

- **Recommendation TK: Continue to update tests to reflect state-of-the-art advances in face recognition and mobile biometrics.**

Face recognition technology continues to advance. To NIST's credit, it has kept pace with these developments, offering a Face in Video Evaluation (FIVE) competition that is currently in progress. NIST should continue to monitor developments in face recognition and test accordingly. For live video streams, we recommend that, in addition to testing for accuracy, NIST should emphasize measuring computational resource consumption—the constraint that researchers have noted to be the technology's primary limiting factor.

- **Recommendation TK: Develop tests that closely mirror law enforcement workflows, and issue best practices for accuracy testing.**

Law enforcement agencies ask face recognition algorithms to perform a wide variety of tasks; an algorithm that excels at one task may struggle at another. NIST should strive to ensure that FRVT competitions explicitly test algorithms in ways that mimic each of these real-world law enforcement workflows, ensuring that agencies can make informed procurement decisions tailored to their intended use-cases. Since NIST tests are considered the gold standard among both researchers and companies, we recommend that NIST establish a standards or best practices document to assist other organizations or law enforcement agencies that wish to test face recognition algorithms.

- **Recommendation TK: Develop and distribute diverse datasets of photos.**

Researchers and engineers universally complain about the lack of large, high-quality, diverse datasets of faces. NIST, along with other government efforts (such as the IARPA Janus project), is well placed to take the lead in developing and distributing such data, which would both aid algorithm design and provide a continual source of independent benchmarks.

D. FACE RECOGNITION COMPANIES

- **Recommendation TK: Internally check for algorithmic bias along the lines of race, gender, and age.**

Neither of the major face recognition companies that we interviewed in the spring of 2016 could point to an internal test that specifically checked for racial bias. Companies should develop tests to measure this bias. Furthermore, companies should work to find the sources of this bias, mitigate it where possible, and inform law enforcement agencies when it cannot be eliminated completely.

- **Recommendation TK: Submit to public, independent accuracy competitions and publish performance results using modern, publicly available datasets.**

Public, independent accuracy tests by NIST and the University of Washington offer the only basis for comparing the performance of face recognition algorithms. Companies should continue to submit their algorithms for these tests; they should also voluntarily publish performance results for modern, publicly available benchmarks that can serve as an additional basis for comparison. Some companies, such as Cognitec,[295] have done so in part, but only for older datasets such as the NIST Color FERET Database,[296] which was created in 1996.

E. COMMUNITY LEADERS

- **Recommendation TK: Press local and state police departments and the FBI to be transparent and adopt policies to protect privacy, civil liberties, and civil rights.**

Face recognition systems cost money. Taxpayers are paying the bill. They have a right to know how those systems are being used, and demand that they respect their privacy, civil liberties, and civil rights.

Community leaders should press state and local agencies, and the FBI, to be fully transparent about how they use face recognition; if those agencies refuse, advocates should use state and federal Freedom of Information laws to take them to court. Advocates should also press city councils, state legislatures, and law enforcement for laws and use manuals that protect individual liberties and civil rights.

The **City and State Backgrounders** in the **Appendix** summarize face recognition systems in 25 different jurisdictions and link to the original documents from those agencies. Whether or not a backgrounder is available, citizens should ask their elected officials or local law enforcement agency the following questions:

(1) **Who is enrolled in the police face recognition database?** Is it built from mug shots, driver's license and ID photos, or other sources? If mug shots are used, do

[295] *See* Cognitec, *FaceVACS Technology: A16 Algorithm Performance*, http://www.cognitec.com/files/layout/downloads/FaceVACS-algorithm-performance-A16.pdf (last visited Sept. 22, 2016).
[296] *See* National Institute of Standards and Technology, U.S. Department of Commerce, *Color FERET Database*, http://www.nist.gov/itl/iad/ig/colorferet.cfm (last visited Sept. 22, 2016).

police eliminate photos from cases involving no-charge arrests or not guilty verdicts? If they use driver's license and ID photos, are people notified of this at the DMV?

(2) **Who can search the face recognition database?** Can other local, state, or federal law enforcement agencies (like the FBI) search or request searches of the system?

(3) **What kinds of face recognition searches are run?** Do they use it to identify people they arrest or stop on patrol? Do they use it to identify criminal suspects from surveillance video footage? Do they have plans to use face recognition to identify people in real-time from live surveillance video?

(4) **Does the agency have a face recognition use policy?** If not, why not?

(5) **What legal requirements must be met before officers run a face recognition search?** Does an officer at least need a reasonable suspicion that someone is involved in a crime before he can run a search to identify that person? Or can officers run a search on anyone, so long as it is for a law enforcement purpose? Do searches of license and ID photos require a higher standard, like probable cause? Will the agency require warrants for real-time searches on live surveillance video?

(6) **Is the agency's face recognition use policy available to the public?** Was it approved by a city council or other elected officials? Did privacy and civil liberties groups review it?

(7) **How does the agency ensure that its face recognition system is accurate?** Has the company submitted its algorithm to accuracy tests conducted by the National Institute of Standards and Technology? Does the purchase contract require certain accuracy thresholds and require ongoing accuracy tests in operational conditions? Are all candidate matches screened by specially trained human examiners whose decisions are peer reviewed?

(8) **How does the agency ensure that its face recognition system is not biased on the basis of race, gender or age?** Has the agency tested the system to make sure it is not biased against certain demographic groups? Has the agency asked its face recognition vendor about this possibility, and if so, what steps has the vendor taken to address this problem?

(9) **How does the agency's face recognition use policy protect free speech?** Does the policy expressly prohibit using the technology to identify individuals based solely on their political or religious beliefs or their membership in a racial or ethnic minority, or is this in a separate, general document? Does the policy allow face recognition to be used near schools and hospitals?

(10) **How does the agency stop and detect misuse and abuse?** Does it log all searches and audit them? If not, why not?

For law enforcement face recognition to be brought under a reasonable system of regulation, communities need to ask questions—and take action.

VII. CONCLUSION

On September 17, 2016, a week after the 15th anniversary of the September 11th attacks, New Jersey and the New York City region were shaken by two bombings and gripped with the fear of more to come. A suspect, Ahmad Khan Rahami, was apprehended just two days after the initial attack in Seaside Park, New Jersey. In the press, news emerged that a powerful technology had been used in the investigation: face recognition.[297]

It is unclear if face recognition actually helped investigators find Rahami.[298] But the attacks in New York and New Jersey raise an urgent question: In regulating law enforcement use of face recognition, will we blunt our ability to respond quickly and effectively to threats to our safety?

We believe that the answer to this question is clearly "no." A core conclusion of this report is that deployments of face recognition are diverse and differentiable. 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. The regulatory scheme that we propose will allow communities to enforce that difference.

Face recognition is not a monolith. Certain uses of the technology present fewer risks and conform to longstanding police practice. But as face recognition advances, it creates profound questions about the future of our society.

Are we comfortable with a world where face recognition is used to identify someone who police officers have legally stopped or arrested, or where it is used, in emergencies, to locate violent criminal suspects and terrorists? Perhaps.

Are we comfortable with a world where anyone with a driver's license is automatically enrolled in a virtual, perpetual line-up? Are we comfortable with a world where the government can find anyone, at any time, by scanning the faces of people on the sidewalk? Are we comfortable with a world where this technology is less accurate on African Americans, yet more likely to be used to try to identify them?

As face recognition advances, it creates profound questions about the future of our society.

---

[297] *See* Shanika Gunaratna, *The tech that went into catching the NY, NJ bombing suspect*, CBS News (Sept. 19, 2016), http://www.cbsnews.com/news/tech-that-went-intro-catching-nj-nj-bomb-suspect/; Anthony M. DeStefano, *How bomb suspect Ahmad Khan Rahami was caught in just 50 hours*, Newsday (Sept. 19, 2016), http://www.newsday.com/news/new-york/how-bomb-suspect-ahmad-khan-rahami-was-caught-in-just-50-hours-1.12339972.

[298] *See* Shanika Gunaratna, *The tech that went into catching the NY, NJ bombing suspect*, CBS News (Sept. 19, 2016), http://www.cbsnews.com/news/tech-that-went-intro-catching-nj-nj-bomb-suspect/ ("It's still unclear to what extent officials used automated facial recognition technology"); Anthony M. DeStefano, *How bomb suspect Ahmad Khan Rahami was caught in just 50 hours*, Newsday (Sept. 19, 2016), http://www.newsday.com/news/new-york/how-bomb-suspect-ahmad-khan-rahami-was-caught-in-just-50-hours-1.12339972 ("NYPD investigators tried to use facial recognition software to identify Rahami, but the images of him captured on surveillance cameras around the bombing sites were either too grainy or didn't show his face at the proper angle").

Technology will not wait for us to answer these questions. Neither will law enforcement. Yet state legislatures and Congress have not passed a single law to comprehensively regulate police use of face recognition—and the Supreme Court has never formally recognized a right to privacy in public. With little to guide them, most—though not all—police departments have not taken adequate steps to rein in this surveillance technology.

In a rapidly evolving world, technology often outpaces privacy law. It is time for privacy law to catch up. Achieving this will require the action of all stakeholders. Privacy protections will not succeed if they are imposed unilaterally without the involvement of law enforcement, face recognition experts, and community leaders. It is time to enact 21st Century privacy protections for a 21st Century surveillance technology.

VIII. ACKNOWLEDGEMENTS

This report would not be possible without the foundational research and advocacy of the American Civil Liberties Union, the Electronic Frontier Foundation, and the Electronic Privacy Information Center; the oversight actions of Senator Al Franken of Minnesota and the Government Accountability Office; and the foresight of Professor Laura Donohue of Georgetown University Law Center, who also serves as a faculty director of the Center. We are grateful for the pioneering work of Upturn and the Leadership Conference on Civil and Human Rights, whose scorecard to evaluate the civil rights impact of police-worn body cameras was a model for this report.

Many of the ideas in this report were developed in the course of the 2015 and 2016 Georgetown Law/Massachusetts Institute of Technology privacy practicums. We owe a particular debt to the two student teams, comprised of law students and engineers, that each spent a semester exploring regulatory solutions to the thorny problems that face recognition presents: Kelly Singleton, Benjamin Tidor, and Madars Virza (2016); and Shirley Chen, Camille Fischer, Leah Rabkin, and Harrison Rudolph (2015). Ben Sobel contributed key insights and ideas to a predecessor to this report.

In a talented team of researchers, Katie Evans, Edward George, Moriah Daugherty, Sabrina McCubbin, Harrison Rudolph, and Ilana Ullman went above and beyond and were central to the development and execution of this report. Critical guidance and close reading were provided by Professors Paul Ohm and David Vladeck, both Center faculty directors, and Professor Andrew Ferguson of the University of the District of Columbia David A. Clarke School of Law. The remainder of our expert reviewers will remain anonymous, but we are deeply thankful for their time and attention to this effort.

The Center on Privacy & Technology at Georgetown Law is supported by the Ford Foundation, the Open Society Foundations, the Georgetown University Law Center, the Media Democracy Fund, and the Google Policy Fellowship.

Most importantly, we are grateful to the men and women in police departments around the country who provided us with detailed records on how their agencies use face recognition and took the time to answer our detailed follow-up questions.

IX. ENDNOTES

[All the footnotes in the document will be converted to endnotes and placed here.]

X. METHODOLOGY

A. Records request survey of law enforcement agencies.

We submitted an initial 106 public records requests to state and local law enforcement agencies across the country.[299] We selected agencies that met at least one of two criteria:

(1) Agencies we could identify as having piloted or implemented face recognition. We identified these agencies from news articles, vendor or agency press releases and annual reports, or other publicly available sources discussing the implementation of face recognition for law enforcement purposes.

(2) The 50 largest law enforcement agencies in the country, by force size.

Each records request asked for any policies, manuals, or procedure documents the agency had created or received; audit reports; training manuals and technical specifications; contracting and financial documents; and any memoranda of understanding or other agreements pertaining to face recognition. In total, we received substantive responses from 90 agencies, and over 15,000 pages of responsive records. A list of the agencies we surveyed, grouped by type of response received, and a template of the records request, can be found in this section.

Following up on our records request, we conducted over a dozen phone interviews with agency officials about their current or former use of face recognition. We also conducted site visits and more extensive in-person interviews with two agencies, the Michigan State Police and the Pinellas County Sheriff's Office. In the interest of obtaining candid answers, some of the interviews with engineers and vendor companies were conducted on the condition of anonymity.

All City and State Backgrounders were sent in draft form to the respective agencies in advance of publication, with an invitation to submit edits if needed. We have incorporated the relevant information that was provided to us in response to these drafts.

