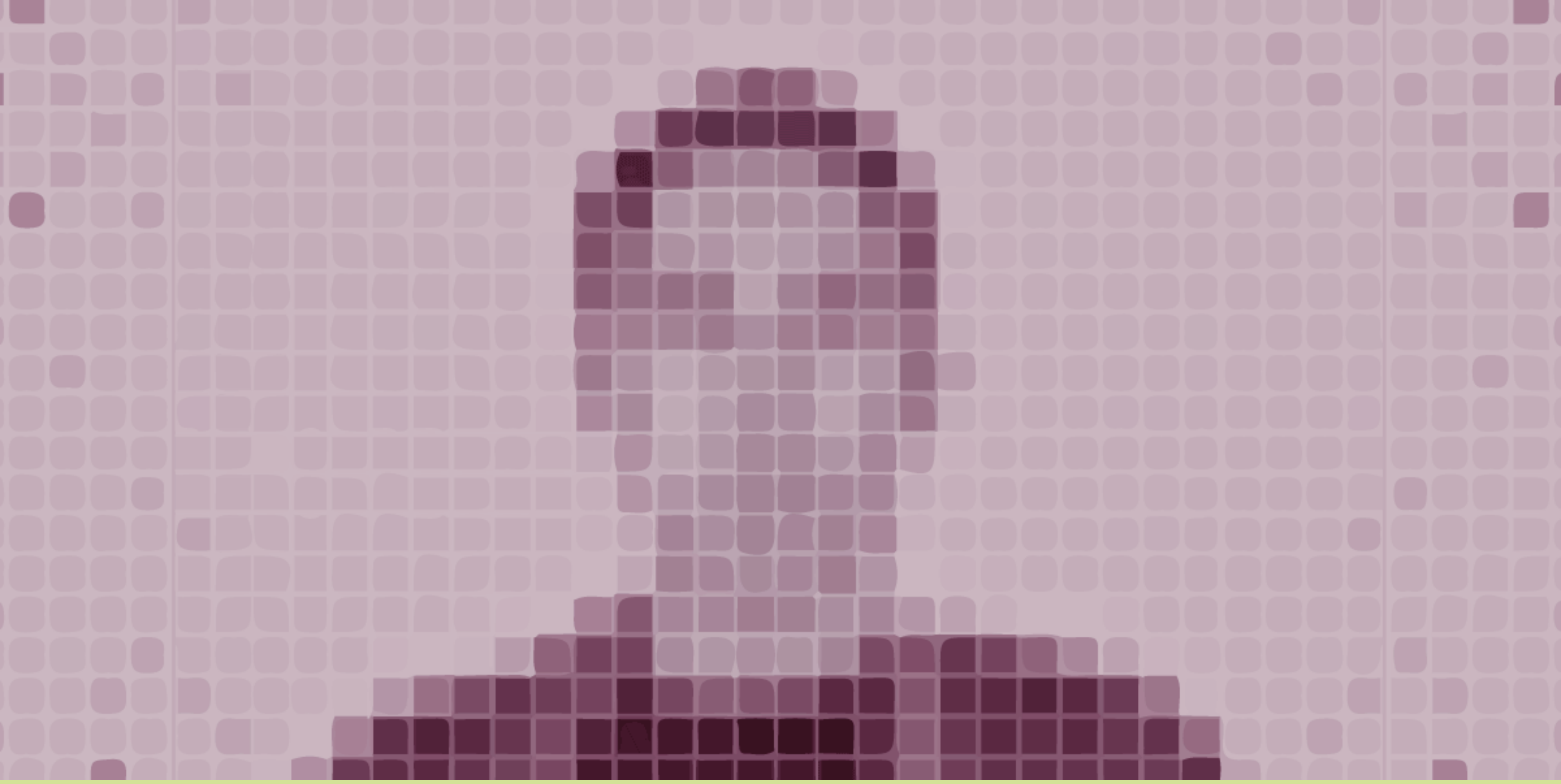


Face Off

LAW ENFORCEMENT USE OF FACE RECOGNITION TECHNOLOGY

by Jennifer Lynch, Senior Staff Attorney

ELECTRONIC FRONTIER FOUNDATION

FEBRUARY 2018

Author: Jennifer Lynch

Editor: Gennie Gebhart

With assistance from: Hugh D'Andrade, Sarah Glendon, Jason Kelley, Irene Lee, Dave Maass, Caroline Shen, Seth Schoen

View this report online: https://www.eff.org/wp/face-off

ELECTRONIC FRONTIER FOUNDATION

Contents

Face Off

LAW ENFORCEMENT USE OF FACE RECOGNITION TECHNOLOGY

Executive Summary

Face recognition is poised to become one of the most pervasive surveillance technologies, and law enforcement's use of it is increasing rapidly. Today, law enforcement officers can use mobile devices to capture face recognition-ready photographs of people they stop on the street; surveillance cameras boast real-time face scanning and identification capabilities; and federal, state, and local law enforcement agencies have access to hundreds of millions of images of faces of law-abiding Americans. On the horizon, law enforcement would like to use face recognition with body-worn cameras, to identify people in the dark, to match a person to a police sketch, or even to construct an image of a person's face from a small sample of their DNA.

However, the adoption of face recognition technologies like these is occurring without meaningful oversight, without proper accuracy testing of the systems as they are actually used in the field, and without the enactment of legal protections to prevent internal and external misuse. This has led to the development of unproven, inaccurate systems that will impinge on constitutional rights and disproportionately impact people of color.

Without restrictive limits in place, it could be relatively easy for the government and private companies to build databases of images of the vast majority of people living in the United States and use those databases to identify and track people in real time as they move from place to place throughout their daily lives. As researchers at Georgetown posited in 2016, one out of two Americans is already in a face recognition database accessible to law enforcement.[1]

This white paper takes a broad look at the problems with law enforcement use of face recognition technology in the United States. Part 1 provides an overview of the key issues with face recognition, including accuracy, security, and impact on privacy and civil rights. Part 2 focuses on FBI's face recognition programs, because FBI not only manages the repository for most of the criminal data used by federal, state, local, and tribal law enforcement agencies across the United States, but also provides direct face recognition services to many of these agencies, and its systems exemplify the wider problems with face recognition. After considering these current issues, Part 3 looks ahead to potential future face recognition capabilities and concerns. Finally, Part 4 presents recommendations for policy makers on the limits and checks necessary to ensure that law enforcement use of face recognition respects civil liberties.

Part 1 provides a brief introduction to how face recognition works before exploring areas in which face recognition is particularly problematic for law enforcement use, presenting the following conclusions:

- **When the uncertainty and inaccuracy inherent in face recognition technology inform law enforcement decisions, it has real-world impact.** An inaccurate system will implicate people for crimes they did not commit. And it will shift the burden onto defendants to show they are *not* who the system says they are.
- **Face recognition uniquely impacts civil liberties**. The accumulation of identifiable photographs threatens important free speech and freedom of associations rights under the First Amendment, especially because such data can be captured without individuals' knowledge.
- **Face recognition disproportionately impacts people of color**. Face recognition misidentifies African Americans and ethnic minorities, young people, and women at higher rates than whites, older people, and men, respectively.[2] Due to years of well-documented, racially biased police practices, all criminal databases—including mugshot databases—include a disproportionate number of African Americans, Latinos, and immigrants.[3] These two facts mean people of color will likely shoulder significantly more of the burden of face recognition systems' inaccuracies than whites.

- **The collection and retention of face recognition data poses special security risks.** All collected data is at risk of breach or misuse by external and internal actors, and there are many examples of misuse of law enforcement data in other contexts.[4] Face recognition poses additional risks because, unlike a social security number or driver's license number, we can't change our faces. Law enforcement must do more to explain why it needs to collect so much sensitive biometric and biographic data, why it needs to maintain it for so long, and how it will safeguard it from breaches.

Part 2 explores how FBI's face recognition programs exemplify these and other problems. FBI has positioned itself to be the central source for face recognition identification for not only federal but also state and local law enforcement agencies. FBI collects its own data, maintains data provided by state and local agencies, and facilitates access to face recognition data for more than 23,000 law enforcement agencies across the country and around the world. This makes it particularly important to look closely at FBI's system, as its issues are likely present in other law enforcement systems.

After describing **FBI's internal and external face recognition programs**—including the Next Generation Identification database and Interstate Photo System—and **access to external data**, Part 2 highlights three of FBI's most urgent failures related to face recognition:

- **FBI has failed to address the problem of face recognition inaccuracy.** The minimal testing and reporting conducted by FBI showed its own system was incapable of accurate identification at least 15 percent of the time. However, it refuses to provide necessary information to fully evaluate the efficacy of its system, and it refuses to update testing using the current, much larger database.
- **For years, FBI has failed to meet basic transparency requirements as mandated by federal law** about its Next Generation Identification database and its use of face recognition. The agency took seven years, for example, to update its Privacy Impact Assessment for its face recognition database, and failed to release a new one until a year after the system was fully operational.
- **The scope of FBI's face recognition programs is still unclear.** The public still does not have as much information as it should about FBI's face recognition systems and plans for their future evolution.

Part 3 looks toward face recognition capabilities and concerns on the horizon, including the use of face recognition with police body-worn cameras, crowd photos, and social media photos.

Finally, **Part 4** provides proposals for change. In particular, it provides a roadmap to policy makers considering face recognition legislation. It recommends concrete and specific technical and legal limits to place meaningful checks on government use of face recognition technology.

People should not be forced to submit to criminal face recognition searches merely because they want to drive a car. They should not have to worry their data will be misused by unethical government officials with unchecked access to face recognition databases. They should not have to fear that their every move will be tracked if face recognition is linked to the networks of surveillance cameras that blanket many cities. Without meaningful legal protections, this is where we may be headed.

