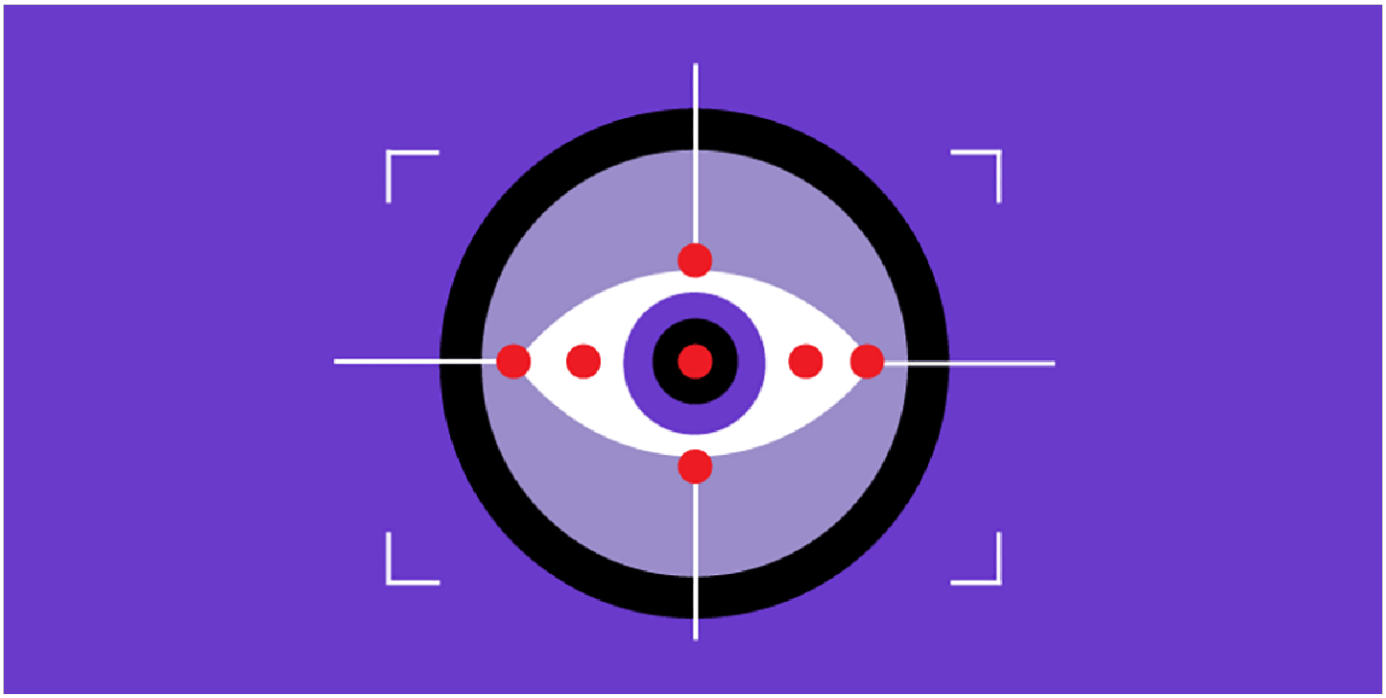
STREET LEVEL SURVEILLANCE



BIOMETRIC SURVEILLANCE

Biometric surveillance encompasses a collection of methods for tracking individuals using physical or biological characteristics, ranging from fingerprint and DNA collection to gait recognition and heartbeat tracking.

These methods rely heavily on algorithms to identify certain characteristics from a sample, like the image of a face or the sound of a voice, and match it to one other particular sample or a group of samples.

Biometric identification can be flawed due to issues in the algorithm, gaps and biases in the training data, and problems with the samples used. For example, gait analysis, the use of a walking pattern to identify a person, is dependent on movement tåhat can vary based on the level of fatigue, footwear, environmental conditions, and health of a person. And voice recognition depends on voiceprints, graphical representations of a voice, which can be mimicked by AI-generated spoofs.

Because biometric features are unique and irreplaceable, this type of surveillance is particularly concerning. A person cannot simply change their eyes or DNA in the way they can change a password or credit card. Tracking done in this way can be extremely and persistently intrusive. Further, the black box nature of many types of biometric identification can perpetuate patterns of biased policing and result in errors that can be difficult to defend against.