B. Face recognition technology research and literature review.

To complement our records request survey and to gain an understanding of the state of face recognition technology today, we conducted interviews with researchers both in academia and government who worked on: (1) the application of face recognition to law enforcement; (2) issues surrounding biases in accuracy rates across race; and (3) the role of trained human review of face recognition results. We also spoke with technologists and representatives from two of the leading companies that provide face recognition algorithms to law enforcement about their approach to testing and compensating for accuracy biases. Additionally, we conducted an in-depth review of the existing technical literature on face recognition, focusing particularly on research addressing the presence of bias in the accuracy rates of face recognition algorithms.

[299] As of October TK, 2016, we have submitted an additional TK records requests to state agencies not surveyed in the first round of records requests.

C. Fifty-state legal survey of biometrics laws.

We conducted a fifty-state survey of laws that may govern or inform the use of face recognition by law enforcement, or, for comparison, state laws that govern the use of other tracking or surveillance technology. This survey answered the following questions:

(1) Does the state have any non-fingerprint biometrics law that would control law enforcement use of face recognition?

(2) Does the state have a law that either allows or restricts law enforcement use of or access to photographs from driver's license records?

(3) Does the state have a "stop-and-identify" law?

(4) Has the state passed a law regulating law enforcement use of geolocation tracking?

(5) Has the state passed a law regulating the use of drones?

(6) Has the state passed a law regulating the use of automated license plate readers (ALPRs)?

D. The Face Recognition Scorecard.

We evaluated each agency on seven criteria. We scored all agencies that (1) owned a face recognition system and provided us with responsive documents, as well as (2) the agencies that access the FBI's face recognition database, the Next Generation Identification Interstate Photo System, and (3) the FBI face recognition unit (FACE Services). There is overlap between the first two categories. Entries are greyed out where we did not have sufficient information to evaluate the agency on that criterion.

- **People in the Database.** Who is enrolled in the face recognition database or network of databases available to the law enforcement agency?
    - Green: Mug shots of individuals arrested, with enrollment limited based on the underlying offense, and/or with mug shots affirmatively "scrubbed" by police to eliminate no-charge arrests or not-guilty verdicts.
    - Yellow: Mug shots of individuals arrested, with no limits or rules to limit which mug shots are enrolled, or where mug shots are removed only after the individual applies for, and is granted, expungement.
    - Red: Driver's license photos in addition to mug shots of individuals arrested.

- **Real-Time Video Surveillance.** How has the agency addressed the risks of real-time or historical video surveillance?
    - Green: Written policy (1) prohibiting the use of face recognition for real-time video or historical video surveillance, or (2) that restricts its use only to life-threatening public emergencies and requires a warrant.
    - Yellow: No written policy addressing real-time or historical video surveillance, but agency has affirmatively stated that it does not use face recognition in this manner.

- Red: Agency has deployed, purchased, or indicated a written interest in purchasing face recognition for real-time or historical video surveillance but has not developed a written policy or affirmatively disclaimed these practices.

- **4th Amendment.** What legal standard does the agency require prior to a face recognition search? This is a bifurcated standard. If the agency uses face recognition on databases that include only mug shots, earning it a "green" or "yellow" in the first column (People in Database), the first standard is used. If the agency uses face recognition on databases that include driver's license photos, earning it a "red" in the first column, the second standard is used.

  Targeted database—mug shots only.
  - Green: Reasonable suspicion of the subject to be searched, and at least one of the following: (1) searches are limited to suspects and victims of crimes; and (2) Investigate and Identify searches are limited to felonies only.
  - Yellow: Reasonable suspicion of the subject to be searched but the standard has exceptions or allows for searches for bystanders or witnesses as well.
  - Red: No legal standard stated, or a statement that face recognition may be used for any "law enforcement" or "criminal justice" purpose.

  Dragnet database—license and ID photos.
  - Green: (1) Searches are limited to investigations of serious offenses *and* require a warrant or court order supported by probable cause; or (2) searches are limited to identity-related crimes.
  - Yellow: Probable cause *or* searches are limited to investigations of serious offenses (for non-identity related crimes).
  - Red: Anything less than probable cause (for non-identity related crimes).

- **Free Speech.** Has the agency considered and taken steps to limit the use of face recognition in a way that would pose risks to free speech, assembly, and association?

  - Green: Express statement in a face recognition use policy prohibiting the use of face recognition to target or collect information on individuals on the basis of their race, religion, or other bases that may stifle speech.
  - Yellow: (1) A statement in a face recognition use policy prohibiting the use of face recognition in violation of state or federal law, including the First Amendment; or (2) a statement in a general operating policy or police manual prohibiting the targeting or collection of information on individuals on the basis of their race, religion, or other bases that may stifle speech.
  - Red: No statements outlined in either section above.

- **Accuracy.** How has the agency built safeguards against errors into their face recognition program?

  - Green: Agency demonstrates **four** or **five** criteria listed below.
  - Yellow: Agency demonstrates **three** of the criteria.
  - Red: Agency demonstrates **two** or fewer of the criteria.

  - The criteria are:

  - Algorithms have been tested by the National Institute of Standards and Technology;
  - Contract with vendor company contains provisions that require face recognition algorithms to have been tested for accuracy and will be tested at all future opportunities;
  - Most or all face recognition queries are validated by trained human examiners or agencies have a unit or designated personnel that perform a review and screening function of the candidate lists (weighted as two criteria);
  - Face recognition results or candidate lists are treated as investigative leads only.

- **Public Transparency.** Has the agency publicly posted its face recognition use policy, and has it been reviewed or approved by a legislature or privacy and civil liberties groups?

  - Green: Agency has a public face recognition use policy that has been reviewed or approved by a legislature and/or privacy and civil liberties groups.
  - Yellow: Agency has a public use policy, but there is no evidence the policy received external review or approval.
  - Red: Agency has not made its use policy public, or has no use policy.

- **Internal Audits.** Does the agency monitor and conduct audits of face recognition use by its officers and other accessing agencies? (Since our records request specifically asked for records pertaining to audits, when an agency did not provide audit records or sample audit forms and did not deny this request, it was assumed that no audits were conducted.)

  - Green: Formal audit procedure is in place and there is evidence that audits are indeed conducted.
  - Yellow: Audit procedure in place but it is unclear if audits are conducted.
  - Red: No audit procedure in place and/or no audits are conducted.

E. Agencies Surveyed Grouped by Response

Currently use or have acquired face recognition

1. Albuquerque Police Department
2. Baltimore Police Department
3. Carlisle Borough Police Department
4. Carlsbad Police Department
5. Chicago Police Department
6. Chula Vista Police Department
7. Daytona Beach Police Department
8. Fairfax County Police Department
9. Hawaii Criminal Justice Data Center
10. Honolulu Police Department
11. Iowa Department of Public Safety
12. Jacksonville Sheriff's Office
13. King County Sheriff's Office
14. Lincoln Police Department
15. Los Angeles County Sheriff's Department
16. Los Angeles Police Department
17. Maricopa County Sheriff's Office
18. Maryland Department of Public Safety and Correctional Services
19. Maryland State Police
20. Miami Police Department
21. Michigan State Police
22. Minnesota Department of Public Safety
23. Montgomery County Police
24. Nebraska State Patrol

25. Northern Virginia Regional Information System
26. Ohio Bureau of Criminal Investigation
27. Palm Beach County Sheriff's Office
28. Pennsylvania State Police
29. Pennsylvania JNET
30. Philadelphia Police Department
31. Pierce County Sheriff's Department
32. Pinellas County Sheriff's Office
33. Prince George's County Police Department
34. San Diego Association of Governments
35. San Diego County Sheriff's Department
36. San Diego Police Department
37. San Francisco Police Department
38. Seattle Police Department
39. Snohomish County Sheriff's Office
40. South Sound 911
41. Tampa Police Department
42. Texas Department of Public Safety
43. Virginia State Police
44. West Virginia Intelligence Fusion Center

Formerly used or acquired face recognition

45. Arizona Department of Public Safety
46. Auburn Police Department
47. Cumberland County Sheriff's Department
48. Illinois State Police
49. Kansas City Police Department
50. New Bedford Police Department
51. Plymouth County Sheriff's Department
52. San Jose Police Department

Planned future use of face recognition

53. Dallas Area Rapid Transit Police

No responsive records—agency stated it does not use face recognition

54. Arkansas State Police
55. Atlanta Police Department
56. Austin Police Department
57. Blount County Police Department
58. Boston Police Department
59. Charleston Police Department
60. Charlotte-Mecklenburg Police
61. Cincinnati Police Department
62. City of Ogden Police
63. Columbus Police Department
64. D.C. Metro Police Department
65. Denver Police Department
66. Detroit Police Department
67. Las Vegas Metro Police
68. Louisville Metro Police
69. Memphis Police Department
70. Milwaukee Police Department
71. Nashville Metro Police
72. New Orleans Police Department
73. Oklahoma City Police
74. Pinal County Sheriff's Office
75. San Antonio Police Department
76. Tucson Police Department
77. Vermont State Police

No responsive records—response did not indicate whether other not agency uses face recognition

78. Dallas Police Department
79. El Paso Police Department
80. Fort Worth Police Department
81. Houston Police Department

82. Nassau County Sheriff's Office
83. New Jersey State Police
84. Oakland Police Department
85. Orange County Sheriff's Department
86. Phoenix Police Department
87. Rhode Island State Police
88. South Carolina Department of Public Safety
89. Saint Louis Police Department
90. Utah Department of Public Safety

Complete denial of records request; appeal pending

91. New York City Police Department

No response to records request

92. Baltimore County Police Department
93. Brockton Police Department
94. Broward County Sheriff's Department
95. Cleveland Police Department
96. Essex County Police Department
97. Indianapolis Metro Police
98. Massachusetts Department of Public Safety
99. Miami-Dade County Sheriff
100. Mississippi Department of Public Safety
101. New Mexico Department of Public Safety
102. Newark Police Department
103. Raleigh Police Department
104. Salt Lake City Police
105. Saint Louis County Police Department
106. Suffolk County Police

F. Records Request Template

[Date]

[Agency Address]

Re.: **Public Records Request—Facial Recognition Technology**

Dear Public Records Officer:

The Center on Privacy & Technology, a think tank based at the Georgetown University Law Center, is conducting a survey of law enforcement agencies' use of facial recognition technology (FRT). This is part of a project examining the benefits and possible risks of FRT in policing.

Pursuant to [State Records Request Law and citation], we request the following records pertaining to FRT. We intend this request to cover all software, hardware, databases and other technology used in FRT systems. However, we realize the following list of records is long, and not all records will be relevant or available. Therefore if it would be helpful, we welcome a phone conversation to narrow this request up front.

Records Requested

Please provide copies of the following records:

- Any manuals, policies, procedures and practices the agency follows for *using* the FRT system or requesting a FRT search from another party. This request includes, but is not limited to:
    - Procedures for using, deleting or retaining probe photos (photos of subjects being identified);
    - Sources of probe photos, such as mobile devices, body cameras or surveillance videos;
    - Procedures the agency follows after a positive match, such as requiring independent or in-person verification;
    - Permitted uses of the information created from a system match.

- Any manuals, policies, procedures and practices the agency follows for *inputting* photos and other information or migrating photo databases into the FRT system. This could be a list of sources for photos and other information (e.g., mug shot photos, driver's license records, or prior probe photos).

- Any audits of the FRT system, including but not limited to: audits of the system, misuse reports, and reports to oversight bodies.

- The legal standard, if any, (e.g., probable cause, court order, relevance, consent) that is required before using the FRT system.

- Warrant applications for facial recognition searches, or judicial decisions and orders in the agency's possession governing the agency's use of the FRT system or requests to obtain a facial recognition search.

- Purchasing and procurement documents, including but not limited to: purchase orders, RFPs, responses to RFPs, invoices, and contracts for FRT hardware, software, and services.

- Any materials for training law enforcement and other personnel on using and maintaining the FRT system, including training manuals for mobile devices or other FRT hardware.

- Any manuals from the companies providing FRT system components, including but not limited to any technical specifications they have provided.

- Memoranda of Understanding (MOUs) or agreements with other state or local agencies—such as the Dep't of Motor Vehicles or a municipal agency—on the use of, or requests to search, their FRT systems. Records of the requests made, including but not limited to: the number of requests made and the number granted.

- MOUs or agreements with federal, state or local law enforcement agencies on the use or sharing of FRT systems, and the results from those systems, including but not limited to: the number of requests made and the number granted.