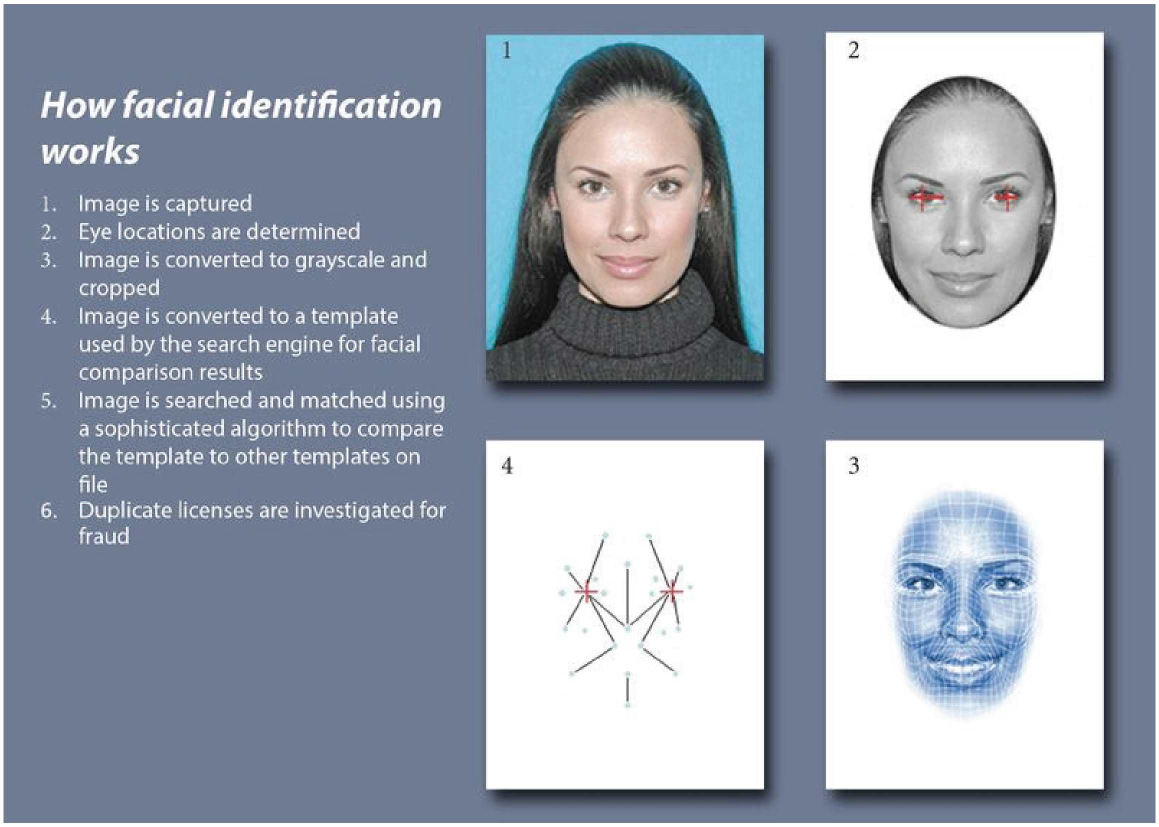
Want to learn more? For additional information on law enforcement use of technology, check out EFF's Street-Level Surveillance project. For more on face recognition and related technologies, visit our issue pages on face recognition and biometrics.

Part 1: How Does Face Recognition Work and What Are The Risks?

What is Face Recognition and How Does it Work?

Face recognition is a type of biometric identification. Biometrics are unique markers that identify or verify the identity of someone using their intrinsic physical or behavioral characteristics. Fingerprints are the most commonly known biometric, and they have been used regularly by criminal justice agencies to identify people for over a century. Other biometrics like face recognition, iris scans, palm prints, voice prints, wrist veins, a person's gait, and DNA are becoming increasingly common.

Face recognition systems use computer algorithms to pick out specific, distinctive details about a person's face from a photograph, a series of photographs, or a video segment. These details, such as the distance between the eyes or the shape of the chin, are then converted into a mathematical representation and compared to data on other faces previously collected and stored in a face recognition database. The data about a particular face is often called a "face template." It is distinct from a photograph because it is designed to only include certain details that can be used to distinguish one face from another.



How facial identification works

1. Image is captured
2. Eye locations are determined
3. Image is converted to grayscale and cropped
4. Image is converted to a template used by the search engine for facial comparison results
5. Image is searched and matched using a sophisticated algorithm to compare the template to other templates on file
6. Duplicate licenses are investigated for fraud

The data that comprises a face template is distinct from a photograph because it is designed to only include certain details that can be used to distinguish one face from another.
Source: Iowa Department of Transportation

Face recognition systems are generally designed to do one of three things. First, a system may be set up to identify an unknown person. For example, a police officer would use this type of system to try to *identify* an unknown person in footage from a surveillance camera. The second type of face recognition system is set up to *verify the identity* of a known person. Smartphones rely on this type of system to allow you to use face recognition to unlock your phone. A third type, which operates similarly to a verification system, is designed to *look for multiple specific, previously-identified faces*. This system may be used, for example, to recognize card counters at a casino, or certain shoppers in a store, or wanted persons on a crowded subway platform.

Instead of positively identifying an unknown person, many face recognition systems are designed to calculate a probability match score between the unknown person and specific face templates stored in the database. These systems will offer up several potential matches, ranked in order of likelihood of correct identification, instead of just returning a single result. FBI's system works this way.

Accuracy Challenges

Face recognition systems vary in their ability to identify people, and no system is 100 percent accurate under all conditions. For this reason, every face recognition system should report its rate of errors, including the number of false positives (also known as the "false accept rate" or FAR) and false negatives (also known as the "false reject rate" or FRR).

A "false positive" is generated when the face recognition system matches a person's face to an image in a database, but that match is incorrect. This is when a police officer submits an image of "Joe," but the system erroneously tells the officer that the photo is of "Jack."

A "false negative" is generated when the face recognition system fails to match a person's face to an image that is, in fact, contained in a database. In other words, the system will erroneously return zero results in response to a query. This could happen if, for example, you use face recognition to unlock your phone but your phone does not recognize you when you try to unlock it.

When researching a face recognition system, it is important to look closely at the "false positive" rate and the "false negative" rate, because there is almost always a trade-off. For example, if you are using face recognition to unlock your phone, it is better if the system fails to identify you a few times (false negative) than if it misidentifies other people as you and lets those people unlock your phone (false positive). Matching a person's face to a mugshot database is another example. In this case, the result of a misidentification could be that an innocent person is treated as a violent fugitive and approached by the police with weapons drawn or even goes to jail, so the system should be designed to have as few false positives as possible.

Technical issues endemic to all face recognition systems mean false positives will continue to be a common problem for the foreseeable future. Face recognition technologies perform well when all the photographs are taken with similar lighting and from a frontal perspective (like a mug shot). However, when photographs that are compared to one another contain different lighting, shadows, backgrounds, poses, or expressions, the error rates can be significant.[5] Face recognition is also extremely challenging when trying to identify someone in an image shot at low resolution[6] or in a video,[7] and performs worse overall as the size of the data set (the population of images you are checking against) increases, in part because so many people within a given population look similar to one another. Finally, it is also less accurate with large age discrepancies (for example, if people are compared against a photo taken of themselves when they were ten years younger).

Unique Impact on Civil Liberties

Some proposed uses of face recognition would clearly impact Fourth Amendment rights and First Amendment-protected activities and would chill speech. If law enforcement agencies add crowd, security camera, and DMV photographs into their databases, anyone could end up in a database without their knowledge—even if they are not suspected of a crime—by being in the wrong place at the wrong time, by fitting a stereotype that some in society have decided is a threat, or by engaging in "suspect" activities such as political protest in public spaces rife with cameras. Given law enforcement's history of misuse of data gathered based on people's religious beliefs, race, ethnicity, and political leanings, including during former FBI director J. Edgar Hoover's long tenure and during the years following September 11, 2001,[8]Americans have good reason to be concerned about expanding government face recognition databases.

Like other biometrics programs that collect, store, share, and combine sensitive and unique data, face recognition technology poses critical threats to privacy and civil liberties. Our biometrics are unique to each of us, can't be changed, and often are easily accessible. Face recognition, though, takes the risks inherent in other biometrics to a new level because it is much more difficult to prevent the collection of an image of your face. We expose our faces to public view every time we go outside, and many of us share images of our faces online with almost no restrictions on who may access them. Face recognition therefore allows for covert, remote, and mass capture and identification of images.[9] The photos that may end up in a database could include not just a person's face but also how she is dressed and possibly whom she is with.

Face recognition and the accumulation of easily identifiable photographs implicate free speech and freedom of association rights and values under the First Amendment, especially because face-identifying photographs of crowds or political protests can be captured in public, online, and through public and semi-public social media sites without individuals' knowledge.

2007-01-25 08:37:46, Ort: R
Matchscore: 0.859449
System: C-Vis

When law enforcement uses face recognition on crowd photographs of political gatherings or protests, documented "chilling effects" on First Amendment-protected speech can occur.
Source: https://www.eff.org/files/filenode/vorder_bruegge-facial-recognition-and-identification-initiatives_0.pdf

Law enforcement has already used face recognition technology at political protests. Marketing materials from the social media monitoring company Geofeedia bragged that, during the protests surrounding the death of Freddie Gray while in police custody, the Baltimore Police Department ran social media photos against a face recognition database to identify protesters and arrest them.[10]

Government surveillance like this can have a real chilling effect on Americans' willingness to engage in public debate and to associate with others whose values, religion, or political views may be considered different from their own. For example, researchers have long studied the "spiral of silence"— the significant chilling effect on an individual's willingness to publicly disclose political views when they believe their views differ from the majority.[11] In 2016, research on Facebook users documented the silencing effect on participants' dissenting opinions in the wake of widespread knowledge of government surveillance—participants were far less likely to express negative views of government surveillance on Facebook when they perceived those views were outside the norm.[12]

In 2013, a study involving Muslims in New York and New Jersey found that excessive police surveillance in Muslim communities had a significant chilling effect on First Amendment-protected activities.[13] Specifically, people were less inclined to attend mosques they thought were under government surveillance, to engage in religious practices in public, or even to dress or grow their hair in ways that might subject them to surveillance based on their religion. People were also less likely to engage with others in their community who they did not know for fear any such person could either be a government informant or a radical. Parents discouraged their children from participating in Muslim social, religious, or political movements. Business owners took conscious steps to mute political discussion by turning off Al-Jazeera in their stores, and activists self-censored their comments on Facebook.[14]

These examples show the real risks to First Amendment-protected speech and activities from excessive government surveillance—especially when that speech represents a minority or disfavored viewpoint. While we do not yet appear to be at point where face recognition is being used broadly to monitor the public, we are at a stage where the government is building the databases to make that monitoring possible. We must place meaningful checks on government use of face recognition now before we reach a point of no return.

Disproportionate Impact on People of Color

The false-positive risks discussed above will likely disproportionately impact African Americans and other people of color.[15] Research—including research jointly conducted by one of FBI's senior photographic technologists—found that face recognition misidentified African Americans and ethnic minorities, young people, and women at higher rates than whites, older people, and men, respectively.[16] Due to years of well-documented racially-biased police practices, all criminal databases—including mugshot databases—include a disproportionate number of African Americans, Latinos, and immigrants.[17] These two facts mean people of color will likely shoulder exponentially more of the burden of face recognition inaccuracies than whites.