DNA Collection and Searches

information such as our ancestry, biological relationship, and propensity for certain medical conditions. Although DNA has been used by law enforcement since the 1980s, technology relating to it, and the methods used by the police, have evolved significantly.

In recent decades, DNA collection has become mandatory from those convicted of or even arrested for many crimes. In the United States, that information is entered into the national Combined DNA Index System (CODIS) DNA database, which is maintained by the FBI. This database contains nearly 16 million offender profiles and 5 million arrestee profiles.

Previously, a useful forensic sample could only be obtained from blood, semen, or other bodily fluids. However, today forensic investigators can detect, collect, and analyze trace amounts of DNA from objects a person merely touches.

Genetic Genealogy Searches

Over the past decade, there has been a proliferation of genetic genealogy sites. These sites are run by private companies and offer to help people find long-lost relatives, learn more about their families and ancestors, and identify their own traits and health predispositions. There are two main types of consumer genetic databases:closed databases like Ancestry and 23andMe, where the company controls and limits search results and direct access to other users' data (most of which restrict law enforcement access to warranted searches); and open databases like GEDmatch, FamilyTreeDNA, and MyHeritage, which offer consumers much broader access and allow users to search their own genetic data against genetic information submitted by all other site users. For the open databases, users upload extensive genetic data, either as a biological sample or an electronic file containing their raw genotyped DNA data, which the company converts into a genetic genealogy profile.

Forensic genetic genealogy (FGG) searches differ from traditional criminal DNA searches in several respects. First, genetic genealogy databases are privately maintained and contain DNA data voluntarily submitted by consumers. There are no laws specifically regulating how these sites collect, handle, and share data. In contrast, DNA data entered into CODIS—which is made up of national, state, and local DNA databases—is subject to state and federal statutes that govern exactly how, when, and from whom it can be collected, as well as expungement from the database.

Second, genetic genealogy databases collect and store significantly more—and more revealing—genetic data than the limited information collected and entered into CODIS. CODIS profiles typically consist of one or two alleles at each of the 13 to 20 loci that are part of CODIS's "Core Loci." These short tandem repeat ("STR") DNA markers are taken from "non-coding" parts of the human genome. In contrast, genetic genealogy profiles are made up of more than half a million single nucleotide polymorphisms ("SNPs") that can reveal family members and distant ancestors as well as predict a person's propensity for various diseases like breast cancer and traits like addiction and drug response. Both STR and SNPs can be inherited from and passed on by anyone. This means that while both CODIS and genetic genealogy databases can identify some biological familial relationships, the latter can also predict indirect and very distant familial relationships.

Police have used FGG searches in a number of high profile cases, including ones implicating innocent people who are then subject to police investigation and interference with their lives. Although the most famous example of an FGG search is that which identified the "Golden State Killer," an earlier search in

Idaho cold case led police to suspect an innocent man. Even without FGG, DNA matches have led officers to suspect—and jail—the wrong person. In 2012, a California man spent five months in jail after a database search linked his DNA to DNA found on the fingernails of a murder victim—although he was in the hospital when the murder occurred. Prosecutors believe paramedics may have transferred his DNA to the murder victim when they responded to the crime scene hours after dropping him off at the hospital.

In an effort to ensure FGG searches accord with constitutional rights, EFF has filed briefs in multiple cases challenging the collection of DNA and FGG searches. We have also advocated for legislative restrictions on how FGG searches are conducted.

Probabilistic Genotyping Software

Although DNA is unique, DNA samples used in criminal prosecutions are generally of low quality, making them particularly complicated to analyze. A new generation of software called probabilistic genotyping software is often used these days to determine whether a suspect's DNA matches samples found at a crime scene. However, this software is fraught with issues of accuracy, human imputed bias, and opaque processes and algorithms.

When the results of this software are used in criminal cases, defendants should have the right to evaluate any DNA analysis tool's source code. It is critical to determine the weight that should be given to such a tool's results—and whether these programs are reliable enough to be used at all in the criminal justice system.