This request is made on behalf of a not-for-profit organization whose mission is to advance the field of privacy and technology policy and to train law students from around the county in this field. Because of our not-for-profit status and the fact that this request is about a matter in the public interest, we request a fee waiver. If such a waiver is denied, please inform us in advance if the cost will be greater than $50.

According to [State Records Request Law], a custodian of public records shall comply with a request [within X business days of receipt / timeframe specified in the law]. Please furnish all responsive documents to Clare Garvie at (b) (6) or:

Center on Privacy & Technology
McDonough Hall 444
600 New Jersey Ave, NW
Washington DC 20001

If you have any questions or want to discuss narrowing this request, please contact me at (b) (6) or (b) (6) within the above timeframe. Thank you for your prompt attention to this matter.

Sincerely,

Clare Garvie

XI. MODEL FACE RECOGNITION LEGISLATION

This model bill is written for either Congress or a state legislature.

- The federal bill would control all federal and state law enforcement (1) access to all arrest photo databases and driver's license and ID photo databases, and (2) use of real-time face recognition.

- The state bill would control (1) state law enforcement access to arrest photo databases, (2) state *and federal* law enforcement access to the driver's license and ID photo databases maintained by that state, and (2) state law enforcement use of real-time face recognition within the state.

Language specific to state legislation is in blue; federal legislation language is in red. To produce a copy of the state bill, delete red text and keep blue text; for the federal bill, delete blue text and keep red text.

This bill is written to regulate law enforcement use of face recognition. However, other remotely capturable biometric technology—such as iris scanning and voice or gait analysis—is rapidly evolving. The Center on Privacy & Technology would welcome the opportunity to assist community advocates or elected officials who wish to craft legislation to regulate remote biometric identification more broadly.

* * *

IN THE _____

A
BILL

To regulate law enforcement use of face recognition technology.

Be it enacted by the _____,

Section 1. Short Title.

This Act may be cited as the "Face Recognition Act of 2016."

Section 2. Definitions. As used in this Act—

(a) **"Face recognition"** means the automated or semi-automated process by which a person is identified based on the characteristics of his or her face.

(b) **"Targeted face recognition"** means the use of face recognition to identify or attempt to identify a specific person on a case-by-case basis.

(c) **"Continuous face recognition"** means the use of face recognition to identify or attempt to identify groups of persons without any particularized suspicion of criminal conduct, including the use of face recognition to continuously identify persons whose images are captured or recorded by a public surveillance camera.

(d) **"Arrest photo database"** means a database populated primarily by booking or arrest photographs or photographs of persons encountered by investigative or law enforcement officers.

(e) **"[State] identification photo database"** means a database populated primarily by photos from driver's licenses or identification documents made or issued by or under the authority of [the/a] State, or a political subdivision of [the/a] State [, or the United States government].

(f) **"Emergency watchlist"** means a highly targeted database populated by a specific person or persons whom there is probable cause to believe have committed, are committing, or are about to commit an offense that involves the immediate danger of death to any person.

(g) [**"Investigative or law enforcement officer"** means any officer of a State or a political subdivision a State or of the United States, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in the State criminal code or Title 18 of the U.S. Code, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses.]

(h) [**"State investigative or law enforcement officer"** means any officer of the State or a political subdivision the State who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in the State criminal code, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses.]

Title I. Use of Face Recognition by Law Enforcement

Section 101. Targeted Face Recognition.

(a) **Arrest photo databases.—**

(1) **General.** [A state/Any] investigative or law enforcement officer shall not use targeted face recognition in conjunction with an arrest photo database except as provided in this section.

(2) **Permitted uses.** [A state/Any] investigative or law enforcement officer may use targeted face recognition in conjunction with an arrest photo database maintained pursuant to paragraph (3)—

(A) To identify any person whom the officer encounters under circumstances which reasonably indicate that the person has committed, is committing or is about to commit a criminal offense;

(B) To identify any person whom the officer reasonably suspects has committed, is committing or is about to commit an offense punishable by imprisonment for more than one year.

(3) The custodian of an arrest photo database used by an investigative or law enforcement officer in conjunction with targeted face recognition shall, every six months, eliminate from that database photos of persons—

(A) Released without a charge;

(B) Released after charges are dropped or dismissed or a nolle prosequi notice is entered; or

(C) Not convicted of the charged offense.

(b) **Identification Photo Databases.**[300]—

(1) **General.** Any investigative or law enforcement officer, state or federal, shall not use targeted face recognition in conjunction with [a state/an] identification photo database except as provided in this section.

(2) **Permitted uses.** An investigative or law enforcement officer, state or federal, may use targeted face recognition in conjunction with [a state/an] identification photo database pursuant to an order issued under paragraph (2);

(3) **Orders.**—

(A) **Authority.** The principal prosecuting attorney of [the/any] State or any political subdivision thereof and any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure), is authorized to make an application to a [Name of State/State or federal] judge of competent jurisdiction for, and such judge may grant in conformity with subparagraph (C), an order authorizing the use of targeted face recognition in conjunction with a [a state/an] identification photo database [within the jurisdiction of that judge] to identify any person whom there is probable cause to believe has committed, is committing, or is about to commit an offense enumerated in subsections (1) and (2) of section 2516 of Title 18 of the U.S. Code.

(B) **Application.** Each application for an order authorizing the use of targeted face recognition in conjunction with a [state] identification photo database shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall indicate the applicant's authority to make such application. Each application shall include the following information:

[300] **Authors' note:** To *prohibit* the use of driver's license and ID photos for criminal face recognition searches, delete the text in this subsection and include in its place the following statement: "Any investigative or law enforcement officer, state or federal, shall not use targeted face recognition in conjunction with a [state] identification photo database, or acquire in bulk the photos in that database." To institute a truly total ban, even in emergency cases, you will also have to amend the exceptions set out at subsection (c). To *allow* limited use of these photos, include the language set out in subsection (b).

(i) The identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(ii) As full and complete description as possible of the person or persons that the officer seeks to identify;

(iii) A full and complete description of the photos or video portraying that person or persons that will be used to search the [state] identification photo database;

(iv) A full and complete statement as to whether or not other investigative procedures to identify that person or persons, including the use of targeted face recognition in conjunction with an arrest photo database, have been tried and failed or why they reasonably appear to be unlikely to succeed;

(v) The specific [state] identification photo database or databases to be searched[, and, in the case of a state identification photo database, a certification that the individuals portrayed in that database primarily reside within the jurisdiction of the judge].

(vi) The particular offense enumerated in subsections (1) and (2) of section 2516 of the U.S. Code that are being investigated; and

(vii) A full and complete statement of the facts and circumstances that provide the officer probable cause to believe that the person or persons have committed, are committing, or are about to commit that offense or offenses.

(C) **Issuance.—**

(i) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving the use of targeted face recognition in conjunction with [a state/an] identification photo database [within the jurisdiction of that judge], if the judge determines that—

(I) there is probable cause to believe that the person or persons described committed, are committing, or are about to commit a particular offense or offenses enumerated in subsections (1) and (2) of section 2516 of Title 18 of the U.S. Code; and

(II) normal investigative procedures, including the use of targeted face recognition in conjunction with an arrest photo database, have been tried and have failed or reasonably appear to be unlikely to succeed.

(ii) Each order authorizing or approving such use shall specify—

(I) The identity of the state or federal law enforcement agency authorized to conduct targeted face recognition, and of the officer authorizing the application;

(II) In as much detail as necessary, the person or persons that the officer seeks to identify;

(III) The photos or video portraying that person or persons that will be used to search the identification photo database;

(IV) The [state] identification photo database or databases to be searched; and

(V) The particular offense enumerated in subsections (1) and (2) of section 2516 of Title 18 of the U.S. Code that are being investigated.

(D) **Notice to the Public.** [The] State department[s] of motor vehicles shall post notices in conspicuous locations at all department driver licensing offices, make written information available to all applicants at department driver licensing offices, and provide information on the department[s'] web site[s] regarding [state] investigative or law enforcement officers' searches of driver's license and ID photos through targeted face recognition. The notices, written information, and online information must address how officers use and access targeted face recognition in criminal investigations.

(E) **Conforming Amendments.**[301]**—**[The Driver's Privacy Protection Act, section 2721 of Title 18 of the U.S. Code, shall be amended as follows—

(i) Insert after subparagraph (a)(2) the following subparagraph: "(3) a department-operated face recognition system, except as provided in subsection (c) of this section";

(ii) Insert at the end of subparagraph (b)(1) the following text: "but if the personal information or highly restricted personal information to be disclosed is a person's photograph to be used or enrolled in a law enforcement face recognition system, only on a case-by-case basis that does not involve the bulk transfer of persons' photographs to a state or federal law enforcement agency or a third party entity that will allow law enforcement to access those photographs for the purposes of face recognition"; and

[301] **Authors' note:** The federal government has a driver's privacy law (18 U.S.C. 2721); most states do, too. To prevent loopholes, that law has to be amended to ensure (1) that DMV face recognition systems only allow law enforcement to search or request searches of their face recognition systems pursuant to this statute; and (2) that law enforcement agencies do not transfer, in bulk, the photos in those systems to themselves or a third party. The language below amends the *federal* driver's privacy law to achieve that objective. For state bills, the state driver's privacy law *will* need to be amended in a similar manner.

(iii) Insert after subsection (b) the following section: "(c) Law Enforcement Access to Face Recognition Systems.— A State department of motor vehicles, and any officer, employee, or contractor thereof, may make available a department-operated face recognition system to a state or federal law enforcement agency, or perform searches of such a system on behalf of the agency, only pursuant to an order issued under subparagraph (b)(3) of Title 1 of the Face Recognition Act, or pursuant to the exceptions enumerated in subsection (c) of that Act."]

(c) **Emergencies and exceptions.—**

(1) Notwithstanding subsections (a) and (b), [a state/an] investigative law enforcement officer may use targeted face recognition in conjunction with an arrest photo database, and an investigative law enforcement officer, state or federal, may use targeted face recognition in conjunction with a [state] identification photo database—

(A) To identify any person who is deceased, incapacitated or otherwise physically unable of identifying himself;

(B) To identify a minor whom the officer believes, in good faith, is the subject of an AMBER Alert, as that term is used in section 5791 of Title 42 of the U.S. Code;

(C) To identify any person who has been lawfully arrested, during the process of booking that person after an arrest or during that person's custodial detention; or

(D) To conduct targeted face recognition in conjunction with [a state/an] identification photo database to identify any person—

(i) if the principal prosecuting attorney of [the/any] State or any political subdivision thereof, or any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) determines that an emergency situation exists that involves—

(I) immediate danger of death or serious physical injury to any person; or

(II) conspiratorial activities threatening the national security interest.

that requires the use of targeted face recognition in conjunction with an identification photo database to occur before an order authorizing such use can, with due diligence, be obtained; and

(ii) there are grounds upon which an order could be entered under this chapter to authorize such use.

(2) If an investigative or law enforcement officer uses targeted face recognition pursuant to subparagraph (D) above, he shall apply for an order approving the use under paragraph (b)(3) above within forty-eight hours after the use occurred. The use shall immediately terminate when the application for approval is denied, or in the absence of an application, within forty-eight hours.

Section 102. Continuous Face Recognition.[302]

(a) **General.** [A state/any] investigative or law enforcement officer shall not use continuous face recognition [within the State] except as provided in this section.

(b) **Permitted uses.** [A state/any] investigative or law enforcement officer may use continuous face recognition pursuant to an order issued under paragraph (2);

(1) **Authority.** The principal prosecuting attorney of [the/any] State or any political subdivision thereof [, and the Attorney General of the United States, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division specially designated by the Attorney General,] is authorized to make an application to a [Name of State/state or federal] judge of competent jurisdiction for, and such judge may grant in conformity with paragraph (5), an order authorizing the use of continuous face recognition within [the State/that judge's jurisdiction] in conjunction with a emergency watchlist.

(2) **Application.** Each application for an order authorizing continuous face recognition shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(A) The identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(B) The number of persons on the emergency watchlist;

(C) As full and complete description as possible of the person or persons on the emergency watchlist, or their identities, if known, and the photos or video through which they have been enrolled on the emergency watchlist;

(D) A full and complete description of the nature and specific locations within [the State/the judge's jurisdiction] where continuous face recognition will be performed;

[302] **Authors' note:** To *prohibit* the use of continuous face recognition, delete the text in this section and include in its place the following statement: "(a) General.—[A state/any] investigative or law enforcement officer shall not use continuous face recognition [within the State]." To institute a truly total ban, even in emergency cases, you will also have to amend the exceptions set out at subsection (c). To *allow* limited use of continuous face recognition, include the language set out below.

