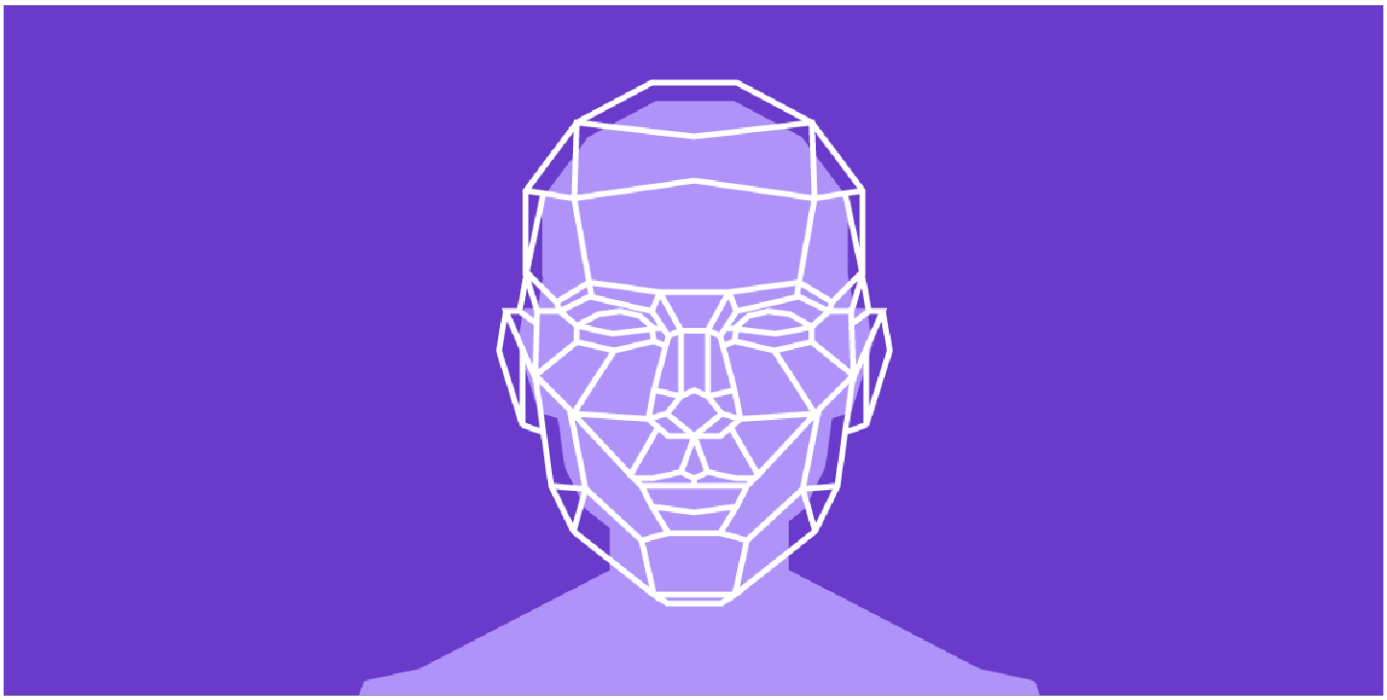
STREET LEVEL SURVEILLANCE



FACE RECOGNITION

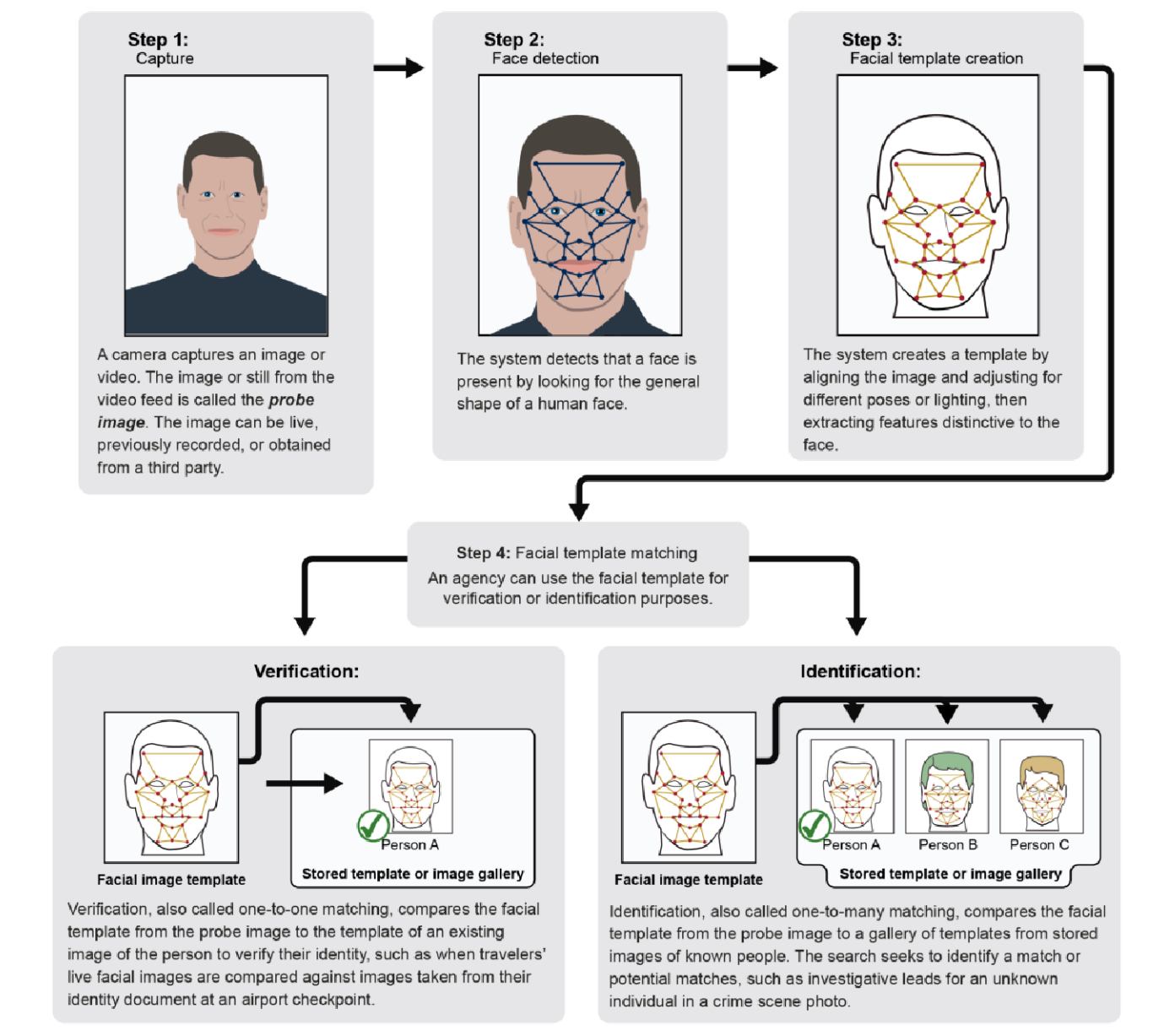
Face recognition is a biometric technology that uses a face or the image of a face to identify or verify the identity of an individual in photos, video, or in real-time. It is commonly used by law enforcement and private businesses. Face recognition systems depend on databases of individuals' images to train their underlying algorithms. Face recognition can be applied retroactively to video footage and photographs, it can be used in coordination with other surveillance technologies and databases when creating profiles of individuals, including those who may never have been involved in a crime. It can facilitate the tracking of individuals across video feeds and can be integrated into camera systems and other technologies, as we have seen at sporting events in the United States.

Face recognition can be prone to failures in its design and in its use, which can implicate people for crimes they haven't committed and make people into targets of unwarranted or dangerous retaliation. Facial recognition software is particularly bad at recognizing African Americans and other ethnic minorities, women, young people, and transgender and nonbinary individuals. People in these demographic groups are especially at risk of being misidentified by this technology and are disparately impacted by its use. Face recognition contributes to the mass surveillance of individuals,

practices, and it has been used to target people engaging in protected speech and alienate perceived enemies.

Hundreds of law enforcement agencies and a rapidly growing number of private entities use face recognition across the United States. Its use in other countries is also growing.

How Face Recognition Works



SOURCE: GOVERNMENT ACCOUNTABILITY OFFICE

identification.

Face recognition systems use computer algorithms to pick out specific, distinctive details about a person's face and make a judgment of its similarity to other faces. Details, such as distance between the eyes or shape of the chin, are converted into a mathematical representation and compared to data on other faces collected in a face recognition database. The data about a particular face is often called a face template and is distinct from a photograph because it's designed to only include certain details that can be used to distinguish one face from another. The term "face recognition" is also often used to describe "face detection" (identifying whether an image contains a face at all) and "face analysis" (the assessment of certain traits, like skin color and age, based on the image of a face).