EFF has successfully argued in state and federal courts that information regarding probabilistic genotyping software must be provided to the defense.

Tattoo Recognition

Tattoo recognition technology uses images of people's tattoos to identify them, reveal information about them such as their religion or political beliefs, and associate them with people with similar tattoos. The technology is being actively developed by private companies with the support of federal agencies, state law enforcement, and universities. Researchers test and train the technology using photographs of incarcerated people or from social media, raising critical issues of ethics, privacy, and our First Amendment rights. Tattoo recognition is a form of biometric technology in the same category as face recognition, fingerprinting, and iris scanning.

How Tattoo Recognition Works

Tattoo recognition functions in a similar manner as face recognition. Once an image of a tattoo is captured and submitted to the system, image recognition software creates a mathematical representation, analyzes it for specific details, and matches those against images already in the database. Humans can also tag these images with metadata to further describe or categorize them.

What Kinds Of Data Are Collected for Tattoo Recognition

Tattoo recognition often captures multiple images of an individual's tattoos and may also capture a person's whole face or entire body.

The National Institute on Standards and Technology (NIST) has developed a series of "Best Practices" for capturing images of tattoos for use with tattoo recognition technology. This includes taking two photographs of each tattoo, one that narrows in on the tattoo itself and another that more clearly shows where tattoos are located on the body. For large tattoos, NIST encourages police to take a full photo of the tattoo in its entirety, followed by photos of particular areas of interest in the tattoo. It is important to note that in detention environments, images of tattoos may be collected from the entire body, including areas that would not be publicly visible, such as the upper legs, chest, and genital areas.

These tattoos are often tagged with metadata about the tattoo, including the position on the body and ink color. The recommended tagging system (ANSI/NIST-ITL Standard) has dozens of codes to categorize the imagery of the tattoo, ranging from general categories such as political symbols and sports icons to very specific images such as a dragon or the American flag.

Law enforcement may also collect images in the field during routine police stops using regular cameras or mobile biometric devices.

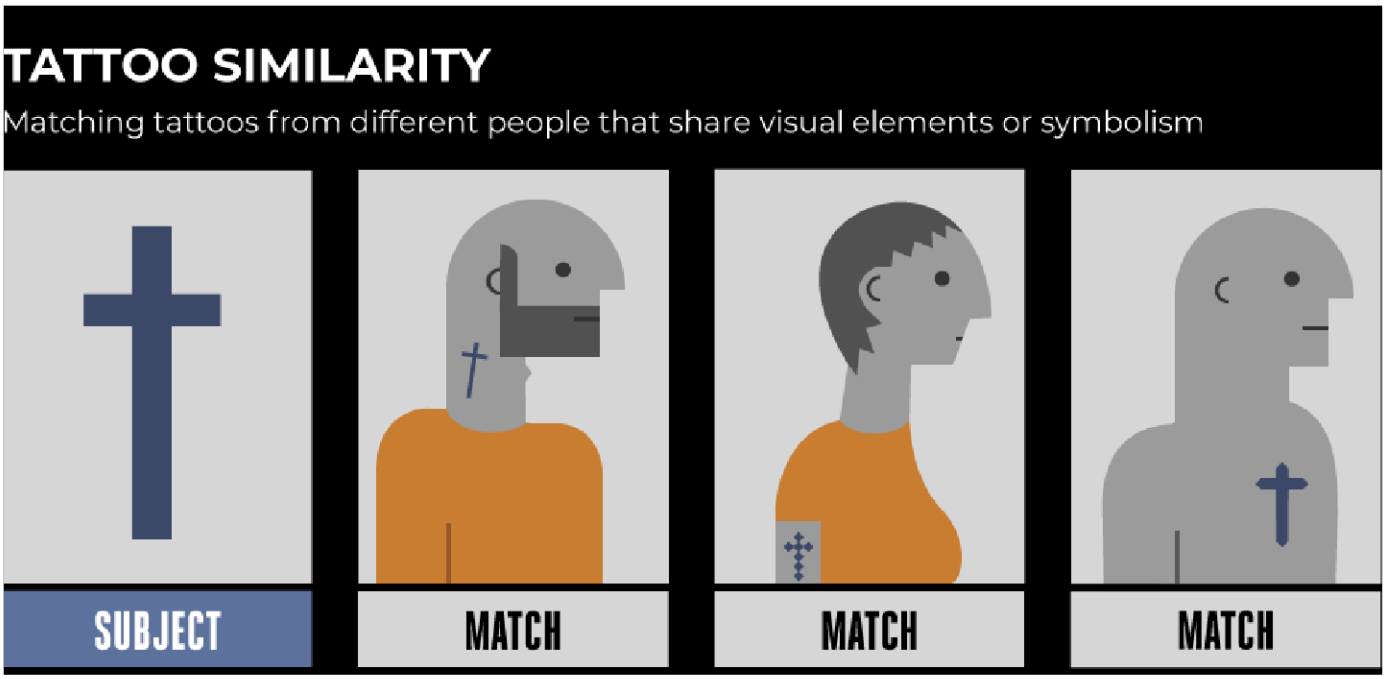
In addition, tattoo recognition software may ingest images found online on websites or social media.