(E) A statement of the period of time for which the continuous face recognition is required to be maintained;

(F) A full and complete statement as to whether or not other investigative procedures to locate the person or persons on the emergency watchlist have been tried and failed or why they reasonably appear to be unlikely to succeed;

(G) The particular offense involving the immediate danger of death that are being investigated;

(H) A full and complete statement of the facts and circumstances that—

(i) provide the officer probable cause to believe that the person or persons have committed, are committing, or are about to commit that offense or offenses; and

(ii) give reason to believe that an emergency situation exists that requires the use of continuous face recognition without delay;

(I) Where the application is for the extension of an order, a statement setting forth the results thus far obtained from the continuous face recognition, or a reasonable explanation of the failure to obtain such results.

(J) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) **Issuance.—**

(A) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving the use of continuous face recognition within [the State/that judge's jurisdiction] in conjunction with a emergency watchlist, if the judge determines that—

(i) there is probable cause to believe that the specific person or persons on the emergency watchlist committed, are committing, or are about to commit a particular offense involving the immediate danger of death;

(ii) normal investigative procedures to locate the person or persons on the emergency watchlist, have been tried and have failed or reasonably appear to be unlikely to succeed; and

(iii) an emergency situation exists that requires the use of continuous face recognition without delay.

(B) Each order authorizing or approving such use shall specify—

(iv) The identity of the law enforcement agency authorized to conduct continuous face recognition, and of the officer authorizing the application;

(v) In as much detail as necessary, the person or persons on the emergency watchlist, or their identities, if known, and the photos or video through which they have been enrolled on the emergency watchlist;

(vi) The nature and specific locations within [the State/the judge's jurisdiction] where continuous face recognition will be performed;

(vii) The particular offense that is being investigated; and

(viii) The period of time during which such continuous face recognition is authorized.

(C) No order entered pursuant to this paragraph may authorize or approve continuous face recognition for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than 7 days. Extensions of an order may be granted, but only upon application for an extension made in accordance with paragraph (4) of this section and the court making the findings required by subparagraph (5)(A) of this section.

(D) Whenever an order authorizing continuous face recognition is entered pursuant to paragraph (5), the order may require reports to be made to the judge who issued the order showing what progress has been made toward the achievement of the authorized objective and the need for ongoing continuous face recognition. Such reports shall be made at such intervals as the judge may require.

(c) **Emergencies and exceptions.**

(1) Notwithstanding subsections (a) and (b), [a state/any] investigative law enforcement officer may use continuous face recognition in conjunction with a emergency watchlist if—

(A) the principal prosecuting attorney of [the/any] State or any political subdivision thereof [, or the Attorney General of the United States, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division specially designated by the Attorney General,] determines that—

(i) an emergency situation exists that involves immediate danger of death to any person;

(ii) that requires the use of continuous face recognition in conjunction with a emergency watchlist before an order authorizing such use can, with due diligence, be obtained; and

(B) there are grounds upon which an order could be entered under this chapter to authorize such use.

(2) If [a state/an] investigative or law enforcement officer uses continuous face recognition pursuant to subparagraph (1) above, he shall apply for an order approving the use under paragraph (b)(2) above within forty-eight hours after the use occurred or began. The use shall immediately terminate when the application for approval is denied, or in the absence of an application, within forty-eight hours.

Section 103. Civil Rights and Civil Liberties. [A state/an] investigative or law enforcement officer shall not—

(a) use face recognition to create a record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual for whom the record is created or unless pertinent to and within the scope of an authorized law enforcement activity; or

(b) rely on actual or perceived race, ethnicity, national origin, religion, gender, gender identity, or sexual orientation in selecting which person to subject to face recognition, except when there is trustworthy information, relevant to the locality and timeframe, that links a person with a particular characteristic described in this subsection to an identified criminal incident or scheme.

Section 104. Logging of Searches. [A state/a] law enforcement agency whose investigative or law enforcement officers use face recognition shall log its use of the technology to the extent necessary to comply with the public reporting and audit requirements of sections 105 and 106 of this Act.

Section 105. Public Reporting.

(a) In January of each year, any judge who has issued an order under subparagraph (b)(3)(C) of section 101 of this Act or an order (or extension thereof) under paragraph (b)(3) of section 102 of this Act in the preceding calendar year, or who has denied approval of an application for such orders or extensions during that period, shall report to [the chief judge of the highest court of the State/the Administrative Office of the United States Courts]—

(1) the fact that an order or extension was applied for;

(2) whether the order or extension was issued pursuant to subparagraph (b)(3)(C) of section 101 of this Act, or paragraph (b)(3) of section 102 of this Act;

(3) the fact that the order or extension was granted as applied for, was modified, or was denied;

(4) the offense specified in the order or application, or extension of an order;

(5) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application;

(6) for orders issued pursuant to subparagraph (b)(3)(C) of section 101 of this Act, the [state] identification photo database that was searched;

(7) for orders issued pursuant to subparagraph (b)(3) of section 102 of this Act—

(A) the number of persons in the emergency watchlist;

(B) the nature and specific locations [within the State] where continuous face recognition was performed; and

(C) the period of time during which continuous face recognition was performed.

(b) In March of each year, the principal prosecuting attorney for [the/a] State, or the principal prosecuting attorney for any political subdivision of [the/a] State [, and the Attorney General, an Assistant Attorney General specially designated by the Attorney General], shall report to [the chief judge of the highest court of the State/the Administrative Office of the United States Courts], with respect to the preceding calendar year—

(1) For the use targeted face recognition in conjunction with an arrest photo database—

(A) the number of such searches run;

(B) the offenses that those searches were used to investigate;

(C) the arrests that resulted from such searches, and the offenses for which arrests were made;

(D) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained; and

(E) the number of motions to suppress made with respect to those searches, and the number granted or denied.

(2) For orders granted under subparagraph (b)(3)(C) of section 101 for targeted face recognition in conjunction with [a state/an] identification photo database, for each order—

(A) the information specified in paragraphs (1) through (6) of subsection (a); and

(B) the information specified in subparagraphs (B) through (E) of paragraph (1) in this subsection;

(3) For orders or extensions of orders granted under paragraph (b)(3) of section 102 for continuous face recognition, for each order—

(A) the information specified in paragraphs (1) through (5) and (7) of subsection (a); and

(B) the information specified in subparagraphs (B) through (E) of paragraph (1) in this subsection.

(c) In June of each year [the chief judge of the highest court of the State/the Administrative Office of the United States Courts] shall release to the public and transmit to [the State Legislature/the Congress] a full and complete report concerning the use of targeted and continuous face recognition in conjunction with arrest photo databases, [state] identification databases, and emergency watchlists, including—

(1) the number of applications for orders or extensions authorizing or approving targeted face recognition in conjunction with [a state/an] identification photo database or continuous face recognition in conjunction with an emergency watchlist and the number of orders and extensions granted or denied pursuant to this Act during the preceding calendar year.

(2) a summary and analysis of the data required to be filed with [the chief judge of the highest court of the State/the Administrative Office of the United States Courts] by subsections (a) and (c) of this section and sections 105 and 106 of this Act.

(d) The [the chief judge of the highest court of the State/the Administrative Office of the United States Courts] is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (a) and (c) of this section and sections 105 and 106 of this Act.

Section 106. Audits. Any [state] law enforcement agency whose [state] investigative or law enforcement officers use targeted or continuous face recognition, regardless of whether they use a system operated by that agency or another agency, shall annually audit that use to prevent and identify misuse and to ensure compliance with sections 101, 102, and 103 of this Act, and shall report—

(a) a summary of the findings of the audit, including the number and nature of violations identified, to [the chief judge of the highest court of the State/the Administrative Office of the United States Courts]; and

(b) any violations identified to [the principal prosecuting attorney for the State/the Attorney General].

Section 107. Accuracy and Bias Testing.

(a) Any [state] law enforcement agency whose [state] investigative or law enforcement officers operate a system of targeted or continuous face recognition shall regularly submit that system to independent testing to determine—

(1) the accuracy of the system; and

(2) whether the accuracy of the system varies significantly on the basis of race, ethnicity, gender or age.

(b) A summary of the findings of the tests required by subsection (a) shall be submitted to the [the chief judge of the highest court of the State/the Administrative Office of the United States Courts].

Section 108. Enforcement.

(a) **Suppression.** Whenever targeted or continuous face recognition has occurred, no results from those searches and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the use of face recognition violated sections 101, 102 or 103 of this Act.

(b) **Administrative Discipline.** If a court or law enforcement agency determines that an investigative or law enforcement officer has violated any provision of this Act, and the court or agency finds that the circumstances surrounding the violation raise serious questions about whether or not the officer acted willfully or intentionally with respect to the violation, the agency shall promptly initiate a proceeding to determine whether disciplinary action against the officer is warranted.

(c) **Civil Action.**

(1) **In General**. Any person who is subject to identification or attempted identification through targeted continuous face recognition in violation of this Act may in a civil action recover from the state or federal law enforcement agency which engaged in that violation such relief as may be appropriate.

(2) **Relief**. In an action under this subsection, appropriate relief includes—

(i) such preliminary and other equitable or declaratory relief as may be appropriate;

(ii) damages under subsection (d) and punitive damages in appropriate cases; and

(iii) a reasonable attorney's fee and other litigation costs reasonably incurred.

(2) **Computation of Damages**. The court may assess as damages whichever is the greater of—

(i) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(ii) statutory damages of whichever is the greater of $500 a day for each day of violation or $50,000;

(3) **Defense**. A good faith reliance on—

(i) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization; or

(ii) a good faith determination that subsection (c) of section 101 or subsection (c) of section 102 of this Act permitted the conduct complained of;

(iii) is a complete defense against any civil or criminal action brought under this chapter or any other law.

(4) **Limitation.** A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

Title II. Funding for Law Enforcement Face Recognition Systems and Research

Section 201. Law Enforcement.[303]

(a) No [state/federal] financial assistance or funds may be expended for the creation, maintenance, or modification of a law enforcement face recognition system unless the agency operating that system—

(1) certifies compliance with sections 104, 106 and 107 of this Act;

(2) certifies that the algorithm employed by its face recognition system has been submitted for testing in the most recent Face Recognition Vendor Test administered by the National Institute of Standards and Technology;

(3) provides documentation to confirm that the agency has posted online a use policy governing its use of face recognition and has secured approval for that policy from a city council or other body primarily comprised of elected officials.

(b) Subsection (a) shall take effect 18 months after the enactment of this Act, except for paragraph (2) of that subsection, which shall take effect five years after enactment.

[**Section 202. The National Institute for Standards and Technology**

(a) The National Institute of Standards and Technology (NIST) shall—

(1) Develop best practices for law enforcement agencies to evaluate the accuracy of their face recognition systems;

[303] **Authors' Note:** This section (1) uses the power of the purse to condition federal or state funding for law enforcement face recognition on agencies adopting measures to ensure transparency and accountability; and, in the case of federal legislation, (2) authorizes additional funding for the National Institute of Standards and Technology. Appropriations legislation is highly complex; this language will have to be adapted to the state in which it is offered. Furthermore, these provisions, particularly section 201, may best function as stand-alone amendments to *other* funding legislation. If these subsections are indeed offered as "riders," additional provisions may be added that incorporate some of the protections of sections 101, 102 and 103 of this legislation.

(2) Offer biennial Face Recognition Vendor Tests to evaluate the accuracy of face recognition algorithms;

(3) Develop, and implement as part of Face Recognition Vendor Tests, evaluations of whether the accuracy of a face recognition algorithm varies on the basis of race, ethnicity, gender or age; and

(4) Develop large, high-quality publicly available datasets of facial images to support NIST accuracy and bias testing and similar testing conducted by independent entities.

(b) There is authorized to be appropriated to the National Institute of Standards and Technology to carry out subsection (a) $_____ for each of the fiscal years 2018, 2019, 2020 and 2021.]