Face verification typically compares the image of a known individual against an image of, ideally, that individual, to confirm that both images represent the same person. Face identification generally involves comparing a sample image of an unknown individual against a collection of known faces and attempting to find a match. Some face recognition systems, instead of positively identifying an unknown person, 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.

Face recognition systems vary in their ability to identify people under challenging conditions such as poor lighting, low quality image resolution, and suboptimal angle of view (such as in a photograph taken from above looking down on an unknown person).

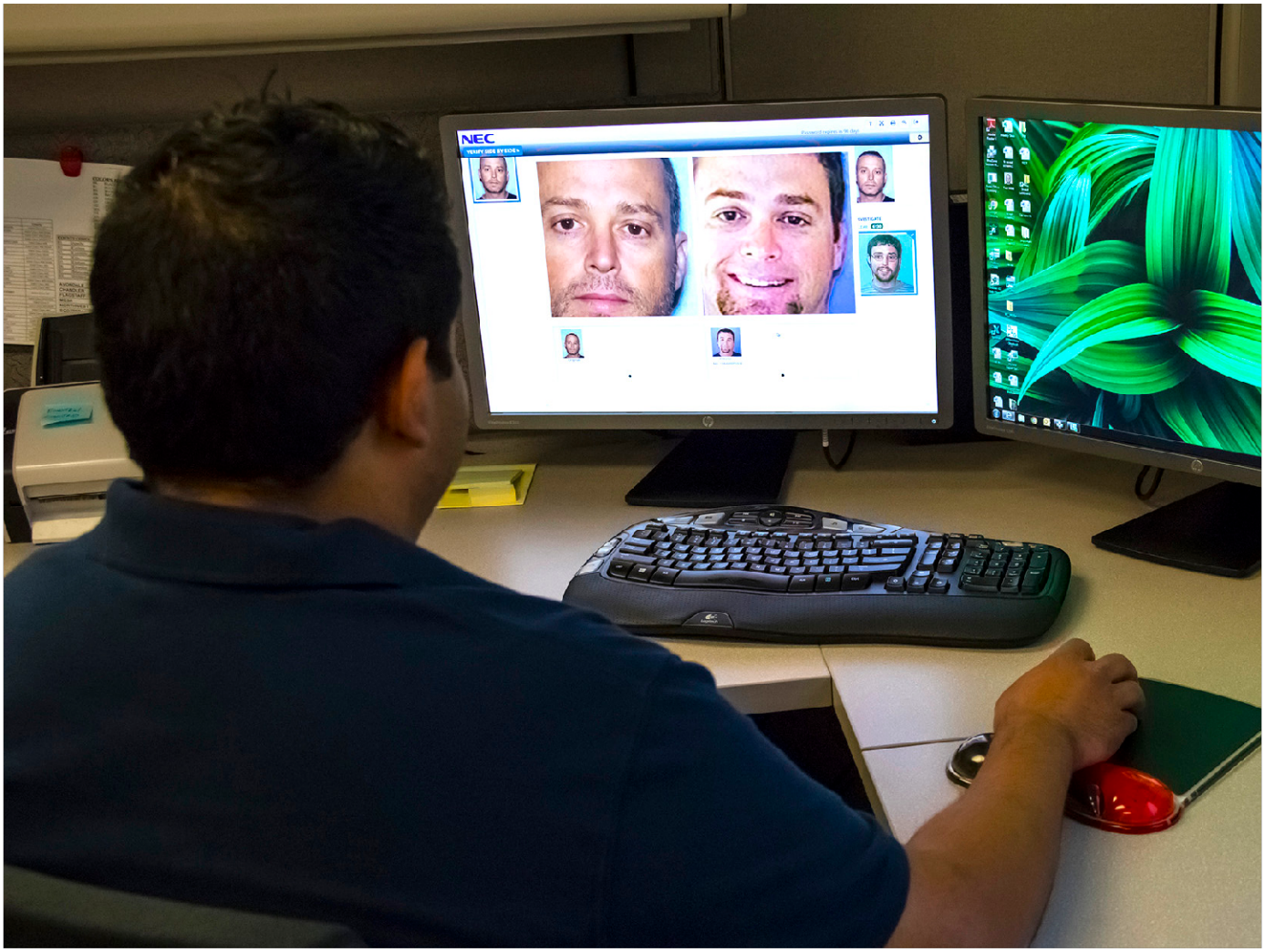
When it comes to errors, there are two key concepts to understand:

- A "false negative" is 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.
- A "false positive" is when the face recognition system does match a person's face to an image in a database, but that match is actually 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."