How Law Enforcement Uses Tattoo Recognition

Before automation, tattoo recognition often involved maintaining binders of tattoo photographs, similar to a mugshot book. In recent years, police departments have begun digitizing these images and adding them to databases, along with tagged metadata. These have been used to identify alleged suspects and victims of crime.

In research funded by the FBI, NIST identified several specific uses for tattoo recognition technology by law enforcement. These include identifying a person by their tattoos, as well as identifying a suspect

person's tattoos by matching it to similar imagery and mapping out connections between people with similar tattoos.



SOURCE: EFF

One real-word deployment of tattoo recognition technology was "Gang Graffiti Automatic Recognition and Interpretation" (GARI), a project between Purdue University and the Indiana State Police that allowed law enforcement around the country to share photos of graffiti and gang tattoos, along with time stamps and GPS coordinates, through a web app. The recognition software promised to allow law enforcement to map out gang activity and growth in communities. The program was supported by the U.S. Department of Homeland Security, which believes it can be used to identify international gangs involved in drug and human trafficking.

The Arizona Department of Public Safety has been using tattoo recognition since 2022, using a system built on more than a million images taken during criminal bookings. The agency receives requests to send images through the system from Arizona police departments.

Who Sells Tattoo Recognition Technology

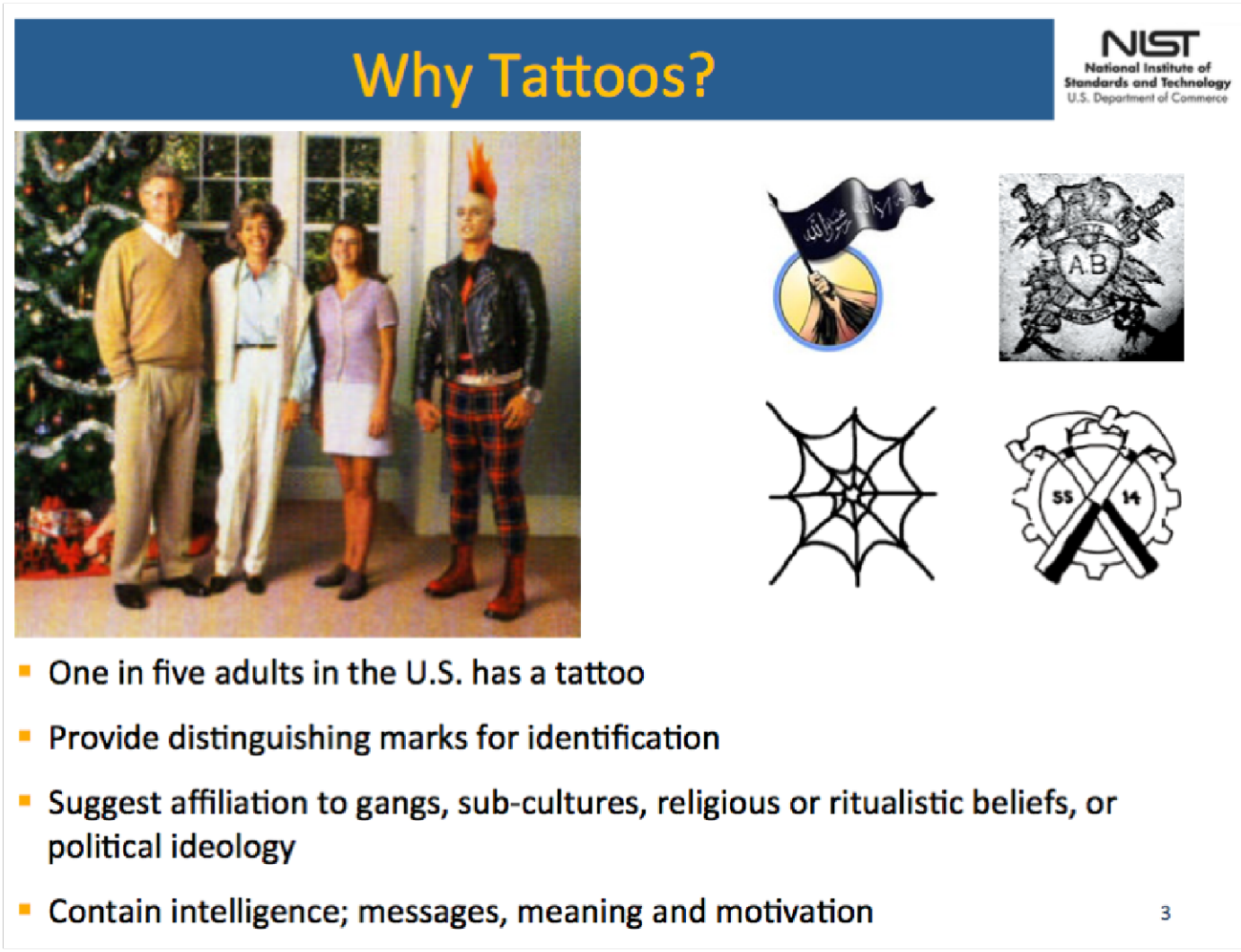
Idemia (formerly known as OT-Morpho or Safran) is one of the largest vendors of biometric identification technology in the United States, including tattoo recognition technology. Other vendors include Face Forensics, DataWorks, Rank One Computing, and Neurotechnology, which includes tattoo recognition in its MegaMatcher collection of biometric tools.