XII. MODEL FACE RECOGNITION USE POLICY

1. Purpose.

a. To establish procedures for the acceptable use of the images, information, and tools within the face recognition system.[304]

2. Background.

a. Face recognition refers to an automated process of matching face images utilizing algorithms and biometric scanning technologies.[305]

b. This face recognition system was established [date] in conjunction with [other agency partners, if applicable]. The system helps identify possible criminal suspects or unidentified victims.[306]

c. Personnel from the following agencies can request face recognition searches:

i. [List; date of last update to list]

3. Scope.

a. This policy applies to all law enforcement personnel who are granted direct access to the face recognition system as well as personnel who are permitted to request face recognition searches. Any outside agency, or personnel from an outside agency, requesting face recognition assistance with an investigation must adhere to this policy.[307]

4. Database and Data Limitations.

a. The face recognition system runs searches against a database of mug shots that is updated twice per year to eliminate profiles of individuals who were not charged, had charges against them dropped, or who were found not guilty. Profiles of individuals whose records have been expunged are also removed immediately upon expungement.[308]

---

[304] Based on: Michigan State Police, *Statewide Network of Agency Photos (SNAP) Acceptable Use Policy*, Document p. 011436.
[305] Based on: SANDAG, *ARJIS Acceptable Use Policy for Facial Recognition* (Feb. 13, 2015), Document p. 008448.
[306] Based on: Honolulu Police Department, *Policy: Facial Recognition Program* (Sept. 14, 2015), Document p. 014704.
[307] Based on: *Seattle Police Manual, Booking Photo Comparison Software* (Feb. 19, 2014), Document p. 009907.
[308] Based on: Michigan State Police, *Interview with Peter Langenfeld, Program Manager, Digital Analysis and Identification Section* (May 25, 2016) (describing the practice of MSP to remove individuals not charged or found not guilty from the face recognition system in accordance with MCL § 28.243. Notes on file with authors).

b. No other databases, such as driver's licenses photo databases, are linked to or accessible via the face recognition system.[309]

c. Probe photos are the images of unknown suspects or victims that are submitted for comparison against the mug shot database. Probe photos are not enrolled into the face recognition database.

    i. **Unsolved Photo File.** A probe photo of an unknown suspect *may* be added to an unidentified photo file if there is probable cause to believe that suspect has committed a felony. Photos in this file are searched against new mug shot enrollments and future face recognition probe photos in an attempt to identify the photo suspect. Once the individual has been identified, the image shall be removed from the file.[310]

d. There is no interface of the face recognition system to any form of video surveillance, including surveillance cameras, drone footage, and body worn cameras.[311] The system will not be configured to conduct real-time or near-real-time face recognition analysis on live video.

e. Potential matches returned by the face recognition system are to be considered investigative leads only, and cannot be used as the sole basis for an arrest.

Acceptable Uses of Face Recognition.

1. **Field Identification (mobile searches).** Face recognition may be used on a mobile device as an identification tool by an officer in the field in one of three instances:

    a. When an individual consents to have his or her photograph taken for the purpose of identification.

        i. If consent is withdrawn, use of face recognition is not authorized and its use must stop immediately.[312]

    b. When the officer reasonably believes an individual is concealing his or her true identity *and* has reasonable suspicion the individual has committed a crime other than concealing his or her identity.

        i. An officer must first attempt to ascertain the individual's identity by means other than face recognition, such as requesting identification.

    c. When an individual is unable to provide reliable identification due to physical incapacitation or defect, mental incapacitation or defect, or death, and immediate

[309] Based on: SANDAG, *ARJIS Acceptable Use Policy for Facial Recognition* (Feb. 13, 2015), Document p. 008450.
[310] Based on: Pennsylvania JNET, *JNET Facial Recognition User Guide* (Dec. 4, 2014), Document p. 010907.
[311] Based on: SANDAG, *ARJIS Acceptable Use Policy for Facial Recognition* (Feb. 13, 2015), Document p. 008450.
[312] Based on: Albuquerque Police Department, *Procedural Orders: Facial Recognition Technology*, Document pp. 009202–009203.

identification is needed to assist the officer in performance of his or her lawful duties.[313]

Field photographs shall be taken and stored or deleted in accordance with the relevant department policies and procedures.

2. **Investigative Searches.** Face recognition may be used as an investigative tool to identify suspects caught on camera committing a felony. Investigative searches may be conducted in one of two instances:

    a. When an officer has reasonable suspicion that the suspect to be searched has committed a felony.

    b. When the suspect to be searched is believed to be a victim of a crime.

    Investigative searches shall only be conducted by trained Face Examiners. Face Examiner refers to an individual who has received advanced training in the face recognition system and its features. Examiners have at least a working knowledge of the limitations of face recognition and the ability to use image editing software. They are qualified to assess image quality and appropriateness for face recognition searches and to perform one-to-many and one-to-one face image comparisons.

    Examiners determine if images are suitable for face recognition searches, and may enhance images for the purpose of conducting a face recognition search. Though enhancements to the probe image are permissible, the examiner shall not base any conclusions on a comparison between an enhanced image and a potential candidate image. All human comparison shall take place between the original unknown image and the potential candidate image.

    Examiners shall submit the conclusions of their analyses for peer review for investigative leads resulting from one-to-many searches and both peer review and administrative review for one-to-one comparisons. Examiners shall return a maximum of two images to the requesting officer or agency to be used as investigative leads only.[314]

3. **Arrest.** Face recognition may be used upon the arrest of an individual to identify that individual and/or determine whether he or she has previously been arrested and charged with a crime. Since the probe photo is also a mug shot, it may be enrolled in the face recognition database, but must be removed if the individual is never charged or convicted, or if the record is expunged.

Face Recognition Privacy Protections and Oversight.

1. **Constitutional Guarantees.**

    a. Face recognition is uniquely powerful investigative and identification tool. Law enforcement officers shall not employ this technology to conduct dragnet

[313] Based on: Michigan State Police, *Statewide Network of Agency Photos (SNAP) Acceptable Use Policy*, Document p. 011438.
[314] This section describing the role of Facial Examiners is based on: Michigan State Police, *Best Practice Guidelines for Facial Recognition and Facial Comparison* (Feb. 2, 2014), Document pp. 011323–011331.

screening of individuals, nor shall they use it to facilitate mass surveillance of places, groups or activities unless doing so furthers an official law enforcement activity and is conducted in accordance with this policy.

i. For example, it would not be appropriate for officers to use face recognition technology to conduct surveillance of persons or groups based solely on their religious, political or other constitutionally protected activities,[315] or their race, ethnicity, gender, or sexual orientation.

b. Face recognition must be used in accordance with all federal and state laws, and all departmental policies, including those addressing improper racial profiling.[316]

2. Training.

a. All personnel who are authorized to run a field identification (mobile) search or request an investigative search shall be trained in the following areas prior to utilizing face recognition:

i. The proper and lawful use of face images for face recognition purposes;

ii. How to take high quality face images in the field for most accurate results;

iii. The appropriate use and sharing of information obtained from a face recognition search;

iv. The deletion of a field identification probe image used for comparison.

b. Personnel who have not received this training shall not utilize face recognition or request an investigative search.[317]

3. Audits and Penalties for Misuse.

a. All face recognition use and search requests are subject to audit. In the event of an audit, the user will be required to provide appropriate justification for the use or request of a face recognition search.

Appropriate justification shall include a situation description and purpose for the search, including a detailed account of circumstances amounting to reasonable suspicion, and a case/complaint number and file class/crime type, if available. For searches conducted on behalf of another individual, the name and rank/job title of other individual requesting the search shall also be included.[318]

[315] Ohio Bureau of Criminal Investigation, *OHLEG Rules and Regulations*, 1.11: Facial Recognition (July 1, 2016), Document p. 009218.
[316] Based on: Albuquerque Police Department, *Procedural Orders: Facial Recognition Technology*, Document p. 009203.
[317] Based on: *San Diego Police Department Procedure* (June 19, 2015), Document p. 013761.
[318] Based on: Michigan State Police, *Statewide Network of Agency Photos (SNAP) Acceptable Use Policy*, Document p. 011439.

b. Penalties for misuse that may be imposed include, but are not limited to, termination of a user's access to the face recognition system or the termination of agency-wide access to the system.[319]

4. Approvals and Transparency.

This policy shall be reviewed annually by [City Council or other body primarily comprised of elected officials]. The policy, and any updates to it, shall be made publicly available.[320]

[319] Based on: Michigan State Police, *Statewide Network of Agency Photos (SNAP) Acceptable Use Policy*, Document p. 011439.
[320] Based on: SANDAG, *ARJIS Acceptable Use Policy for Facial Recognition* (Feb. 13, 2015), Document p. 008453.

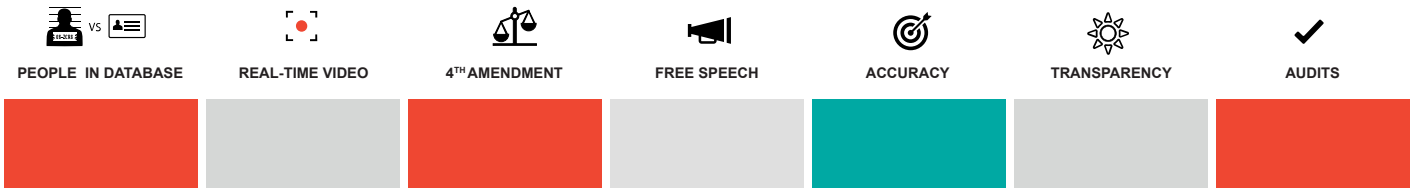
JURISDICTION

FEDERAL BUREAU OF INVESTIGATION FACE SERVICES UNIT

The FBI can search 411 million photos, including 24.9 million mug shots, 140 million visa photos and over 185 million state driver's license and ID photos.

The FBI does not require reasonable suspicion to run a search.

The FBI has searched state license and ID databases over 36,000 times but has not audited those searches for misuse.



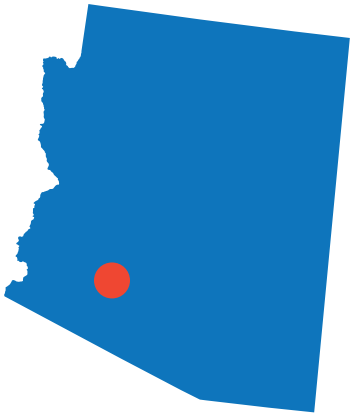
The Facial Analysis, Comparison, and Evaluation (FACE) Services Unit runs face recognition searches for other FBI divisions and federal partners. FACE Services can search or request searches of 411 million photos, including 24.9 million mug shots, over 140 million visa photos and over 185 million state driver's license and ID photos in: Alabama; Arkansas; Delaware; Illinois; Iowa; Kentucky; Michigan; Nebraska; New Mexico; North Carolina; North Dakota; South Carolina; Tennessee; Texas; Utah; and Vermont (GAO). In total, almost one in three U.S. drivers' photos can be searched by FACE Services.

The FBI does not require reasonable suspicion to run a search; searches can be run in cases where "allegation or information" indicates possible criminal activity (FBI). While the FBI has not evaluated the accuracy of the state face recognition systems it relies on, this is partially offset by the fact that search results are manually reviewed by a FACE Services specialist before the top one or two candidate photos are sent to the requesting FBI agent as a potential lead (GAO). In a March 2015 Privacy Impact Assessment, the FBI asserted that audit procedures were in place to prevent misuse (FBI). A summer 2016 GAO investigation found that in the previous four and a half years, the FBI had not, in fact, audited its use of these databases (GAO).

Sources: FBI FACE Services Privacy Impact Assessment, GAO (*Last updated: September 2016*)

JURISDICTION

MARICOPA COUNTY SHERIFF'S OFFICE (MCSO)



Police can search 14.5 million driver's license and ID photos, 3.2 million mug shots, and other databases.

Police are not required to have reasonable suspicion to run a search.

In 2007, Maricopa County enrolled all driver's license photos and mug shots from Honduras in its databases.

The Maricopa County Sheriff's Office first purchased a face recognition system in 2006 (015026). MCSO can search 14.5 million Arizona driver's license photos, 3.2 million Arizona mug shots, and other databases, such as the DOJ's Federal Joint Automated Booking System, which contains another 1.5 million booking photos (014954). In 2007, MCSO also enrolled all Honduran driver's license and booking photos, provided by the Honduran government. (015058). Reasonable suspicion is not required for the MCSO to run a face recognition search (014949). African Americans are likely overrepresented in the system; they are arrested in Arizona at a rate 143% higher than their population share.

A specialized Facial Recognition Unit (FRU) runs the searches. Reviewers are instructed to "review the results and identify possible leads" and receive supervisor approval before returning possible leads to the requester (014963–014964). There are no records of any audits being conducted on the system (014949). The Arizona Department of Public Safety previously submitted face recognition search requests to the FRU, but in response to our records request indicated that it has not done so since 2013 (010717).

We understand that MCSO uses a system initially provided by Hummingbird Defense Systems, but it is unclear if this is the current provider, as well as what algorithm the system uses (014976).

Sources: Maricopa County Sheriff's Office, Arizona Department of Public Safety, U.S. Census (*Last updated: September 2016*)

JURISDICTION

ARKANSAS STATE POLICE (ASP)

Police can search 24.9 million mug shots in the FBI database.

The FBI can search 15.4 million driver's license and ID photos.