False positives can alter the traditional presumption of innocence in criminal cases by placing more of a burden on suspects and defendants to show they are *not* who the system identifies them to be. This is true even if a face recognition system offers several results for a search instead of one; each of the people identified could be brought in for questioning, even if there is nothing else linking them to the crime. Former German Federal Data Protection Commissioner Peter Schaar has noted that false positives in face recognition systems pose a large problem for democratic societies: "[I]n the event of a genuine hunt, [they] render innocent people suspects for a time, create a need for justification on their part and make further checks by the authorities unavoidable."[18]

Face recognition accuracy problems also unfairly impact African American and minority job seekers who must submit to background checks. Employers regularly rely on FBI's data, for example, when conducting background checks. If job seekers' faces are matched mistakenly to mug shots in the criminal database, they could be denied employment through no fault of their own. Even if job seekers are properly matched to a criminal mug shot, minority job seekers will be disproportionately impacted due to the notorious unreliability of FBI records as a whole. At least 50 percent of FBI's arrest records fail to include information on the final disposition of the case: whether a person was convicted, acquitted, or if charges against them were dropped.[19] Because at least 30 percent of people arrested are never charged with or convicted of any crime, this means a high percentage of FBI's records incorrectly indicate a link to crime. If these arrest records are not updated with final disposition information, hundreds of thousands of Americans searching for jobs could be prejudiced and lose work. Due to disproportionately high arrest rates, this uniquely impacts people of color.

Security Risks Posed by the Collection and Retention of Face Recognition Data

All government data is at risk of breach and misuse by insiders and outsiders. However, the results of a breach of face recognition or other biometric data could be far worse than other identifying data, because our biometrics are unique to us and cannot easily be changed.

The many recent security breaches, email hacks, and reports of falsified data—including biometric data—show that the government needs extremely rigorous security measures and audit systems in place to protect against data loss. In 2017, hackers took over 123 of Washington D.C.'s surveillance cameras just before the presidential inauguration, leaving them unable to record for several days.[20] During the 2016 election year, news media were consumed with stories of hacks into email and government systems, including into United States political organizations and online voter registration databases in Illinois and Arizona.[21] In 2015, sensitive data stored in Office of Personnel Management (OPM) databases on more than 25 million people was stolen, including biometric information, addresses, health and financial history, travel data, and data on people's friends and neighbors.[22] More than anything, these breaches exposed the vulnerabilities in government systems to the public—vulnerabilities that the United States government appears to have known for almost two decades might exist.[23]

The risks of a breach of a government face recognition database could be much worse than the loss of other data, in part because one vendor—MorphoTrust USA—has designed the face recognition systems for the majority of state driver's license databases, federal and state law enforcement agencies, border control and airports (including TSA PreCheck), and the State Department. This means that software components and configuration are likely standardized across all systems, so one successful breach could threaten the integrity of data in all databases.

Vulnerabilities exist from insider threats as well. Past examples of improper and unlawful police use of driver and vehicle data suggest face recognition data will also be misused. For example, a 2011 state audit of law enforcement access to driver information in Minnesota revealed "half of all law-enforcement personnel in Minnesota had misused driving records."[24] In 2013, the National Security Agency's Inspector General revealed NSA workers had misused surveillance records to spy on spouses, boyfriends, and girlfriends, including, at times, listening in on phone calls. Another internal NSA audit revealed the "unauthorized use of data about more than 3,000 Americans and green-card holders."[25] Between

2014 and 2015, Florida's Department of Highway Safety and Motor Vehicles reported about 400 cases of improper use of its Driver and Vehicle Information Database.[26] And a 2016 Associated Press investigation based on public records requests found that "[p]olice officers across the country misuse confidential law enforcement databases to get information on romantic partners, business associates, neighbors, journalists and others for reasons that have nothing to do with daily police work."[27]

Many of the recorded examples of database and surveillance misuse involve male officers targeting women. For example, the AP study found officers took advantage of access to confidential information to stalk ex-girlfriends and look up home addresses of women they found attractive.[28] A study of England's surveillance camera systems found the mostly male operators used the cameras to spy on women.[29] In 2009, FBI employees were accused of using surveillance equipment at a charity event at a West Virginia mall to record teenage girls trying on prom dresses.[30] In Florida, an officer breached the driver and vehicle database to look up a local female bank teller he was interested in.[31] More than 100 other Florida officers accessed driver and vehicle information for a female Florida state trooper after she pulled over a Miami police officer for speeding.[32] In Ohio, officers looked through a law enforcement database to find information on an ex-mayor's wife, along with council people and spouses. [33] And in Illinois, a police sergeant suspected of murdering two ex-wives was found to have used police databases to check up on one of his wives before she disappeared.[34]

It is unclear what, if anything federal and state agencies have done to improve the security of their systems and prevent insider abuse. In 2007, the Government Accountability Office (GAO) specifically criticized FBI for its poor security practices. GAO found, "[c]ertain information security controls over the critical internal network reviewed were ineffective in protecting the confidentiality, integrity, and availability of information and information resources."[35] Given all of this—and the fact that agencies often retain personal data longer than a person's lifetime[36]—law enforcement agencies must do more to explain why they need to collect so much sensitive biometric and biographic data, why they need to maintain it for so long, and how they will safeguard the data from the data breaches we know will occur in the future.

Part 2: FBI's Face Recognition Databases and Systems

FBI's face recognition databases and systems—and the critical problems with them—shed light on broader issues with law enforcement use of face recognition. State and local law enforcement agencies across the country both provide and use much of the data that makes up FBI's main biometric database. With FBI acting as a national repository for law enforcement face recognition data, it is important to look closely at its flaws, in particular its inaccuracy, lack of transparency and oversight, and unclear scope.

Much of what we now know about FBI's use of face recognition comes from a scathing report issued in 2016 by the federal Government Accountability Office (GAO).[37] This report revealed, among other things, that FBI could access nearly 412 million images—most of which were taken for non-criminal reasons like obtaining a driver's license or a passport. The report chastised FBI for being less than transparent with the public about its face recognition programs and security issues.

FBI's Internal and External Access to Face Recognition Data

The Next Generation Identification Database and Interstate Photo System

FBI's Next Generation Identification system (NGI) is a massive biometric database that includes fingerprints, iris scans, and palm prints collected from millions of individuals, not just as part of an arrest, but also for non-criminal reasons like background checks, state licensing requirements, and immigration. The Interstate Photo System (IPS) is the part of NGI that contains photographs searchable through face recognition. Each of the biometric identifiers in NGI is linked to personal, biographic, and identifying information, and, where possible, each file includes multiple biometric identifiers. FBI has designed NGI to be able to expand in the future as needed to include "emerging biometrics," such as footprint and hand geometry, tattoo recognition, gait recognition, and others.[38]

NGI incorporates both criminal and civil records. NGI's criminal repository includes records on people arrested at the local, state, and federal levels as well as biometric data taken from crime scenes and data on missing and unidentified persons. NGI's civil repository stores biometric and biographic data collected from members of the military and those applying for immigration benefits. It also includes biometric data collected as part of a background check or state licensing requirement for many types of jobs, including, depending on the state, licensing to be a dentist, accountant, teacher, geologist, realtor, lawyer, or optometrist.[39] Since 1953, all jobs with the federal government have also required a fingerprint check, no matter the salary range or level of responsibility.[40]

As of December 2017, NGI included more than 74 million biometric records in the criminal repository and over 57.5 million records in the civil repository.[41] By the end of fiscal year 2016, it also already contained more than 51 million civil and criminal photographs searchable through face recognition.[42]

The states have been very involved in the development and use of the NGI database. NGI includes more than 20 million civil and criminal images received directly from at least six states, including California, Louisiana, Michigan, New York, Texas, and Virginia. Five additional states—Florida, Maryland, Maine, New Mexico, and Arkansas—can send search requests directly to the NGI database. As of December 2015, FBI was working with eight more states to grant them access to NGI, and an additional 24 states were also interested.[43]

In 2015, FBI announced that for the first time it would link almost all of the non-criminal data in NGI with criminal data as a "single identity record."[44] This means that, if a person submits fingerprints as part of their job search, those prints will be retained by FBI and searched, along with criminal prints, thousands of times a day[45] as part of investigations into any crime by more than 23,000 law enforcement agencies across the country and around the world.[46]

For the IPS, FBI has said—for now—that it is keeping non-criminal photographs separate from criminal photographs.[47] However, if a person is ever arrested for any crime—even for something as minor as blocking a street as part of a First Amendment-protected protest—their non-criminal photographs will be combined with their criminal record and will become fair game for the same face recognition searches associated with any criminal investigation.[48] As of December 2015, over 8 million civil records were also included in the criminal repository.[49]

FBI Access to External Face Recognition Databases

FBI has been seeking broader access to external face recognition databases, like state DMV databases, since before its NGI IPS program was fully operational.[50] It revealed some information about its program in mid-2015.[51] However, the full scope of that access was not revealed until the GAO issued its report over a year later.[52]

The GAO report disclosed for the first time that FBI had access to over 400 million face recognition images—hundreds of millions more than journalists and privacy advocates had been able to estimate before that. According to the GAO report, the FBI's FACE (Facial Analysis, Comparison, and Evaluation) Services Unit not only had access to the NGI face recognition database of nearly 30 million civil and criminal mugshot photos,[53] but it also had access to the State Department's visa and passport databases, the Defense Department's biometric database, and the driver's license databases of at least 16 states. Totaling 411.9 million images, this is an unprecedented number of photographs, most of which were collected under civil and not criminal circumstances.

Under never-disclosed agreements between FBI and its state and federal partners,[54] FBI may search these civil photos whenever it is trying to find a suspect in a crime. And FBI has been searching its external partner databases extensively; between August 2011 and December 2015, FBI requested nearly 215,000 searches of external partners' databases.[55] As of December 2017, FBI's FACE Services Unit was conducting more than 7,000 searches per month—2,200 more searches per month than the same month a year prior.[56]

Failure to Address Accuracy Problems

FBI has done little to ensure its face recognition search results (which the Bureau calls "investigative leads") do not implicate innocent people. According to the GAO report and FBI's responses to EFF's Freedom of Information Act requests,[57] FBI has conducted only very limited testing to ensure the accuracy of NGI's face recognition capabilities. Further, it has not taken any steps to determine whether the face recognition systems of its external partners—states and other federal agencies—are sufficiently accurate to prevent innocent people from being identified as criminal suspects.