When researching a face recognition system, it is important to look closely at the "false positive" rate and the "false negative" rate, since 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 it is for the system to misidentify

result of a misidentification is that an innocent person goes to jail (like a misidentification in a mugshot database), then the system should be designed to have as few false positives as possible.

How Law Enforcement Uses Face Recognition



SOURCE: ADOT

An Arizona Department of Transportation analyst uses face recognition to compare an image.

Many local police agencies, state law enforcement, and federal agencies use face recognition in routine patrolling and policing. Scores of databases facilitate face recognition use at the local, state and federal level. Law enforcement may have access to face recognition systems through private platforms or through systems designed internally or by other government agencies. Law enforcement can query these vast

(CCTV), traffic cameras, or even photographs they've taken themselves in the field. Faces may also be compared in real-time against "hot lists" of people suspected of illegal activity. Federal law enforcement agencies, like the Department of Homeland Security (DHS) and the State Department, contribute to research and development, and many other agencies have stated their intentions to expand their use of face recognition.

Police agencies may use face recognition to try to identify suspects in a variety of crimes. While police often will assert that face recognition will help them to locate people who have committed violent crimes, there have been multiple instances in which the technology has been used in investigations of much lower-level offenses.

Following the murder of George Floyd in 2020 and the resulting protests and civil unrest, federal agencies used face recognition to identify individuals. Three agencies have also admitted using the technology to identify individuals present at the January 6, 2021 attack on the U.S. Capitol.

The use of face recognition by federal law enforcement agencies is widespread. Agencies use face recognition to generate investigative leads, access devices, and get authorization to enter particular physical locations. At least 20 of 42 federal agencies with policing powers have their own or use another government agency's face recognition system, according to a July 2021 report from the Government Accountability Office (GAO). Agencies reported accessing one or more of 27 different federal face recognition databases.

Face recognition systems in 29 states are accessed and used by federal law enforcement agencies; the extent of this use is not fully known, as at least 10 of the federal agencies accessing these systems do not track use of non-federal face recognition technology, despite GAO recommendations that they do so.

Law enforcement is increasingly using face recognition to verify the identities of individuals crossing the border or flying through U.S. airports. The Transportation Security Administration (TSA) is integrating face recognition into many of the country's airports. As of early 2023, TSA had introduced the technology to 16 major airports, and Customs and Border Protection (CBP) had implemented face recognition technology. at 32 airports for passengers leaving and entering the United States.

Some face recognition systems are based on the mugshots of individuals. Police collect mugshots from arrestees and compare them against local, state, and federal face recognition databases. Once an arrestee's photo has been taken, the mugshot will live on in one or more databases to be scanned every time the police do another criminal search.

recognition records. FBI allows state and local agencies "lights out" access to this database, which means no human at the federal level checks up on the individual searches. In turn, states allow FBI access to their own criminal face recognition databases.

FBI also has a team of employees dedicated just to face recognition searches called Facial Analysis, Comparison and Evaluation ("FACE") Services. FACE can access more than 400 million non-criminal photos from state Departments of Motor Vehicles (DMV) and the State Department; at least 16 U.S. states allow FACE access to driver's license and ID photos. As of 2019, the FBI had conducted nearly 400 thousand searches through FACE services.

Estimates indicate that over a quarter, at least, of all state and local law enforcement agencies in the U.S. can run face recognition searches on their own databases or those of another agency. As of September 2023, the EFF's Atlas of Surveillance, the largest database of known uses of surveillance technology by law enforcement, had cataloged nearly 900 municipal, county, and state agencies using face recognition.

SOURCE: AUTOMATED REGIONAL JUSTICE INFORMATION CENTER/SANDAG

A law enforcement officer in San Diego uses a handheld device to scan a face.

face recognition allows officers to use smartphones, tablets, or other portable devices to take a photo of a driver or pedestrian in the field and immediately compare that photo against one or more face recognition databases to attempt an identification.