ASP stated it "does not currently use" face recognition technology.

The Arkansas State Police (ASP) can search 24.9 million mug shot photos in the FBI's face recognition database, known as the Next Generation Identification Interstate Photo System, or NGI-IPS (GAO). According to a 2016 report by the Government Accountability Office, the FBI can also request searches of Arkansas' 15.4 million driver's license and ID photos (GAO).

In response to our public records request, ASP stated it "does not currently use" face recognition technology (000100).

Sources: ASP, GAO (*Last updated: September 2016*)

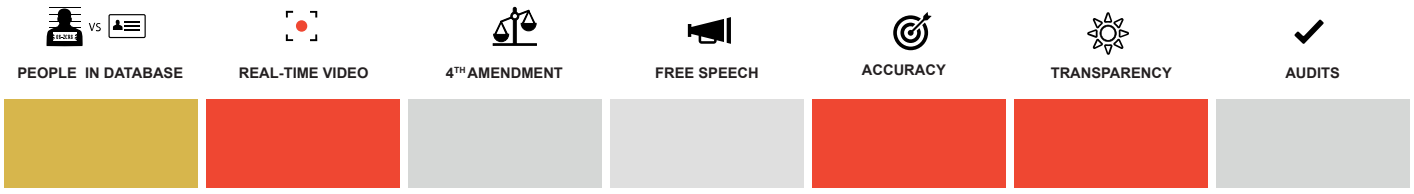
JURISDICTION

LOS ANGELES POLICE DEPARTMENT (LAPD) & LOS ANGELES COUNTY SHERIFF'S DEPARTMENT (LACSD)

The LAPD has publicly reported use of real-time face recognition, but found "no records responsive" to our public records request.

Police in Los Angeles County can run face recognition searches of mug shots.

It's unclear if police are required to have reasonable suspicion to run a search.



The Los Angeles Police Department (LAPD) may have the most advanced face recognition system in the country—yet refused to comply with our public records request. In 2013, it announced a system that could perform real-time face recognition from 600 feet using CCTV cameras in the West San Fernando Valley. In 2007, LAPD said that a "smart car" would be equipped with face recognition. In 2005, LAPD announced a CCTV camera system "equipped with 'intelligent' video capabilities and facial recognition software." Yet in response to a request for documents relating to its use of face recognition, LAPD stated that it has "no records responsive to [the] request" (000102).

The Los Angeles County Sheriff's Department (LACSD) has a face recognition system accessible on desktop and via emails sent from mobile devices (000623). LACSD has no publicly available policy governing when it is appropriate for police to use the face recognition, and provided no such policy in response to our request. It is possible that it does not exist.

The LACSD system searches mug shots "of all subjects criminally booked within Los Angeles County" (000349), but it's unclear what other databases are accessible, how many mug shots are enrolled in the system, or if LACSD "scrubs" its mug shot database to eliminate people who were never charged, had charges dropped or dismissed, or who were found innocent. African Americans are likely overrepresented in the system; they are arrested at a rate 176% higher than their share of the county population.

The LACSD system uses NEC and Cognitec algorithms (000444). We do not know what algorithms are employed by the LAPD systems.

Sources: LAPD, LACSD, State of California Department of Justice Office of the Attorney General, U.S. Census (*Last updated: September 2016*)

JURISDICTION

SAN DIEGO ASSOCIATION OF GOVERNMENTS (SANDAG)

Police can run face recognition searches of 1.4 million mug shots.

License photo searches are prohibited, as is real-time video-based face recognition.

Police need reasonable suspicion to run a search.

SANDAG's use policy must be reviewed and approved annually by local elected officials.

The San Diego Association of Governments (SANDAG) runs the Tactical Identification System (TACIDS) face recognition system. At least 66 agencies have access to the system, at least 28 of which currently run searches (013762, 005699). TACIDS searches a database of 1.4 million mug shots (008449), but does not allow searches of license photos or real-time face recognition from video feeds (016621). TACIDS is accessible by mobile devices used by officers in the field, and primarily designed for identification of arrestees, detainees, and the incapacitated—not after-the-fact investigations (016619–016620, 008389). Officers need reasonable suspicion to run a search (005723). The system use policy is public and must be approved annually by local elected officials (008453).

The system is not without concerns. SANDAG contracted with a face recognition company, FaceFirst, which claims to have "the industry's finest" technology, including an algorithm provided by Cognitec "[w]ith an identification rate above 95%." However, that statistic is a decade old, and in its contracts with SANDAG, FaceFirst repeatedly disclaims any liability for "representations or warranties as to the accuracy" of its face recognition system (008358, 008493). According to the Acceptable Use Policy, SANDAG member agencies, not SANDAG, are responsible for conducting audits—but at least one member agency, the Carlsbad Police Department, reported no audits (008452, 000149).

African Americans are likely overrepresented in the system; in San Diego County, they're arrested at a rate 202% higher than their population share.

Sources: SANDAG, FaceFirst, NIST, California Office of the California Attorney General, U.S. Census (*Last updated: September 2016*)

San Francisco Police Department (SFPD)

- Police can search half a million to one million mug shots.
- It's unclear if officers are required to have reasonable suspicion to run a search.
- SFPD required vendor companies to submit their algorithms to accuracy testing and meet accuracy thresholds.

People in Database	Real-Time Video	4th Amendment	Free Speech	Accuracy	Transparency	Audits
2	0	0	0	2	3	0

The San Francisco Police Department (SFPD) purchased an Automatic Biometric Identification System (ABIS) in 2010. ABIS is a multi-biometric system that includes face recognition capabilities. SFPD can search between half a million to one million mug shots (005501, 005543). It is unclear if reasonable suspicion is required for SFPD to run a search, or if SFPD can search for witnesses and bystanders. SFPD has no publicly available policy governing when it is appropriate for police to use face recognition, and provided no such policy in response to our request. It is possible that it does not exist.

During the contracting process for its multi-biometric system, SFPD included requirements that vendor companies submit their face recognition algorithms to accuracy testing and that their algorithms meet specific accuracy thresholds. The Request for Proposal (RFP) states that on-site tests will be conducted and that "[a]fter system acceptance, accuracy tests will continue to run on a regular basis to reconfirm system performance and detect any degradation" (005557).

African Americans are likely overrepresented in the system; they are arrested at a rate 185% higher than their share of the city population.

The SFPD system uses an algorithm provided by 3M Cogent (005591).

Read the documents →

Sources: San Francisco Police Department, State of California Department of Justice Office of the Attorney General, U.S. Census (*Last updated: September 2016)*

JURISDICTION

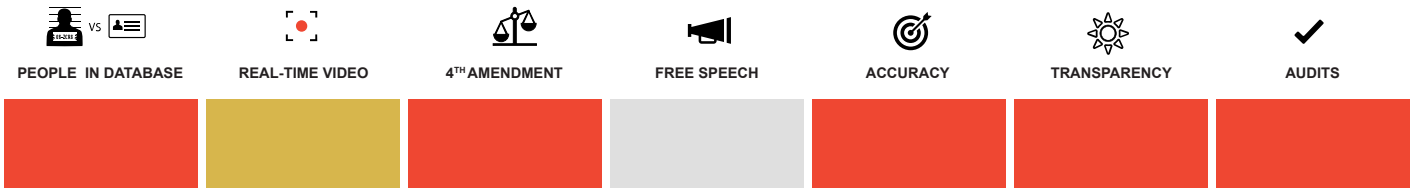
FLORIDA & PINELLAS COUNTY SHERIFF'S OFFICE (PCSO)

Police can run face recognition searches of 22 million Florida driver's license and ID photos, over 11 million mug shots and other photos, and 24.9 million mug shots in the FBI database.

FBI field offices in Florida can search the Pinellas County database, including license and ID photos.

Police and the FBI are not required to have reasonable suspicion to run a search.

Florida's database is searched 8,000 times per month. Searches are not audited for misuse.



In 2001, the Pinellas County Sheriff's Office (PCSO) launched the Face Analysis Comparison & Examination System (FACES) (013980). It searches over 33 million faces, including 22 million Florida driver's license and ID photos and over 11 million law enforcement photos (014736, 014739). Florida law enforcement can also search the FBI's database of 24.9 million mug shots (GAO).

The FBI has not signed an MOU to let its FACE Services unit search the system. In an apparent workaround, FBI's Florida field offices can search PCSO's system and are among the 243 local, state, and federal agencies that run close to 8,000 searches per month (014396). Asked if PCSO audits searches for misuse, Sheriff Bob Gualtieri replied, "No, not really." The Pinellas County Public Defender's Office reports that PCSO has never disclosed use of face recognition in Brady evidence.

FACES users aren't required to have reasonable suspicion to run a search. The manual encourages officers to use biometric identification "whenever practical" (014375). The system does not allow real-time face recognition from video, but this is not codified in its use manuals.

FACES uses a MorphoTrust algorithm (013791).

Sources: PCSO, Interviews (Sheriff Gualtieri, Public Defender Dillinger), GAO, Washington Post (*Last updated: September 2016*)

Honolulu Police Department & Hawaii Criminal Justice Data Center (CJDC)

- Police can search mug shots.
- Police generally need reasonable suspicion to run a search, with exceptions.
- Hawaii is one of four agencies we received records from that has made its use policy public.

People in Database	Real-Time Video	4th Amendment	Free Speech	Accuracy	Transparency	Audits
2	0	2	2	1	2	3

The Honolulu Police Department's (HPD) face recognition program was established in 2014 in conjunction with the Hawaii Criminal Justice Data Center (CJDC) (014704). In 2015, the system was expanded to all counties in Hawaii, and accesses a statewide database of mug shot photos. Driver's license photos are not included in the database; Hawaii has determined that current statutes, rules, and regulations prohibit driver's license and ID photos from being included in the face recognition system (016846). African Americans are likely overrepresented in the database; they are arrested at a rate 111% higher than their share of Hawaii's population.

HPD requires that police have reasonable suspicion to run a face recognition search, with an exception for "requests that come directly from the Chief" (016851). Searches are also permitted to identify deceased persons. It is unclear if police can run searches of bystanders or witnesses. Only staff who have completed face recognition training are permitted to access the system, and potential matches are manually reviewed by an analyst from the Crime Analysis Unit (014705, 014707). If no match is found in HPD's system, a requester can send the image to the FBI to be run against its database of 24.9 million mug shots (014706). Hawaii signed a Memorandum of Understanding with the FBI in 2011 to participate in its face recognition pilot.

HPD is one of four agencies we received responsive records from that has made its use policy public. CJDC stated it does not maintain audit records, and email correspondence with HPD indicates it maintains no records aside from the use policy, which suggests that no audits are conducted (015310, 016615).

The HPD face recognition system uses a Morpho algorithm (016851).

Read the documents →

Sources: HPD, CJDC, State of Hawaii Department of the Attorney General, U.S. Census (*Last updated: September 2016*)

JURISDICTION

CHICAGO POLICE DEPARTMENT (CPD)

CPD can run face recognition searches of mug shots.

The FBI can run face recognition searches of 43 million Illinois driver's license photos.

It's unclear if police are required to have reasonable suspicion to run a search.

In 2012, CPD requested funding for real-time face recognition. It's unclear if CPD runs real-time searches.

The Chicago Police Department (CPD) uses face recognition, but limits public information on how it is used. CPD has no public policy governing law enforcement use of face recognition. As of August 2016, phone calls to follow up on public records requests were directed to a full voicemail account that provides no further contact information. CPD can run face recognition searches against a mug shot database (008686). It's unclear if police are required to have reasonable suspicion to run a search, and if the CPD "scrubs" its mug shot database to eliminate people who were never charged, had charges dropped or dismissed, or were ultimately found innocent. According to a 2016 report by the Government Accountability Office, the FBI can request face recognition searches of 43 million Illinois driver's license and ID photos (GAO). It's unclear whether CPD can run searches against these photos.

In 2012, CPD requested $2 million to support real-time video-based face recognition (008725). They also bought an exceptionally large amount of network hardware and spent $450,000 on enterprise-class database and computing infrastructure (008671–008685). It's unclear if they currently run face recognition searches against real-time or archival video.

CPD uses a DataWorks Plus face recognition system, but it is unclear which algorithm that system uses.

Sources: CPD, GAO (*Last updated: September 2016*)

IOWA DEPARTMENT OF PUBLIC SAFETY (DPS)

Police can run face recognition searches of 13 million Iowa driver's license and ID photos.

The FBI can request searches of 13 million driver's license and ID photos.

Police need reasonable suspicion to run a search.

The Iowa Department of Public Safety has not finalized a face recognition use policy.