FBI admits its system is inaccurate, noting in its Privacy Impact Assessment (PIA) for the IPS that it "may not be sufficiently reliable to accurately locate other photos of the same identity, resulting in an increased percentage of misidentifications."[58] However, FBI has disclaimed responsibility for accuracy in its face recognition system, stating that "[t]he candidate list is an investigative lead not an identification."[59] Because the system is designed to provide a ranked list of candidates, FBI has stated the IPS never actually makes a "positive identification," and "therefore, there is no false positive rate."[60] In fact, FBI only ensures that "the candidate will be returned in the top 50 candidates" 85 percent of the time "when the true candidate exists in the gallery."[61] It is unclear what happens when the "true candidate" does *not* exist in the gallery, however. Does NGI still return possible matches? Could those people then be subject to criminal investigation for no other reason than that a computer thought their face was mathematically similar to a suspect's?

The GAO report criticizes FBI's cavalier attitude regarding false positives, noting that "reporting a detection rate without reporting the accompanying false positive rate presents an incomplete view of the system's accuracy."[62] The report also notes that FBI's stated detection rate may not represent operational reality because FBI only conducted testing on a limited subset of images and failed to conduct additional testing as the size of the database increased. FBI also has never tested to determine detection rates where the size of the responsive candidate pool is reduced to a number below 50.[63]

When false positives represent real people who may become suspects in a criminal investigation, the number of false positives a system generates is especially important.[64]

FBI's face recognition programs involve multiple factors that will decrease accuracy. For example, face recognition performs worse overall as the size of the database increases, in part because so many people within a given population look similar to one another. At more than 50 million searchable photos so far,[65] FBI's face recognition system constitutes a very large database.

Face recognition is also extremely challenging at low image resolutions.[66] EFF learned through documents FBI released in response to our 2012 FOIA request that the median resolution of images submitted through an IPS pilot program was "well-below" the recommended resolution of 3/4 of a megapixel.[67] (In comparison, newer iPhone cameras are capable of 12 megapixel resolution.[68]) Another FBI document released to EFF noted that because "the trend for the quality of data received by the customer is lower and lower quality, specific research and development plans for low-quality submission accuracy improvement is highly desirable."[69]

FBI claims it uses human examiners to review the system's face recognition matches, but using humans to perform the final suspect identification from a group of photos provided by the system does not solve accuracy problems. Research has shown that, without specialized training, humans may be worse at identification than a computer algorithm. That is especially true when the subject is someone they do not already know or someone of a race or ethnicity different from their own.[70] Many of the searches conducted in NGI are by state and local agencies. NGI provides search results to these agencies on a blind or "lights out" basis (*i.e.* no one at FBI reviews the results before they are provided to the agencies).[71] It is unlikely the smaller agencies will have anyone on staff who is appropriately trained to review these search results, so misidentifications are very likely to occur.

Failure to Produce Basic Information about NGI and its Use of Face Recognition as Required by Federal Law

Despite going live with NGI in increments since at least 2008, FBI has failed to release basic information about its system, including information mandated by federal law, that would have informed the public about what data FBI has been collecting and how that data is being used and protected.

The federal Privacy Act of 1974 and the E-Government Act of 2002 require agencies to address the privacy implications of any system that collects identifiable information on the public.[72] The Privacy Act requires agencies to provide formal notice in the Federal Register about any new system that collects and uses Americans' personal information.[73] This notice, called a System of Records Notice (SORN) must describe exactly what data is collected and how it is being used and protected, and must be published with time for the public to comment. The E-Government Act requires agencies to conduct Privacy Impact Assessments (PIAs) for all programs that collect information on the public and notify the public about why the information is being collected, the intended use of the information, with whom the information will be shared, and how the information will be secured. PIAs should be conducted during the development of any new system "with sufficient lead time to permit final Departmental approval and public website posting on or before the commencement of any system operation (including before any testing or piloting.)"[74]

PIAs and SORNs are an important check against government encroachment on privacy. They allow the public to see how new government programs and technology affect their privacy and assess whether the government has done enough to mitigate the privacy risks. As the DOJ's own guidelines on PIAs explain, "The PIA also . . . helps promote trust between the public and the Department by increasing transparency of the Department's systems and missions."[75] As noted, they are also mandatory.[76]

FBI complied with these requirements when it began developing its face recognition program in 2008 by issuing a PIA for the program that same year. However, as the Bureau updated its plans for face recognition, it failed to update its PIA, despite calls from Congress and members of the privacy advocacy community to do so.[77] It didn't issue a new PIA until late 2015—a full year after the entire IPS was online and fully operational, and at least four years after FBI first started incorporating face recognition-compatible photographs into NGI.[78] Before FBI issued the new PIA, it had already conducted over 100,000 searches of its database.[79]

FBI also failed to produce a SORN for the NGI system until 2016.[80] For years FBI skirted the Privacy Act by relying on an outdated SORN from 1999 describing its legacy criminal database called IAFIS (Integrated Automatic Fingerprint Information System),[81] which only included biographic information, fingerprints, and non-searchable photographs. Even FBI now admits that NGI contains nine "enhancements" that make it fundamentally different from the original IAFIS database that it replaces.[82]

The GAO report specifically faulted FBI for amassing, using, and sharing its face recognition technologies without ever explaining the privacy implications of its actions to the public. As GAO noted, the whole point of a PIA is to give the public notice of the privacy implications of data collection programs and to ensure that privacy protections are built into the system from the start. FBI failed to do this.

Unclear Scope

The public still does not have as much information as it should about FBI's face recognition systems and FBI's plans for their future evolution. For example, a Request for Proposals that FBI released in 2015 indicated the agency planned to allow law enforcement officers to use mobile devices to collect face recognition data out in the field and submit that data directly to NGI.[83] By the end of 2017, state and local law enforcement officers from 29 states and the District of Columbia were already able to access certain FBI criminal records via mobile devices, and the Bureau has said it expects to expand access in 2018.[84]

As we have seen with state and local agencies that have already begun using mobile biometric devices, officers may use such devices in ways that push the limits of and in some cases directly contradict constitutional law. For example, in San Diego, where officers from multiple agencies use mobile devices to photograph people right on the street and immediately upload those images to a shared face recognition database, officers have pressured citizens to consent to having their picture taken.[85] Regional law enforcement policy has also allowed collection based on First Amendment-protected activities like an "individual's political, religious, or social views, associations or activities" as long as that collection is limited to "instances directly related to criminal conduct or activity."[86]

From FBI's past publications related to NGI,[87] it is unclear whether FBI would retain the images collected with mobile devices in the NGI database. If it does, this would directly contradict 2012 congressional testimony where an FBI official said that "[o]nly criminal mug shot photos are used to populate the national repository."[88] A photograph taken in the field before someone is arrested is not a "mug shot."

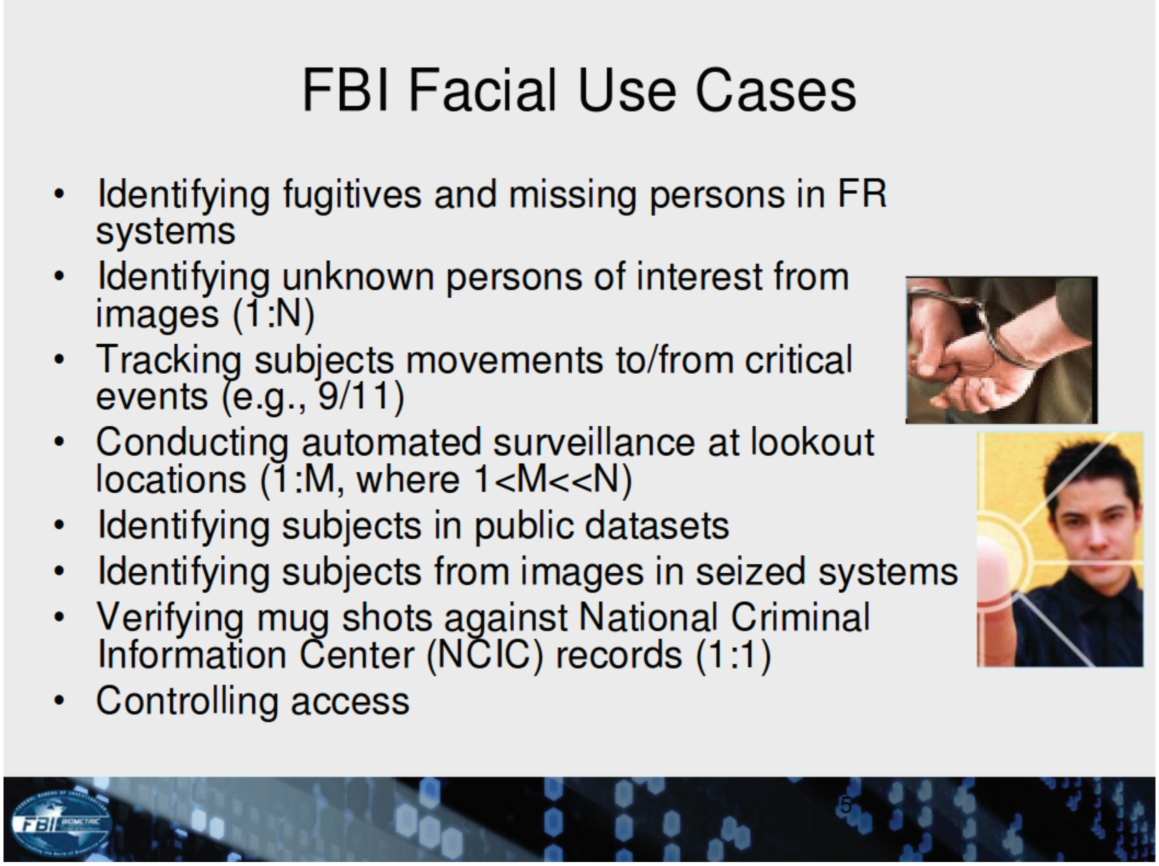
Part 3: Face Recognition Capabilities and Concerns On The Horizon

Law enforcement agencies are exploring other ways to take advantage of face recognition. For example, there is some indication FBI and other agencies would like to incorporate crowd photos and images taken from social media into their databases. A 2011 Memorandum of Understanding (MOU) between Hawaii and FBI shows that the government has considered "permit[ting] photo submissions independent of arrests."[89] It is not clear from the document what types of photos this could include, but FBI's privacy-related publications about NGI and IPS[90] leave open this possibility that FBI may plan to incorporate crowd or social media photos into NGI in the future. FBI's most recent PIA notes that NGI's "unsolved photo file" contains photographs of "unknown subjects,"[91] and the SORN notes the system includes "biometric data" that has been "retrieved from locations, property, or persons associated with criminal or national security investigations."[92] Because criminal investigations may occur in virtual as well as physical locations, this loophole seems to allow FBI to include images collected from security cameras, social media accounts, and other similar sources.