More than half of all adults in the United States have their likeness in at least one face recognition database, according to research from Georgetown University. This is at least partially due to the widespread integration of DMV photographs and databases. At least 43 states have used face recognition software with their DMV databases to detect fraud, and at least 26 of states allow law enforcement to search or request searches of driver license databases, according to a 2013 Washington Post report; it is likely this number has since increased.

Local police also have access to privately-created face recognition platforms, in addition to federal systems. These may be developed internally, but increasingly, access is purchased through subscriptions to private platforms, and many police departments spend a portion of their budgets on access to face recognition platforms.

The Pinellas County Sheriff's Office in Florida, for example, maintains one of the largest local face analysis databases. As of June 2022, its database contains more than 38 million images and was accessible by 263 different agencies.

Face recognition may also be used in private spaces like stores and sports stadiums, but different rules may apply to private sector face recognition.

Who Sells Face Recognition

Law enforcement agencies once attempted to create and share their own facial recognition systems. Now there are many companies that sell face recognition products to identify and analyze individuals' faces at much lower costs than internal development.

Clearview AI is one such popular platform commonly used by law enforcement. Its database of more than 30 million photos, which is based on images scraped from a variety of online and public locations, is one of the most extensive known to be used.

MorphoTrust, a subsidiary of Idemia (formerly known as OT-Morpho or Safran), is another large vendors of face recognition and other biometric identification technology in the United States. It has designed systems for state DMVs, federal and state law enforcement agencies, border control and airports (including TSA PreCheck), and the state department.

Systems, FaceFirst, and NEC Global.

Threats Posed By Face Recognition

Face recognition poses threats to individual privacy and civil liberties and can be used in coordination with other technologies in ways that are additionally threatening to individual rights and legal protections.

Face recognition data is easy for law enforcement to collect and hard for members of the public to avoid. Faces are in public all of the time, but unlike passwords, people can't easily change their faces.

Law enforcement agencies are increasingly sharing information with other agencies and across jurisdictions. Cameras are getting more powerful and more ubiquitous. More photographs and video are being stored and shared for future analysis. It is very common for images captured by a particular agency or for a specific purpose to be used in a face recognition system.

Face recognition data remains prone to error, even as face recognition improves, and one of the greatest risks of face recognition use is the risk of misidentification. At least six individuals have been misidentified by face recognition and arrested for crimes that they did not commit: Robert Williams, Michael Oliver, Nijeer Parks, Randal Reid, Alonzo Sawyer, and Porcha Woodruff. Being misidentified by face recognition can result in unwarranted jail time, criminal records, expenses, trauma, and reputational harm.

The FBI admitted in its privacy impact assessment that its system "may not be sufficiently reliable to accurately locate other photos of the same identity, resulting in an increased percentage of misidentifications." Although the FBI purports its system can find the true candidate in the top 50 profiles 85% of the time, that's only the case when the true candidate exists in the gallery. If the candidate is not in the gallery, it is quite possible the system will still produce one or more potential matches, creating false positive results. These people—who aren't the candidate—could then become suspects for crimes they didn't commit. An inaccurate system like this shifts the traditional burden of proof away from the government and forces people to try to prove their innocence. Face recognition gets worse as the number of people in the database increases. This is because so many people in the world look alike. As the likelihood of similar faces increases, matching accuracy decreases.

Face recognition systems are particularly bad at identifying Black, Brown, Asian, and non-gender conforming individuals. Face recognition software also misidentifies other

a disproportionate number of African Americans, Latinos, and immigrants, due in part to racially-biased police practices; the use of face recognition technology has a disparate impact on people of color. Even if a company or other provider of a face recognition algorithm updates its system to be more accurate, this does not always mean that law enforcement agencies using that particular system discontinue use of the original, flawed system.

Individual privacy and autonomy of all people are threatened by the reach of constant tracking and identification. Face recognition data is often derived from publicly-available photos, social media, and mugshot images, which are taken upon arrest, before a judge ever has a chance to determine guilt or innocence. Mugshot photos are often never removed from the database, even if the arrestee has never had charges brought against them.

Face recognition can be used to target people engaging in protected speech. For example, during protests surrounding the death of Freddie Gray, the Baltimore Police Department ran social media photos through face recognition to identify protesters and arrest them. Of the 52 agencies analyzed in a report by Georgetown Center on Privacy and Technology, only one agency, the Ohio Bureau of Criminal Investigation, has a face recognition policy expressly prohibiting the use of the technology to track individuals engaged in protected free speech.