Iowa's face recognition system is owned by the Iowa Department of Transportation (DOT). In 2014, the Iowa Department of Public Safety (DPS) signed an agreement with the DOT, wherein the DPS would pay for an upgrade to the DOT's face recognition system and in exchange gain access to it (008661). This agreement allows authorized DPS personnel to run face recognition searches on Iowa's 13 million driver's licenses and other DOT photos. According to a 2016 report by the Government Accountability Office, the FBI can also request searches of Iowa's driver's license photos (GAO).

According to DPS, personnel need reasonable suspicion of criminal activity before running a face recognition search (016853). However, DPS "has not yet adopted a final policy" governing law enforcement face recognition searches on the grounds that it is waiting to determine "what uses may be accurate or inaccurate, reliable or unreliable, appropriate or inappropriate" (016854, 011911).

The DOT system uses a MorphoTrust face recognition algorithm (008661).

Sources: DPS, GAO (*Last updated: September 2016*)

MAINE STATE POLICE

Police can search 24.9 million mug shots in the FBI NGI database.

* The Cumberland County Sheriff's Office used to use face recognition.

? A state records request is in process.

Maine State Police can search 24.9 million mug shots in the FBI's Next Generation Identification-Interstate Photo System (NGI-IPS) database (GAO). This database contains mug shots and corresponding fingerprint records submitted by various state and federal agencies.

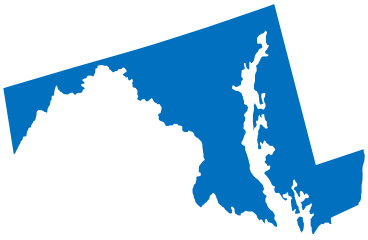
The Cumberland County Sheriff's Office (CCSO) previously used face recognition, beginning in August 2012. When in use, the Cumberland County Sheriff could search all Cumberland County jail booking photos on file, dating back to 1998 (010631).

The CCSO system used a face recognition system provided by Dynamic Imaging, but it is unclear which company provided the algorithm used (010634).

Sources: GAO, Cumberland County Sheriff's Office (*Last updated: September 2016*)

JURISDICTION

MARYLAND DEPARTMENT OF PUBLIC SAFETY & CORRECTIONAL SERVICE



Police can run face recognition searches of over 7 million Maryland driver's license and ID photos, over 3 million Maryland mug shots, and FBI's database of 24.9 million mug shots.

In June 2016, GAO reported that the FBI was negotiating to search Maryland license photos.

Police likely need probable cause to run a search.

Maryland's face recognition system has not been audited since its launch in 2011.

In 2011, the Maryland Department of Public Safety and Correctional Services (DPSCS) began running face recognition searches on mug shots. In 2013, it enrolled photos from the Maryland Motor Vehicle Administration into the database, a measure that does not appear to have received any media coverage. The database, the Maryland Image Repository System (MIRS), includes over 7 million driver's license and other MVA photos and over 3 million mug shots of "known offenders" (011105). Maryland law enforcement can also request searches of the FBI's mug shot database of 24.9 million photos. Many Maryland law enforcement agencies can access MIRS, including the Maryland State Police and the Baltimore City Police Department (010949). The system is also open to agencies outside of Maryland. African Americans are likely overrepresented in the system; in Maryland, they are arrested at a rate 75% higher than their population share. It's unclear if the DPSCS "scrubs" its mug shot database to eliminate people who were never charged, had charges dropped or dismissed, or who were found innocent.

Based on a DPSCS fact sheet, it appears searches of the system require probable cause (011104). However, DPSCS did not produce a use policy in response to our records request. In addition, according to DPSCS, "[t]he MIRS system "has not been audited" in its five years of operation (008906).

The DPSCS system uses NEC and Cognitec face recognition algorithms (008892).

Sources: DPSCS, GAO, Maryland State Police, U.S. Census (*Last updated: September 2016*)

MICHIGAN STATE POLICE (MSP)

Police can run face recognition searches of 41 million Michigan driver's license and ID photos, 4 million mug shots, and FBI's database of 24.9 million mug shots.

The FBI can request searches of at least 35.6 million Michigan license photos and mug shots.

Police need probable cause to run a search on mobile devices, but just a "law enforcement reason" for running desktop searches.

The Michigan State Police runs the Statewide Network of Agency Photos (SNAP), a database of 4 million mug shots and 41 million driver's license and ID photos from the Michigan Department of State. The FBI can request searches of at least 35.6 million of Michigan's driver's license and ID photos (GAO). African Americans are likely overrepresented in SNAP; they're arrested at a rate 136% higher than their state population share.

Officers can run searches from a desktop computer or a mobile device. Trained examiners run desktop searches and potential matches are peer reviewed; results from mobile searches are not peer reviewed (011467–011468). MSP's face recognition use policy, which it has made public, requires that an officer have probable cause before running a mobile search. Desktop searches are only required to be for a "law enforcement reason" (016824). Searches can be run to identify criminal suspects, witnesses, bystanders, victims, unknown decedents, and the incapacitated (010928, 011345, 016824).

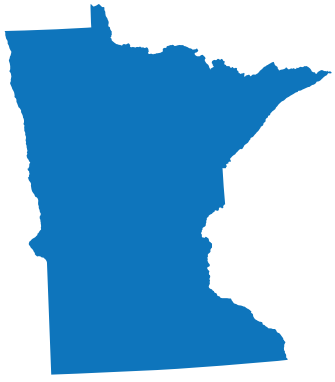
MSP does not use face recognition with real-time video. In accord with Michigan law (MCL 28.243.2), the MSP deletes from its database mug shots and fingerprints of people who are arrested but never charged or are ultimately not convicted. Unlike any other agency in our survey, the MSP provided documentation that their audit regime was functional.

The MSP system uses Cognitec and NEC face recognition algorithms.

Sources: Michigan State Police, GAO, U.S. Census MCL 28.243.2 (*Last updated: September 2016*)

JURISDICTION

MINNESOTA DEPARTMENT OF PUBLIC SAFETY (DPS)



Police can run face recognition searches on mug shots.

In June 2016, GAO reported that the FBI was negotiating to search Minnesota's license photos.

Police are not required to have reasonable suspicion to run a search.

The Minnesota Department of Public Safety's (DPS) Bureau of Criminal Apprehension (BCA) purchased a PictureLink system from Dynamic Imaging to run face recognition searches of the Minnesota Repository of Arrest Photos (MRAP), primarily to generate mug shot photo lineups for criminal investigations (016860). Police do not need reasonable suspicion to run a search. DPS stated it does not currently use the PictureLink system's face recognition, however, because it "does not function in a satisfactory manner" (012103). African Americans are likely overrepresented in MRAP database; they are arrested at a rate 494% higher than their share of the state population.

Driver and Vehicles Services (DVS), a division of the DPS, also operates a face recognition system for de-duplicating driver's license photos and identifying possible fraud (008924). DPS stated that this system cannot be accessed by agencies outside the DVS division (012103).

DPS uses a Dynamic Imaging face recognition system, but it is unclear which algorithm the system employs.

Sources: DPS, GAO, U.S. Census (*Last updated: August 2016*)

NEBRASKA STATE PATROL (NPS)

Police can run face recognition searches of 8 million Nebraska driver's license and ID photos.

The FBI can search 8 million driver's license and ID photos.

Police can run searches only to assist with identity theft investigations.

System access by police is restricted to four analysts.

In 2014, the Nebraska State Police (NSP) signed a Memorandum of Understanding (MOU) with the Nebraska Department of Motor Vehicles (DMV). This grants NSP use of the DMV's face recognition system, which searches 8 million driver's license and ID photos (009190). The FBI can also request searches of Nebraska's driver's license photos (GAO).

In accordance with the MOU, NSP can run searches only for criminal identity theft investigations. System access is restricted to four analysts (009190). The NSP follows procedures dictated by the DMV, and does not have its own policies, procedures, or manuals. NSP does not conduct audits; according to the NSP, the DMV is responsible for conducting any audits of the system (009181).

In 2012, NSP also signed an MOU with the FBI for access to its pilot face recognition database, the Interstate Photo System Facial Recognition Pilot (IPSFRP) (009183). This allowed NSP to search FBI's database of 24.9 million mug shots submitted by various state and federal agencies.

The DMV system uses a MorphoTrust face recognition algorithm (011954).

Sources: Nebraska State Police, GAO (*Last updated: August 2016*)

Lincoln Police Department (LPD)

- Police can run face recognition searches of 8 million driver's license and ID photos.
- Police are not required to have reasonable suspicion to run a search.
- LPD stated it has a use policy but claimed it is exempt from disclosure under Nebraska's public records law.

People in Database	Real-Time Video	4th Amendment	Free Speech	Accuracy	Transparency	Audits
3	0	3	0	0	3	2

In 2013, the Lincoln Police Department (LPD) signed a Memorandum of Understanding (MOU) with the Nebraska Department of Motor Vehicles (DMV) (009175). This grants LPD use, for a four-year term, of the DMV's face recognition system, which searches 8 million driver's license and ID photos. Because LPD does not have its own face recognition system, it is unlikely it can search mug shots.

The MOU permits LPD to use face recognition for identity theft investigations and "for investigation of criminal activity" more generally, unlike the MOU between the Nebraska State Patrol and the DMV, which limits police searches to identity-related crimes only (009175, 009190). LPD does not need reasonable suspicion to run a search; the MOU states searches may be run "for a case being investigated and/or prosecuted in a criminal manner" (009175).

In response to our public records request, LPD stated it has a use policy, but claimed it is exempt from disclosure under Neb. Rev. Stat. 84-712.05(5) (009171).

The DMV system uses a MorphoTrust face recognition algorithm (011947).

Read the documents →

Sources: Lincoln Police Department (*Last updated: September 2016*)

New Mexico Department of Public Safety (DPS)

- Police can search 24.9 million mug shots in the FBI's database.
- The FBI can search New Mexico's 2.9 million driver's license and ID photos.
- The Department of Public Safety never responded to our records request.

People in Database	Real-Time Video	4th Amendment	Free Speech	Accuracy	Transparency	Audits
0	0	0	0	0	3	0

The New Mexico Department of Public Safety can search 24.9 million mug shots in the FBI's Next Generation Identification Interstate Photo System (NGI-IPS) database (GAO). This database contains mug shots and corresponding fingerprint records submitted by various state and federal agencies.

The FBI can also request searches of New Mexico's 2.9 million driver's license photos (GAO). A 2014 DOJ-funded publication by the Police Executive Research Forum reported that police can run face recognition searches on the driver's license photo database as well, although we have not been able to independently verify that. The New Mexico Department of Public Safety never responded to our public records request, filed in January 2016.

Read the documents →

Sources: GAO (*Last updated: September 2016*)

Sources: Lincoln Police Department (*Last updated: September 2016*)

Albuquerque Police Department (APD)

- Police can search 200,000 APD mug shots.
- Police need probable cause or consent to run a search.
- It appears that APD does not audit its face recognition system for misuse or abuse.

People in Database	Real-Time Video	4th Amendment	Free Speech	Accuracy	Transparency	Audits
2	0	2	0	1	3	3

The Albuquerque Police Department (APD) can search a mug shot database of more than 200,000 APD booking photos. The APD uses a Universal Facial Workstation (UFW) software platform provided by the FBI, which uses a Morpho algorithm (009202).

The APD face recognition procedural order, which the Department has not made public, states: “An officer shall have probable cause for an arrest (to include charges other than Concealing Identity) prior to submitting an image for Facial Recognition unless voluntary consent is obtained” (009202). Only authorized personnel of the Real Time Crime Center are allowed to run face recognition searches. Possible matches are considered investigative leads only and cannot be the sole basis for an arrest or detention (009203). The procedural order also states that when using face recognition, officers must adhere to department policies on improper or racial profiling (009203).

It is unclear if African Americans are overrepresented in the face recognition database; recent arrest data that is disaggregated by race does not appear to be available for Albuquerque. It’s also unclear if APD “scrubs” its database to eliminate people who were never charged, had charges dropped or dismissed, or were found innocent. APD does not appear to conduct audits of face recognition use; in response to our request for documentation of audits, APD stated that it “does not exist.” (016700).

Read the documents →

Sources: APD, KRQE News 13 (*Last updated: September 2016*)

Ohio Bureau of Criminal Investigation (BCI)

- Police can search 24 million driver's license and ID photos and mug shots.
- FBI officials may be granted access to search 24 million driver's license photos and mug shots.
- Police are not required to have reasonable suspicion to run a search.
- Cincinnati Police stated it does not use face recognition.