At some point in the future, FBI may also attempt to populate NGI with millions of other non-criminal photographs. The GAO report notes FBI's FACE Services Unit already has access to the IPS, the State Department's Visa and Passport databases, the Defense Department's biometric database, and the driver's license databases of at least 16 states.[93] However, the combined 412 million images in these databases may not even represent the full scope of FBI access to face recognition data today. When GAO's report first went to press, it noted that FBI officials had stated FBI was in negotiations with 18 additional states to obtain access to their driver's license databases.[94] This information was kept out of later versions of the report, so it is unclear where these negotiations stand today. The later version of the report also indicates Florida does not share its driver's license data with FBI, but Georgetown's 2016 report on law enforcement access to state face recognition databases contradicts this; Georgetown found FBI field offices in Florida can search all driver's license and ID photos in the state.[95]

FBI has hinted it has broader plans than these, however. FBI indicated in a 2010 presentation that it wants to use NGI to track people's movements to and from "critical events" like political rallies, to identify people in "public datasets," to "conduct[] automated surveillance at lookout locations," and to identify "unknown persons of interest" from photographs.[96] This suggests FBI wants to be able to search and identify people in photos of crowds and in pictures posted on social media sites—even if the people in those photos haven't been arrested for or suspected of a crime.

While identifying an unknown face in a crowd in real time from a very large database of face images would still be particularly challenging,[97] researchers in other countries claim they are well on the way to solving this problem. Recently, Russian developers announced that their system, called FindFace, could identify a person on the street with about 70 percent accuracy if that person had a social media profile.[98] Law enforcement agencies in other countries are partnering with face recognition vendors to identify people from archived CCTV footage,[99] and the United States National Institute of Standards and Technology (NIST), in partnership with the Department of Homeland Security, has sponsored research to assess the capability of face recognition algorithms to correctly identify people in videos.[100] As NIST notes, use cases for this technology include "high volume screening of persons in the crowded spaces (*e.g.* an airport)" and "[l]ow volume forensic examination of footage from a crime scene (*e.g.* a convenience store)." While NIST recognizes the ability to recognize "non-cooperative" people in video is still incredibly challenging, it notes, "Given better cameras, better design, and the latest algorithm developments, recognition accuracy can advance even further."[101] In fact, face recognition vendors are already working with large events organizers to identify people in real time at sports events in the United States and abroad.[102]



FBI Facial Use Cases

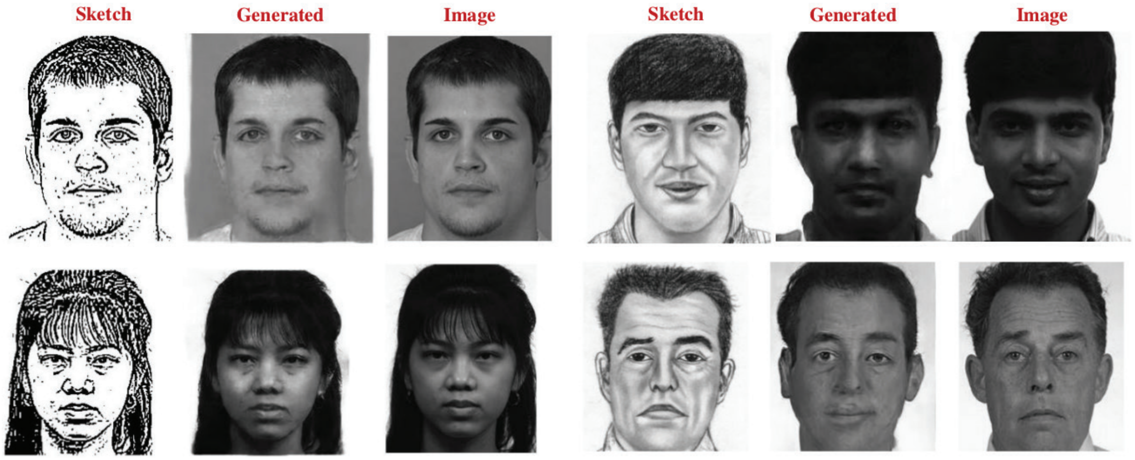
- Identifying fugitives and missing persons in FR systems
- Identifying unknown persons of interest from images (1:N)
- Tracking subjects movements to/from critical events (e.g., 9/11)
- Conducting automated surveillance at lookout locations (1:M, where 1<M<<N)
- Identifying subjects in public datasets
- Identifying subjects from images in seized systems
- Verifying mug shots against National Criminal Information Center (NCIC) records (1:1)
- Controlling access

This slide from a 2010 FBI presentation indicates plans to use NGI more broadly. Source: https://www.eff.org/document/fbi-facial-recognition-initiatives-presentation-2010-biometrics-conference.

Police officers are also increasingly interested in using face recognition with body-worn cameras, despite the clear security risks and threats to privacy posed by such systems.[103] A U.S. Department of Justice-sponsored 2016 study found that at least nine of 38 manufacturers currently include face recognition in body-worn cameras or are making it possible to include in the future.[104] Some of these body-worn camera face recognition systems allow cameras to be turned on and off remotely and allow camera feeds to be monitored back at the station.[105]As we have seen with other camera systems, remote access and control increases the security risk that bad actors could hijack the feed or that the data could be transmitted in the clear to anyone who happened to intercept it.[106]

Adding face recognition to body-worn cameras would also undermine the primary original purposes of these tools: to improve police interactions with the public and increase oversight and trust of law enforcement. People are much less likely to seek help from the police if they know or suspect not only that their interactions are not being recorded, but also that they can be identified in real time or in the future. This also poses a grave threat to First Amendment-protected speech and the ability to speak anonymously, which has been recognized as a necessity for a properly-functioning democracy since the birth of the United States.[107] Police officers are almost always present at political protests in public places and are increasingly wearing body-worn cameras while monitoring activities. Using face recognition would allow officers to quickly identify and record specific protesters, chilling speech and discouraging people who are typically targeted by police from participating. Face recognition on body-worn cameras will also allow officers to covertly identify and surveil the public on a scale we have never seen before.

Near-future uses of face recognition may also include identifying people at night in the dark,[108] projecting what someone will look like later in life based on how they look as a child,[109] and generating a photograph-like image of person from a police sketch or even from a sample of DNA.[110] Researchers are also developing ways to apply deep learning and artificial intelligence to improve the accuracy and speed of face recognition systems.[111] Some claim these advanced systems may in the future be able to detect such private information as sexual orientation, political views, high IQs, a predisposition to criminal behavior, and specific personality traits.[112]



Near-future uses include generating a photograph-like image of a person from a sketch.
Source: Center for Identification Technology Research.

Face recognition does not work without databases of pre-collected images. The federal government and state and local law enforcement agencies are working hard to build out these databases today, and NIST is sponsoring research in 2018 to measure advancements in the accuracy and speed of face recognition identification algorithms that search databases containing at least 10 million images.[113] This means the time is ripe for new laws to prevent the overcollection of images in the future and to place severe limits on the use of images that already exist.

Part 4: Proposals for Change

The over-collection of face recognition data has become a real concern, but there are still opportunities—both technological and legal—for change. Transparency, accountability, and strict limits on use are critical to ensuring that face recognition not only comports with constitutional protections but also preserves democratic values.

Legislation is an important option for addressing these issues, and the federal government's response to two seminal wiretapping cases in the late 1960s could be used as a model for face recognition legislation today.[114] In the wake of *Katz v. United States*[115] and *New York v. Berger*,[116] the federal government enacted the Wiretap Act,[117] which lays out specific rules that govern federal wiretapping, including the evidence necessary to obtain a wiretap order, limits on a wiretap's duration, reporting requirements, a notice provision, and also a suppression remedy that anticipates wiretaps may sometimes be conducted unlawfully.[118] Since then, law enforcement's ability to wiretap a suspect's phone or electronic device has been governed primarily by statute rather than Constitutional case law.

Legislators could also look to the Video Privacy Protection Act (VPPA).[119] Enacted in 1988, the VPPA prohibits the "wrongful disclosure of video tape rental or sale records" or "similar audio-visual materials," requires a warrant before a video service provider may disclose personally identifiable information to law enforcement, and includes a civil remedies enforcement provision.

Although some believe that Congress is best positioned to ensure that appropriate safeguards are put in place for technologies like face recognition, Congress has been unable to make non-controversial updates to *existing* law enforcement surveillance legislation,[120] much less enact new legislation. For that reason, the best hope at present is that states will fill the void, as several states have already in other contexts by passing legislation that limits surveillance technologies like location and communications tracking.[121]

Legislators and regulators considering limits on the use of face recognition should keep the following nine principles in mind to protect privacy and security.[122] These principles are based in part on key provisions of the Wiretap Act and VPPA and in part on the Fair Information Practice Principles (FIPPs), an internationally-recognized set of privacy protecting standards.[123] The FIPPs predate the modern Internet but have been recognized and developed by government agencies in the United States, Canada, and Europe since 1973, when the United States Department of Health, Education, and Welfare released a seminal report on privacy protections in the age of data collection called *Records, Computers, and the Rights of Citizens*.[124]

Limit the Collection of Data

The collection of face recognition data should be limited to the minimum necessary to achieve the government's stated purpose. For example, the government's acquisition of face recognition from sources other than directly from the individual to populate a database should be limited. The government should not obtain face recognition data en masse to populate its criminal databases from sources where the biometric was originally acquired for a non-criminal purpose (such as state DMV records), or from crowd photos or data collected by the private sector. Techniques should also be employed to avoid over-collection of face prints (such as from security cameras or crowd photos) by, for example, scrubbing the images of faces that are not central to an investigation. The police should not retain "probe" images—that is, images of unidentified individuals—or enter them into a database. Agencies should also not retain the results of image searches, except for audit purposes.

Define Clear Rules on the Legal Process Required for Collection

Face recognition should be subject to clear rules on when it may be collected and which specific legal processes—such as a warrant based on probable cause—are required prior to collection. Collection and retention should be specifically disallowed without legal process unless the collection falls under a few very limited and defined exceptions. For example, clear rules should define when, if ever, law enforcement and other agencies may collect face recognition images from the general public without their knowledge.

Limit the Amount and Type of Data Stored and Retained

A face print can reveal much more information about a person than his or her identity, so rules should be set to limit the amount of data stored. Retention periods should be defined by statute and limited in time, with a high priority on deleting data. Data that is deemed to be "safe" from a privacy perspective today could become highly identifying tomorrow. For example, a dataset that includes crowd images could become much more privacy-invasive as identification technology improves. Similarly, data that is separate and siloed or unjoinable today might be easily joinable tomorrow. For this reason retention should be limited, and there should be clear and simple methods for a person to request removal of his or her biometric from the system if, for example, they have been acquitted or are no longer under investigation.[125]

Limit the Combination of More than One Biometric in a Single Database

Different biometric data sources should be stored in separate databases. If a face template needs to be combined with other biometrics, that should happen on an ephemeral basis for a particular investigation. Similarly, biometric data should not be stored together with non-biometric contextual data that would increase the scope of a privacy invasion or the harm that would result if a data breach occurred. For example, combining face recognition images or video from public cameras with license plate information increases the potential for tracking and surveillance. This should be avoided, or limited to specific individual investigations.