Face recognition may also be abused by individual officers or used for reasons unrelated to investigations or their work. Few face recognition systems are audited for misuse. Less than 10 percent of agencies admitting to face recognition use in the Georgetown survey had a publicly-available use policy. Only two agencies, the San Francisco Police Department and the Seattle region's South Sound 911, restrict the purchase of technology to those that meet certain accuracy thresholds. Only one—Michigan State Police—provides documentation of its audit process.

There are few measures in place to protect everyday Americans from the misuse of face recognition technology. In general, agencies do not require warrants. Many do not even require law enforcement to suspect someone of committing a crime before using face recognition to identify them. While the Illinois Biometric Information Privacy Act requires notice and consent before the private use of face recognition tech, this only applies to companies and not to law enforcement agencies.

Some argue that human backup identification (a person who verifies the computer's identification) can counteract false positives. However, research shows that, if people lack specialized training, they make the wrong decisions about whether a candidate

personnel review and narrow down potential matches.

Some cities have implemented bans on the use of face recognition. However, these bans and restrictions are constantly being undermined and adjusted at the behest of law enforcement. Virginia, for example, enacted a complete ban on police use of face recognition in 2021, only to roll back those restrictions the following year. In California, a three-year moratorium on face recognition passed in 2019, but the restrictions it implemented have not been reinstated since the temporary ban expired at the beginning of 2023. New Orleans replaced its 2020 ban with regulated access for the local police department. As face recognition databases expand their reach and law enforcement agencies push to use them, the threats posed by the technology persist.

EFF's Work on Face Recognition

EFF supports meaningful restrictions on face recognition use both by government and private companies, including total bans on the use of the technology. We believe that face recognition in all of its forms, including face scanning and real-time tracking, pose threats to civil liberties and individual privacy.

We have called on the federal government to ban the use of face recognition by federal agencies. We have testified about face recognition technology before the Senate Subcommittee on Privacy, Technology, and the Law, as well as the House Committee on Oversight and Government Reform Hearing on Law Enforcement's Use of Facial Recognition Technology. We also participated in the NTIA face recognition multistakeholder process but walked out, along with other NGOs, when companies couldn't commit to meaningful restrictions on face recognition use. EFF has supported local and state bans on facial recognition and opposes efforts to expand its use. In New Jersey, EFF, along with Electronic Privacy Information Center (EPIC) and the National Association of Criminal Defense Lawyers (NACDL), filed an amicus brief supporting a defendant's discovery rights to know the face recognition algorithms used in their case, and the court agreed, a win for due process protections.

EFF has consistently filed public records requests to obtain previously secret information on face recognition systems. We've pushed back when cities haven't properly complied with our requests, and we even sued the FBI for access to its face recognition records. In 2015, EFF and MuckRock launched a crowdsourcing campaign to request information on various mobile biometric technologies acquired by law enforcement around the country. We filed an amicus brief, along with the ACLU of Minnesota, demanding the

program that were requested by one local participant in the project.

EFF has repeatedly sounded the alarm on face recognition and work to educate the public about the harms of facial recognition, including through initiatives like our "Who Has Your Face" project, which helps individuals learn about the databases in which their image likely exists. EFF has supported local bans on face recognition and provides resources to activists who are fighting face surveillance.

EFF Legal Cases

State of New Jersey v. Arteaga

EFF v. U.S. Department of Justice

Tony Webster v. Hennepin County and Hennepin County Sheriff's Office

Willie Allen Lynch v. State of Florida

Suggested Additional Reading

Garbage In, Garbage Out (Georgetown Law, Cennter on Privacy and Technology)

Face Off: Law Enforcement Use of Face Recognition Technology (EFF)

The Perpetual Line-Up (Georgetown Law Center on Privacy and Technology)

Police Surveillance and Facial Recognition: Why Data Privacy Is Imperative for Communities of Color (Brookings Institute)

Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy (Government Accountability Office)

Federal Agencies' Use and Related Privacy Protections (Government Accountability Office)

California Cops Are Using These Biometric Gadgets in the Field (EFF)

Face Recognition Performance Role of Demographic Information (IEEE)

Privacy Impact Assessment for the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit (FBI)

Most recently updated September 5, 2023

TECHNOLOGIES