People in Database	Real-Time Video	4th Amendment	Free Speech	Accuracy	Transparency	Audits
3	0	3	1	3	3	2

Ohio began a face recognition pilot program in 2008; its current statewide system went live in 2013 (015278, 015285). The system was almost entirely unknown to the public until a 2013 investigation by the Cincinnati Enquirer, which uncovered that the Bureau of Criminal Investigation (BCI) had enrolled all state driver's license photos with no notice to the public. Officers can also run searches against mug shot photos (015285). It is unclear if the mug shot database is "scrubbed" to eliminate people who were never charged, had charges dropped or dismissed, or who were found innocent. The Bureau of Criminal Investigation confirmed that the FBI—along with other law enforcement agents—may also access Ohio's database "based upon a stated need" (016842). When the system went live, it was reported that 30,000 police officers and court employees could access the system. In its first eight months of operation, 504 different agencies conducted 6,618 searches (015285). At present, 4,406 individuals can access the system, and in the first four months of 2016, 1,429 searches were conducted by 104 agencies. BCI stated that it regularly conducts audits of the agencies that use facial recognition (016843).

Police are not required to have reasonable suspicion to run a search, but are prohibited from using face recognition to "conduct dragnet screening of individuals" or to conduct surveillance based on constitutionally protected activity "unless doing so furthers an official law enforcement activity" (009218). Ohio's use policy has not been made public, though the Attorney General did establish an Advisory Board with community and civil rights group representatives to provide input on face recognition use and concerns (016843).

It appears that Ohio's system uses a 3M Cogent face recognition algorithm (009222).

Read the documents →

Sources: Attorney General's Office BCI, Ohio Rev. Code Ann. § 4501.27
(*Last updated: September 2016*)

PENNSYLVANIA JUSTICE NETWORK (JNET)

Police can run face recognition searches of over 34 million driver's license and ID photos and over 4 million mug shots.

In June 2016, GAO reported that the FBI was negotiating to search state license photos. GAO retracted that claim at the FBI's request.

It's unclear if police are required to have reasonable suspicion to run a search.

Police from over 500 agencies use the system.

The Pennsylvania Justice Network (JNET) manages the face recognition system used by police throughout Pennsylvania. The system is owned by the Pennsylvania Chiefs of Police Association; as a non-profit entity, however, it is not subject to the Freedom of Information Act, potentially making much of the information about face recognition use by Pennsylvania police unavailable to the public. The system launched in 2006. In 2013, it gained access to the state driver's license photo database (016734). In April 2014, the system could search over 34 million driver's license and other ID photos, and over four million mug shots (010750). The system is open "to any municipal, county, state or federal law enforcement agency" in the state; over 500 agencies use it (103787, 013785). JNET has not made its policy face recognition use available to the public. Its internal manual does not indicate if reasonable suspicion is required to run a search, but permits searches of witnesses (010845). JNET has stated that it conducts triennial audits of agencies with access to its system, but provided no records of such audits in response to our request (016857, 010955–010956).

The system has been used for public surveillance. In Cheltenham Township, "[o]fficers took photos of the attendees in the parking lot" at the court hearing of an alleged gang member, and used face recognition to identify "other gang members" (016738). African Americans are likely overrepresented in the database; they are arrested at a rate 192% higher than their share of the state population.

The JNET system uses Cognitec, NEC, and MorphoTrust algorithms.

Sources: JNET, GAO, Pennsylvania State Police, Pennsylvania Uniform Crime Reporting System, U.S. Census (*Last updated: September 2016*)

Texas Department of Public Safety (DPS)

- Police can search 24.9 million mug shots in FBI's database and 24 million driver's license and ID photos.
- It is unclear if police are required to have reasonable suspicion to run a search.
- FBI can search 24 million driver's license and ID photos.
- Dallas Transit Police are planning to acquire real-time face recognition in late 2016.

People in Database	Real-Time Video	4th Amendment	Free Speech	Accuracy	Transparency	Audits
3	0	0	0	0	3	0

The Texas Department of Public Safety (DPS) purchased a face recognition system in 2005, following the passage of a law requiring the DPS to establish an image verification system for driver's licenses (009310, Tex. Code Ann. § 521.059). This system searches 24 million driver's license and ID photos. DPS can also search 24.9 million mug shots in the FBI's database, the Next Generation Identification Interstate Photos System, or NGI-IPS (GAO). The FBI's FACE Services unit can request searches of the state's 24 million driver's license and ID photos (GAO).

Texas state law requires the DPS face recognition system to be used to aid law enforcement agencies in "conducting an investigation of criminal conduct" (Tex. Code Ann. § 521.059). It is unclear if law enforcement agencies need reasonable suspicion to run a search. In response to our public records request, DPS did not provide a policy specifically regarding the use of face recognition technology.

In February 2016, Dallas Area Rapid Transit (DART) announced plans to deploy real-time face recognition. In response to our public records request, DART indicated that procurement is in its early stages, and no responsive records exist yet (011102). The Dallas Police Department, El Paso Police Department, San Antonio Police Department, and Fort Worth Police Department reported that they do not use face recognition technology.

The initial DPS face recognition system was purchased from Digimarc; it is unclear which company provides the current system or algorithm (009310).

Read the documents →

Sources: Texas DPS, Tex. Code Ann. § 521.059, GAO, Dallas Area Rapid Transit, Fort Worth Police Department (*Last updated: September 2016*)

Vermont

- FBI can search 1.8 million Vermont driver's license and ID photos.
- FBI searches may conflict with a state law that prohibits the use of biometric identification on DMV records.
- Vermont State Police stated it does not use face recognition.

People in Database	Real-Time Video	4th Amendment	Free Speech	Accuracy	Transparency	Audits
3	0	3	0	1	0	3

In response to our public records request, Vermont State Police has stated it does not use face recognition technology (013790). However, according to a 2016 report by the Government Accountability Office, the FBI's FACE Services unit can request face recognition searches of Vermont's 1.8 million driver's license and ID photos (GAO). Since the FBI submits searches to be run by the responsible state agency, this would appear to indicate that the Vermont Department of Motor Vehicles (DMV) has implemented a face recognition system that searches state driver's license photos (GAO).

The DMV face recognition system, and its use by the FBI, may conflict with Vermont state law, which states that the DMV "shall not implement any procedures or processes for identifying applicants for licenses . . . that involve the use of biometric identifiers." (Vt. Stat. Ann. Tit. 23, § 634).

Read the documents →

Sources: GAO, Vermont State Police, Vt. Stat. Ann. Tit. 23, § 634.
(*Last updated: August 2016)*

Virginia State Police (VSP)

- Police can search 1.2 million mug shots.
- Police are not required to have reasonable suspicion to run a search.
- The system can be accessed by all law enforcement agencies in the state on request; audits are not conducted.

People in Database	Real-Time Video	4th Amendment	Free Speech	Accuracy	Transparency	Audits
2	2	3	0	3	3	3

The Virginia State Police (VSP) can run face recognition searches of 1.2 million Virginia mug shots using the VSP's Centralized Criminal Information System (CCIS) (015274). Mug shots are "retained indefinitely," which means VSP does not "scrub" its database to eliminate people who had charges dropped or dismissed except when records are expunged (015264, 016858). "Each criminal justice agency in Virginia" can access the system upon request (015303). Police are not required to have reasonable suspicion to run a search; use of the system is limited to "criminal justice purposes only" (015272). VSP does not conduct audits of how the system is used (015264, 016859).

African Americans are likely overrepresented in the system; statewide, they are arrested at a rate 108% higher than their share of Virginia's population.

VSP uses a DataWorks Plus face recognition system, which employs a NEC algorithm (016858).

Read the documents →

Source: VSP, U.S. Census (*Last updated: September 2016*)

Northern Virginia Regional Information System (NOVARIS)

- Police can search mug shots.
- It's unclear if police are required to have reasonable suspicion to run a search.
- Certified "examiner" status is required for fingerprint searches but not for face recognition searches.

People in Database	Real-Time Video	4th Amendment	Free Speech	Accuracy	Transparency	Audits
2	0	0	0	0	3	0

The Northern Virginia Regional Information System (NOVARIS), located in Fairfax County, is a regional arrest data and evidence sharing system. NOVARIS's face recognition component was acquired in 2007 and can be accessed by law enforcement in Maryland's Prince George's and Montgomery counties, Virginia's Arlington, Fairfax, Loudoun, and Prince William counties, and the cities of Alexandria, Fairfax, and Falls Church (015230). NOVARIS is also part of a face recognition partnership system established by the Pinellas County Sheriff's Office in Florida (015214). It is unclear how many mug shots are enrolled in the database, or if it is "scrubbed" to eliminate people who were never charged, had charges dropped or dismissed, or who were found innocent.

In its response to our public records request, Fairfax County Police indicated: "Only trained examiners who are certified and authorized to operate AFIS searches shall initiate cross-database searches within the AFIS databases," but there is no corresponding "certified examiner" requirement for access to face recognition (014710). This suggests that the required training and certification threshold is lower for officers running a face recognition search than for those running a fingerprint search. It is unclear if reasonable suspicion is required for police to run a search.

Read the documents →

Sources: Fairfax County Police Department (*Last updated: September 2016*)

Seattle Police Department (SPD) & South Sound 911

- Police can run face recognition searches of mug shots.
- Police are required to have reasonable suspicion to run a search.
- South Sound 911 requested real-time capabilities when contracting, but the Seattle PD has since banned such use.

People in Database	Real-Time Video	4th Amendment	Free Speech	Accuracy	Transparency	Audits
2	1	1	2	1	1	2

The Seattle Police Department runs its Booking Photo Comparison Software (BPCS) face recognition system through South Sound 911, an intergovernmental agency. Launched in 2014, it contains mug shots from Snohomish, King, and Pierce Counties, doesn't search driver's license and ID photos, and is accessible to at least eight regional law enforcement agencies (009378, 009826, 011900). The SPD Manual section on face recognition is publicly available online and requires reasonable suspicion to run a search. It does not allow searches of bystanders or witnesses (009907). The Seattle City Council conditioned funding for the system on the policy's review and approval by the ACLU of Washington (012666).

When South Sound 911 solicited face recognition vendors, they expressed a preference for a system with "the ability to do face recognition searches against live-feed video" (012048). A 2013 contract and invoices show that such a system was likely purchased (009790, 011078). The Seattle Police Department subsequently acquired the contract and ownership of the system, and has since *prohibited* the use of real-time video-based face recognition. (011078, 011082).

An FAQ for the system says that it "does not see race, sex, orientation or age" (009377). This contradicts a 2012 FBI co-authored study, and does not reflect the fact that African Americans are likely overrepresented in the system. In King County, for example, they are arrested at a rate 294% higher than their share of the population.

The BPCS system uses an NEC face recognition algorithm (012067).

Read the documents →

Sources: SPD, South Sound 911, King County, IEEE, U.S. Census
(*Last updated: September 2016*)

West Virginia Intelligence Fusion Center (WVIFC)

- The WVIFC bought real-time face recognition capabilities in 2012.
- Federal, state and local law enforcement officers can run face recognition searches of mug shots.
- It's unclear if officers are required to have reasonable suspicion to run a search.

People in Database	Real-Time Video	4th Amendment	Free Speech	Accuracy	Transparency	Audits
2	3	0	0	0	3	2

The West Virginia Intelligence Fusion Center (WVIFC) is operated by the state of West Virginia and runs advanced face recognition that is part of a system "open to all federal, state, county, and local agencies" (009944).

The system searches mug shot photos, but it's unclear what other databases are accessible, how many mug shots are enrolled in the system, and if the WVIFC "scrubs" its mug shot database to eliminate people who were never charged, had charges dropped or dismissed, or who were found innocent. The WVIFC has no publicly available policy governing law enforcement use of face recognition. The internal "Facial Recognition System Policy" is a page and a half long and does not require officers to have a reasonable suspicion before running a search (009959–009960).

In 2012, the WVIFC bought a real-time face recognition system that "[a]utomatically monitor[s] video surveillance footage and other video for instances of persons of interest" (009966). Previously, the WVIFC had told state officials that "automated video processing, search and detection capabilities could provide dramatic payoffs," and that "WVIFC requires a system with the following minimum capabilities: …Ability to automatically detect and extract faces from video" (009971–009972).

"Everyone refers to the *Minority Report*… about how they use facial recognition and iris recognition," said Thomas Kirk, the director of the WVIFC, in a recent interview. He added: "I actually think that that is the way of the future."

The WVIFC system was purchased from Tygart Technologies, but it is unclear which company provides the face recognition algorithm used.

Read the documents →

Sources: WVIFC, Tygart, *Vocativ* (*Last updated: August 2016*)