Define Clear Rules for Use and Sharing

Biometrics collected for one purpose should not be used for another. For example, face prints collected in a non-criminal context, such as for a driver's license or to obtain government benefits, should not be shared with law enforcement—if they are shared at all—without strict legal process. Similarly, face prints collected for use in an immigration context, such as to obtain a visa, should not automatically be used or shared with an agency to identify a person in a criminal context. Face recognition should only be used—if it is used at all—under extremely limited circumstances after all other investigative options have been exhausted. It should not be used to identify and track people in real time without a warrant that contains specific limitations on time and scope. Additionally, private sector databases should not only be required to obtain user consent before enrolling people into any face recognition system, they should also be severely restricted from sharing their data with law enforcement.

Enact Robust Security Procedures to Minimize the Threat of Imposters on the Front End and Avoid Data Compromise on the Back End

Because most biometrics cannot easily be changed, and because all databases are inherently vulnerable to attack, data compromise is especially problematic. The use of traditional security procedures is paramount, such as implementing basic access controls that require strong passwords, limiting access privileges for most employees, excluding unauthorized users, and encrypting data transmitted throughout the system. On top of that, security procedures specific to biometrics should also be enacted to protect the data. For example, data should be anonymized or stored separate from personal biographical information. Strategies should also be employed at the outset to pre-emptively counter data compromise and to prevent digital copies of biometrics. Biometric encryption[126] or "hashing" protocols that introduce controllable distortions into the biometric before matching can reduce the risk of problems later. The distortion parameters can easily be changed to make it technically difficult to recover the original privacy-sensitive data from the distorted data, should the data ever be breached or compromised.[127]

Mandate Notice Procedures

Because of the risk that face prints will be collected without a person's knowledge, rules should define clear notice requirements to alert people to the fact that a face print has been collected. The notice should also make clear how long the data will be stored and how to request its removal from the database.

Define and Standardize Audit Trails and Accountability Throughout the System

All database transactions—including face recognition input, access to and searches of the system, data transmission, etc.—should be logged and recorded in a way that ensures accountability. Privacy and security impact assessments, including independent certification of device design and accuracy, should be conducted regularly.

Ensure Independent Oversight

Government entities that collect or use face recognition must be subject to meaningful oversight from an independent entity. Individuals whose data are compromised by the government or the private sector should have strong and meaningful avenues to hold them accountable.

Conclusion

Face recognition and its accompanying privacy and civil liberties concerns are not going away. Given this, it is imperative that government act now to limit unnecessary data collection; instill proper protections on data collection, transfer, and search; ensure accountability; mandate independent oversight; require appropriate legal process before collection and use; and define clear rules for data sharing at all levels. This is crucial to preserve the democratic and constitutional values that are the bedrock of American society.

Acronyms and Useful Terms

FACE Services Unit - Facial Analysis, Comparison, and Evaluation Services Unit. FBI's internal face recognition team.

Face template - The data that face recognition systems extract from a photograph to represent a particular face. This data consists of specific, distinctive details about a person's face, such as the distance between the eyes or the shape of the chin, converted into a mathematical representation. A face template is distinct from the original photograph because it is designed to only include certain details that can be used to distinguish one face from another. This may also be called a "face print."

False negative - The result when a face recognition system fails to match a person's face to an image that is contained in the database.

False positive - The result when a face recognition system matches a person's face to an image in the database, but that match is incorrect.

FAR - False accept rate. This is the number of false positives a system produces.

FRR - False reject rate. This is the number of false negatives a system produces.

Gallery - The entire database of face recognition data against which searches are conducted.

Gallery of candidate photos - The list of photos a face recognition system produces as potential matches in response to a search. For example, when a law enforcement agency submits a photo of a suspect to find matches in a mugshot database, the list of potential matches from the repository is called the gallery of candidate photos.

GAO - Government Accountability Office.

IPS - Interstate Photo System. The part of the NGI that contains photographs searchable through face recognition.

NGI - Next Generation Identification. The NGI database is a massive biometric database that includes fingerprints, iris scans, and palm prints collected from millions of individuals not just as part of an arrest, but also for non-criminal reasons like background checks, state licensing requirements, and immigration.

OPM - Office of Personnel Management.

PIA - Privacy Impact Assessment.

Probe photo - The photo against which a face recognition system is searched. For example, a law enforcement agency might submit a "probe photo" of an unidentified suspect to search for potential matches in a mugshot database.

SORN - System of Records Notice.

Notes

[1] Clare Garvie, et al., *The Perpetual Line-Up*, Geo. L. Ctr. on Privacy & Tech. (Oct. 18, 2016), https://www.perpetualline-up.org/jurisdiction/florida.

[2] *See* R. W. Vorder Bruegge, et al., *Face Recognition Performance: Role of Demographic Information*, 7 IEEE Transactions on Info. Forensics and Sec. 6, 1789-1801(Dec. 2012), http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6327355&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Ficp.jsp%3Farnumber%3D6327355; Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research (2018) http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[3] *See* Criminal Justice Fact Sheet, NAACP (2009), http://www.naacp.org/criminal-justice-fact-sheet.

[4] *See, e.g.,* Devlin Barrett, *Gun-Show Customers' License Plates Come under Scrutiny*, Wall St. J. (Oct. 2016), http://www.wsj.com/articles/gun-show-customers-license-plates-come-under-scrutiny-1475451302; Dave Elias, *Deputy fired for misusing driver's license database*, NBC2 (April 24, 2014), http://www.nbc-2.com/story/25334275/deputy-fired-for-improperly-accessing-info-about-governor-nbc2-anchors-others; Chris Francescani, *License to Spy,* Medium (Dec. 1, 2014), https://medium.com/backchannel/the-drive-to-spy-80c4f85b4335.

[5] *See, e.g.,* P. Jonathon Phillips, et al., *An Introduction to the Good, the Bad, & the Ugly Face Recognition: Challenge Problem*, Nat'l Inst. of Standards & Testing (Dec. 2011), www.nist.gov/itl/iad/ig/upload/05771424.pdf (noting only 15 percent accuracy for face image pairs that are "difficult to match").

[6] *See, e.g.*, Min-Chun Yang, et al., *Recognition at a Long Distance: Very Low Resolution Face Recognition and Hallucination*, IEEE 2015 Int'l Conf. on Biometrics, 237-42 (May 2015).

[7] *See generally, Face in Video Evaluation*, NIST, https://www.nist.gov/programs-projects/face-video-evaluation-five.

[8] *See, e.g.,* Ariane Wu, *The Secret History of American Surveillance*, Reveal (Oct. 15, 2015), https://www.revealnews.org/article/the-secret-history-of-american-surveillance; *The LAPD: 1926-1950*, Los Angeles Police Dept., http://www.lapdonline.org/history_of_the_lapd/content_basic_view/1109; Andrew Becker & G.W. Schulz, *Mall of America Visitors Unknowingly end up in Counterterrorism Reports*, Reveal (Sept. 7, 2011), https://www.revealnews.org/article/mall-of-america-visitors-unknowingly-end-up-in-counterterrorism-reports; Tim Weiner, Enemies: A History of the FBI (2012); *A Review of the FBI's Use of Nat'l Sec. Letters, Special Report*, DOJ, Office of Inspector General (OIG), (Mar. 2007).

[9] *See* Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 Minn. L. Rev. 407, 415 (Dec. 2012).

[10] *Baltimore County Police Department and Geofeedia Partner to Protect the Public During Freddie Gray Riots*, Geofeedia, https://www.aclunc.org/docs/20161011_geofeedia_baltimore_case_study.pdf.

[11] *See, e.g.*, Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93 Journalism & Mass Comm. Quarterly, 296–311 (2016), http://journals.sagepub.com/doi/pdf/10.1177/1077699016630255.

[12] *See* Karen Turner, *Mass Surveillance Silences Minority Opinions, According to Study*, Wash. Post (Mar. 28, 2016),

https://www.washingtonpost.com/news/the-switch/wp/2016/03/28/mass-surveillance-silences-minority-opinions-according-to-study/?utm_term=.6d51b07dbb33.

13 Diala Shamas & Nermeen Arastu, *Mapping Muslims: NYPD Spying and its Impact on American Muslims* (Mar. 2013), http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf.

14 *Id.*

15 Nellie Bowles, *'I Think My Blackness is Interfering': Does Facial Recognition Show Racial Bias?*, The Guardian (Apr. 8, 2016), https://www.theguardian.com/technology/2016/apr/08/facial-recognition-technology-racial-bias-police.

16 *See* Bruegge, et al.*, supra* note 2; Buolamwini & Gebru, *supra* note 2. This problem is due in part to the fact that people of color and women are underrepresented in training data.

17 *See* NAACP, *supra* note 3.

18 Lucas D. Introna & Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, 37, N.Y.U. (Apr. 2009), https://www.nyu.edu/projects/nissenbaum/papers/facial_recognition_report.pdf.

19 *See* Madeline Neighly & Maurice Emsellem, *WANTED: Accurate FBI Background Checks for Employment*, National Employment Law Project (July 2013), http://www.nelp.org/content/uploads/2015/03/Report-Wanted-Accurate-FBI-Background-Checks-Employment.pdf; *See also* Ellen Nakashima, *FBI Wants to Exempt Its Huge Fingerprint and Photo Database from Privacy Protections*, Wash. Post (June 30, 2016), https://www.washingtonpost.com/world/national-security/fbi-wants-to-exempt-its-huge-fingerprint-and-photo-database-from-privacy-protections/2016/05/31/6c1cda04-244b-11e6-8690-f14ca9de2972_story.html (noting that, according to 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").

20 Rachel Weiner, *Romanian Hackers took over D.C. Surveillance Cameras just before Presidential Inauguration, Federal Prosecutors Say*, Wash. Post (Dec. 28, 2017), https://www.washingtonpost.com/local/public-safety/romanian-hackers-took-over-dc-surveillance-cameras-just-before-presidential-inauguration-federal-prosecutors-say/2017/12/28/7a15f894-e749-11e7-833f-155031558ff4_story.html.

21See, e.g., Tracy Connor, et al., *U.S. Publicly Blames Russian Government for Hacking*, NBC News (Oct. 7, 2016), http://www.nbcnews.com/news/us-news/u-s-publicly-blames-russian-government-hacking-n662066.

22 Julie Hirschfeld Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. Times (July 9, 2015), http://www.nytimes.com/2015/07/10/ us/office-of-personnel-management-hackers-got-data-of-millions.html; *See also, e.g.,* David Stout and Tom Zeller Jr., *Vast Data Cache About Veterans Is Stolen*, N.Y. Times (May 23, 2006), https://www.nytimes.com/2006/05/23/washington/23identity.html; *See also MEPs question Commission over problems with biometric passports*, European Parliament News (Apr. 19, 2012), http://www.europarl.europa.eu/news/en/headlines/content/20120413STO42897/html/MEPs-question-Commission-over-problems-with-biometric-passports (noting that, at the time, "In France 500,000 to 1 million of the 6.5 million biometric passports in circulation are estimated to be false, having been obtained on the basis of fraudulent documents").

23 Davis, *supra* note 22.

24 Francescani, *supra* note 4.

25 Barton Gellman, *NSA Broke Privacy Rules Thousands of Times Per Year, Audit Finds*, Wash. Post (Aug. 15, 2013), https://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html; *NSA watchdog details surveillance misuse*, Assoc. Press (Sept. 27, 2013) https://www.cnbc.com/2013/09/27/nsa-watchdog-details-surveillance-misuse.html.

26 *Id.*

27 Sadie Gurman & Eric Tucker, *Across US, police officers abuse confidential databases*, Assoc. Press (Sept. 28, 2016), https://apnews.com/699236946e3140659fff8a2362e16f43.

[28] *Id.*

[29] Simon Davies, *Little brother is watching you*, Independent (Aug. 25, 1998) https://www.independent.co.uk/arts-entertainment/little-brother-is-watching-you-1174115.html (Researchers found that "10 per cent of the time spent filming women was motivated by voyeurism." One researcher noted, "It is not uncommon for operators to make `greatest hits' compilations."); *Man jailed for eight months for spying on woman with police camera*, TheJournal.ie (Sept. 26, 2014), http://www.thejournal.ie/cctv-police-spying-woman-1693080-Sep2014.

[30] *FBI Workers Suspected of Secretly Taping Teems in Dressing Room*, Assoc. Press (Apr. 20, 2009), http://www.foxnews.com/story/2009/04/20/fbi-workers-suspected-secretly-taping-teens-in-dressing-room.html.

[31] Amy Pavuk, *Law-Enforcer Misuse of Driver Database Soars*, Orlando Sentinel (Jan. 22, 2013), http://articles.orlandosentinel.com/2013-01-22/news/os-law-enforcement-access-databases-20130119_1_law-enforcement-officers-law-enforcers-misuse; *See also* Kim Zetter, *Cops Trolled Driver's License Database for Pic of Hot Colleague*, Wired (Feb. 23, 2012), https://www.wired.com/2012/02/cop-database-abuse.

[32] Dave Elias, *Deputy Fired for Misusing Driver's License Database*, NBC2 (Apr. 24, 2014), http://www.nbc-2.com/story/25334275/deputy-fired-for-improperly-accessing-info-about-governor-nbc2-anchors-others.

[33] Eric Lyttle, *Fairfield County Grand Jury Indicts Two over Misuse of Database for Police*, Columbus Dispatch (Apr. 24, 2015), http://www.dispatch.com/article/20150424/NEWS/304249775.

[34] Brad Flora, *What Do the Cops Have on Me?*, Slate (Dec. 4, 2007), http://www.slate.com/articles/news_and_politics/explainer/2007/12/what_do_the_cops_have_on_me.html.

[35] Government Accountability Office, *Information Security: FBI Needs to Address Weaknesses in Critical Network*, GAO-07-368 (Apr. 2007) http://www.gao.gov/new.items/d07368.pdf.

[36] *See* Systems of Records Notice for Next Generation Identification, 81 Fed. Reg. 27283 (May 5, 2016), https://www.federalregister.gov/documents/2016/05/05/2016-10120/privacy-act-of-1974-systems-of-records (hereinafter "SORN for NGI")

[37] *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, Government Accountability Office, 46, GAO-16-267 (May 2016) http://www.gao.gov/assets/680/677098.pdf (hereinafter "GAO Report").

[38] *Next Generation Identification*, FBI, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi; *see also* FBI, *Biometric Center of Excellence*, FBI, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/biometric-center-of-excellence/modalities.

[39] *See, e.g.*, *Fingerprint Requirement for License Renewal*, Dental Bd. of Cal. (2016), http://www.dbc.ca.gov/licensees/fingerprint_faq.shtml#q1; *New Fingerprinting Process for CPA Exam Applicants*, Tex. St. Bd. of Publ. Acct. (Aug. 1, 2014), https://www.tsbpa.texas.gov/info/2014072801.html; *Completing the Fingerprint Requirement*, Wisc. Dept. of Pub. Instruction (Aug. 1, 2013), http://dpi.wi.gov/tepdl/licensing/fingerprint; *Land Surveyors, and Geologists, Fingerprinting FAQ's*, Cal. Dept. of Consumer Aff. Bd. for Prof. Engineers (2012), http://www.bpelsg.ca.gov/applicants/fingerprinting_faqs.shtml; *Real Estate License Candidate Fingerprinting*, State of New Jersey Dept. of Banking & Insurance (Feb. 1, 2015), http://www.state.nj.us/dobi/division_rec/licensing/fingerprint.html; *Moral Character Determination Instructions*, The State Bar of Cal. (2016), https://www.calbarxap.com/applications/calbar/info/moral_character.html#fingerprints; *Fingerprint Requirement for License Renewal*, Cal. Dept. of Consumer Affairs Board of Optometry (June 21, 2010), http://www.optometry.ca.gov/faqs/fingerprint.shtml#q1.

[40] *See* Executive Order 10450: Sec. Requirements for Gov't Employment (Apr. 27, 1953), https://www.archives.gov/federal-register/codification/executive-order/10450.html.

[41] *See* FBI, *Next Generation Identification (NGI) Monthly Fact Sheet* (Dec. 2017), https://www.eff.org/document/december-2017-next-generation-identification-ngi-system-fact-sheet (hereinafter "December 2017 NGI Monthly Fact Sheet").

[42] FBI, *Criminal Justice Information Services Annual Report 2016*, 16, hhttps://www.eff.org/document/

fbi-criminal-justice-information-services-2016-annual-report (hereinafter "CJIS Annual Report 2016").

43 GAO Report, *supra* note 37, at 13. The Report does not list these remaining states.

44 *Next Generation Identification (NGI)—Retention and Searching of Noncriminal Justice Fingerprint Submissions*, FBI (Feb. 20, 2015), https://www.fbi.gov/foia/privacy-impact-assessments/next-generation-identification-ngi-retention-and-searching-of-noncriminal-justice-fingerprint-submissions.

45 *See* Adam Vrankulj, *NGI: A Closer Look at the FBI's Billion-dollar Biometric Program*, Biometric Update (Nov. 4, 2013), http://www.biometricupdate.com/201311/ngi-a-closer-look-at-the-fbis-billion-dollar-biometric-program.

46 *See* December 2017 NGI Monthly Fact Sheet, *supra* note 41.

47 *See* Ernest J. Babcock, *Privacy Impact Assessment for the Next Generation Identification (NGI) Interstate Photo System*, Senior Component Official for Privacy, FBI (Sept. 2015), https://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system.

48 *See, e.g.*, Ariz. Rev. Stat. § 13-2906 (2016) (obstructing a highway or other public thoroughfare; classification).

49 *See Next Generation Identification (NGI) Monthly Fact Sheet*, FBI (Dec. 2015), https://web.archive.org/web/20160331181001/https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi/december-2015-ngi-fact-sheet.pdf (hereinafter "December 2015 NGI Monthly Fact Sheet"). FBI's current Monthly Fact Sheet omits this information. *Compare* December 2017 NGI Monthly Fact Sheet, *supra* note 41.

50 *See, e.g.,* Jennifer Lynch, *FBI's Facial Recognition is Coming to a State Near You*, EFF (Aug. 2, 2012), https://www.eff.org/deeplinks/2012/07/fbis_facial_recognition_coming_state_near_you; *FBI Scans DMV Photos for Criminals*, Assoc. Press (Oct. 13, 2009) https://www.cbsnews.com/news/fbi-scans-dmv-photos-for-criminals.

51 *Privacy Impact Assessment for the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit*, FBI (May 1, 2015), https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/facial-analysis-comparison-and-evaluation-face-services-unit.

52 *See* GAO Report, *supra* note 37.

53 This number is now more than 50,000. FBI, *CJIS Annual Report 2016*, *supra* note 42.

54 FBI has not released these agreements.

55 GAO Report, *supra* note 37, at 10.

56 *See* December 2017 NGI Monthly Fact Sheet, *supra* note 41.

57 *See* GAO Report, *supra* note 37, at 26-27; Jennifer Lynch, *FBI Plans to Have 52 Million Photos in its NGI Face Recognition Database by Next Year*, and accompanying documents. https://www.eff.org/deeplinks/2014/04/fbi-plans-have-52-million-photos-its-ngi-face-recognition-database-next-year.

58 *Privacy Impact Assessment for the Next Generation Identification (NGI) Interstate Photo System,* FBI, (Sept. 2015), https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/interstate-photo-system (hereinafter "2015 FBI Interstate Photo System PIA").

59 *See* Lynch, *FBI Plans to Have 52 Million Photos in its NGI Face Recognition Database by Next Year*, *supra* note 57. The FBI has also noted that because "this is an investigative search and caveats will be prevalent on the return detailing that the [non-FBI] agency is responsible for determining the identity of the subject, there should be NO legal issues." *Id.*

60 *Id.*

61 *Id.*

62 GAO Report, *supra* note 37, at 27.

63 GAO Report, *supra* note 37, at 26.

64 Security researcher Bruce Schneier has noted that even a 90 percent accurate system "will sound a million false alarms for every real terrorist" and that it is "unlikely that terrorists will pose for crisp, clear photos." Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*, 190 (2003).

65 *CJIS Annual Report 2016*, 16, *supra* note 42.

66 See, e.g., Min-Chun Yang, et al., *supra* note 6.

67 See Lynch, *FBI Plans to Have 52 Million Photos in its NGI Face Recognition Database by Next Year*, *supra* note 57.

68 See Compare iPhone Models, Apple (2017), https://www.apple.com/iphone/compare.

69 *See* Lynch, *FBI Plans to Have 52 Million Photos in its NGI Face Recognition Database by Next Year*, *supra* note 57.

70 See Garvie, *supra* note 1, at 49 (internal citations omitted).

71 Jerome M. Pender, Deputy Assistant Director, Criminal Justice Information Services Division, FBI, *Statement Before the Senate Judiciary Committee, Subcommittee on Privacy, Technology, and the Law*, FBI (July 18, 2012), https://www.justice.gov/sites/default/files/testimonies/witnesses/attachments/07/18/12//07-18-12-fbi-pender.pdf.

72 5 U.S.C. § 552a (2018); Pub. L. 107–347 (2002).

73 5 U.S.C. § 552a(e)(4) (2018).

74 O PCL DOJ, Privacy Impact Assessments Official Guidance, 4 (Rev. March 2012), https://www.justice.gov/opcl/docs/2012-doj-pia-manual.pdf.

75 *Id.* at 3.

76 *Id.* at 4 (footnotes omitted).

77 EFF and other organizations called for years on FBI to release more information about NGI and how it impacts people's privacy. *See, e.g., Testimony of Jennifer Lynch to the Senate Committee on the Judiciary Subcommittee on Privacy, Technology, and the Law*, EFF (July 18, 2012), https://www.eff.org/document/testimony-jennifer-lynch-senate-committee-judiciary-subcommittee-privacy-technology-and-law; *Letter to Attorney General Holder re. Privacy Issues with FBI's Next Generation Identification Database*, EFF (June 24, 2014), https://www.eff.org/document/letter-attorney-general-holder-re-privacy-issues-fbis-next-generation-identification.

78 2015 FBI Interstate Photo System PIA, *supra* note 58; GAO Report, *supra* note 37 at 7; *See also* Tim Cushing, *FBI Rolls Out Biometric Database On Schedule, Accompanying Privacy Impact Assessment Still Nowhere To Be Found*, TechDirt (Sept. 16, 2014), https://www.techdirt.com/articles/20140916/09090628533/fbi-rolls-out-biometric-database-schedule-accompanying-privacy-impact-assessment-still-nowhere-to-be-found.shtml.

79 GAO Report, *supra* note 37, at 49.

80 SORN for NGI, *supra* note 36.

81 FBI, 64 Fed. Reg. 52343 (Sept. 28, 1999), https://www.gpo.gov/fdsys/pkg/FR-1999-09-28/pdf/99-24989.pdf. IAFIS stands for Integrated Automatic Fingerprint Information System.

82 SORN for NGI, *supra* note 36.

83 See Jennifer Lynch, *FBI Plans to Populate its Massive Face Recognition Database with Photographs Taken in the Field*, EFF (Sept. 18, 2015), https://www.eff.org/deeplinks/2015/09/little-fanfare-fbi-ramps-biometrics-programs-yet-again-part-2.

84 FBI, Criminal Justice Information Services Division, 2017: the Year in Review, 12, https://www.fbi.gov/file-repository/2017-cjis-year-in-review.pdf/view.

[85] *See* Jennifer Lynch and Dave Maass, *San Diego Gets in Your Face With New Mobile Identification System*, EFF (Nov. 7, 2013), https://www.eff.org/deeplinks/2013/11/san-diego-gets-your-face-new-mobile-identification-system.

[86] *Id.*

[87] Lynch, *FBI Plans to Populate its Massive Face Recognition Database with Photographs Taken in the Field, supra* note 83; 2015 FBI Interstate Photo System PIA, *supra* note 58; SORN for NGI, *supra* note 36.

[88] Pender, *supra* note 71.

[89] *Hawaii Memorandum of Understanding (MOU) with FBI for Face Recognition Photos*, EFF (Nov. 20, 2011), https://www.eff.org/document/hawaii-memorandum-understanding-mou-fbi-face-recognition-photos.

[90] 2015 FBI Interstate Photo System PIA, *supra* note 58; SORN for NGI, *supra* note 36.

[91] 2015 FBI Interstate Photo System PIA, *supra* note 58.

[92] SORN for NGI, *supra* note 36.

[93] GAO Report, *supra* note 37, at 47-48.

[94] *Compare* map of states sharing data with FACE Services on page 51 of the GAO Report, *supra* note 37, *with* map available in original version of Report, https://www.eff.org/deeplinks/2016/06/fbi-can-search-400-million-face-recognition-photos.

[95] Garvie, *supra* note 1.

[96] *See* Richard W. Vorder Bruegge, *Facial Recognition and Identification Initiatives*, FBI 5 (2010), https://www.eff.org/document/fbi-facial-recognition-initiatives-presentation-2010-biometrics-conference.

[97] Byron Spice, *Finding Faces in a Crowd*, Carnegie Mellon U. (Mar. 30, 2017) https://www.cmu.edu/news/stories/archives/2017/march/faces-in-crowd.html; Introna & Nissenbaum, *supra* note 18 (concluding that, given lighting and other challenges, as well as the fact that so many people look like one another, it is unlikely that face recognition systems with high accuracy rates under these conditions will become an "operational reality for the foreseeable future").

[98] It is unclear at what resolution and distance the probe photos were taken and how many images of each person were available to compare the probe photos against (more photographs taken from different angles and under different lighting conditions could increase the probability of a match). *See, e.g.*, Ben Guarino, *Russia's new FindFace app identifies strangers in a crowd with 70 percent accuracy*, Wash. Post (May 18, 2016) https://www.washingtonpost.com/news/morning-mix/wp/2016/05/18/russias-new-findface-app-identifies-strangers-in-a-crowd-with-70-percent-accuracy.

[99] *NEC Facial Recognition Helps NT Police Solve Cold Cases and Increase Public Safety in Australia*, NEC (Sept. 2, 2015), http://au.nec.com/en_AU/press/201509/nec-facial-recognition-increases-public-safety-in-australia.html.

[100] *Face in Video Evaluation*, NIST, https://www.nist.gov/programs-projects/face-video-evaluation-five (last updated Mar. 6, 2017).

[101] Face In Video Evaluation (FIVE)—Face Recognition of Non-Cooperative Subjects, NISTIR 8173, 2 (Mar. 2017), http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8173.pdf.

[102] Mark Lamport-Stokes, *A Golfing First for Facial Recognition Software at ANA Inspiration*, LPGA (Mar. 27, 2017), http://www.lpga.com/news/2017-nec-introduces-facial-recognition-software-at-ana-inspiration; *NEC contributes to football stadium safety in Colombia*, NEC (Oct. 12, 2016), http://www.nec.com/en/press/201610/global_20161012_03.html; Alex Perala, *NEC Facial Recognition Tech Used to Secure Sports Stadium in Taipei*, FindBiometrics (Nov. 2, 2017), https://findbiometrics.com/nec-facial-recognition-sports-stadium-taipei-411022.

[103] Alex Pasternack, *Police Body Cameras Will Do More Than Just Record You*, Fast Co. (Mar. 3, 2017), https://www.fastcompany.com/3061935/police-body-cameras-livestreaming-face-recognition-and-ai.

104 Vivian Hung, et al., *A Market Survey on Body Worn Camera Technologies*, Nat'l Crim. Just. Reference Serv. (Nov. 2016), https://www.ncjrs.gov/pdffiles1/nij/grants/250381.pdf.

105 Pasternack, *supra* note 103.

106 *See, e.g.,* Cooper Quintin & Dave Maass, *License Plate Readers Exposed! How Public Safety Agencies Responded to Major Vulnerabilities in Vehicle Surveillance Tech*, EFF (Oct. 28, 2015) https://www.eff.org/deeplinks/2015/10/license-plate-readers-exposed-how-public-safety-agencies-responded-massive; Rachel Weiner, *supra* note 20.

107 *See, e.g., Anonymity*, EFF, https://www.eff.org/issues/anonymity.

108 *See, e.g.,* Seyed Mehdi Iranmanesh, et al., *Deep Cross Polarimetric Thermal-to-visible Face Recognition*, arXiv.org (Jan. 4, 2018), https://arxiv.org/pdf/1801.01486.pdf.

109 See, e.g., Wei Wang, et al., Recurrent Face Aging, CVPR 2016 IEEE Conf. on Comput. Vision and Pattern (June 2016), https://www.cv-foundation.org/openaccess/content_cvpr_2016/papers/Wang_Recurrent_Face_Aging_CVPR_2016_paper.pdf.

110 Francie Diep, *Modeling Suspects' Faces Using DNA From Crime Scenes*, Popular Science (Jan. 29, 2015), https://www.popsci.com/new-service-reverse-engineers-faces-dna-samples-crime-scenes.

111 *See, e.g.,* Klemen Grm, et al., *Strengths and Weaknesses of Deep Learning Models for Face Recognition Against Image Degradations* (Oct. 4, 2017), https://arxiv.org/pdf/1710.01494.pdf; Russell Brandom, *Why Facebook is beating the FBI at facial recognition*, The Verge (July 7, 2014), https://www.theverge.com/2014/7/7/5878069/why-facebook-is-beating-the-fbi-at-facial-recognition.

112 *See, e.g.,* Sam Levin, *Face-Reading AI will be able to Detect your Politics & IQ, Professor Says*, The Guardian (Sept. 12, 2017), https://www.theguardian.com/technology/2017/sep/12/artificial-intelligence-face-recognition-michal-kosinski.

113 Face Recognition Vendor Test (FRVT)—1:N 2018 Evaluation, NIST, https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-1n-2018-evaluation (last updated Jan. 4, 2018).

114 *United States v. Jones*, 565 U.S. 400, 427-28, 429 (2012) (Justice Alito, in his concurring opinion, specifically referenced post-*Katz* wiretap laws when he noted that, "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative").

115 *Katz v. United States*, 389 U.S. 347 (1967).

116 *Berger v. New York*, 388 U.S. 41 (1967) (striking down a state wiretapping law as facially unconstitutional. In striking down the law, the Court laid out specific principles that would make a future wiretapping statute constitutional under the Fourth Amendment).

117 18 U.S.C. §§ 2510–2522 (2018).

118 *See, e.g.*, Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 851-52 (2004); 18 U.S.C. § 2515 (2018).

119 18 U.S.C. § 2710 (2018).

120 *See, e.g.,* Sophia Cope, *EFF Supports Senate Email and Location Privacy Bill*, EFF (July 27, 2027) https://www.eff.org/deeplinks/2017/07/eff-applauds-senate-email-and-location-privacy-bill.

121 *See, e.g.*, Cal. Penal Code § 1546 (2017); Rev. Wash. Code § 9.73.260 (2015) (placing limitations on pen registers, trap and trace devices, cell site simulator devices); Brian Fung, *Did you know Montana was a leader on privacy laws? Neither did Montana*, Wash. Post (Aug 28, 2013) https://www.washingtonpost.com/news/the-switch/wp/2013/08/28/did-you-know-montana-was-a-leader-on-privacy-laws-neither-did-montana/?utm_term=.a27cc4023e6f.

122 Researchers at Georgetown have drafted model face recognition legislation that includes many of these principles.