Notably, multiple universities have worked to develop this technology for use by law enforcement and private industry. Idemia is working with the University of Michigan, while the Indiana State Police collaborate with Purdue University. Research institutions such as the French Alternative Energies and Atomic Energy Commission, the Fraunhofer Institute of Optronics, System Technologies and Image

project.

Threats Posed by Tattoo Recognition

Tattoos have meaning for the wearers, whether it's a cross representing their religion, a portrait of their children, or simply the logo for their favorite band. While many of threats posted by face recognition carry over to this and other forms of biometrics, tattoos are unique because they implicate many First Amendment rights and are elective. In fact, in its research, NIST specifically claimed, "Tattoos provide valuable information on an individual's affiliations or beliefs and can support identity verification of an individual." By using this technology, a law enforcement official could use tattoos as a proxy to create lists of people based on their religion, nationality, political ideologies, or common interests.



SOURCE: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

A slide from a NIST presentation on Tattoo Recognition Technology

However, assumptions made about tattoos can be wrong. For example, a Jewish person who wears a Star of David tattoo could be automatically affiliated with a member of a Chicago street gang whose members also wear six-pointed star tattoos. Alternatively, a person who obtained a gang-affiliated

with a gang in decades.

There is also a threat that tattoos may be used to target immigrants for deportation. An immigrant who received Deferred Action for Childhood Arrivals status was detained and fast-tracked for deportation because immigration officials claimed he had a gang tattoo. The immigrant said the tattoo actually signified his place of birth. News outlets have reported that immigrants are seeking tattoo removal services to avoid being caught up in a deportation dragnet.

Tattoo recognition technology may also be used to expose or surveil people on the Internet. German researchers, for example, designed technology that could match photos on an online tattoo website to Germany's police database.

EFF's Work on Tattoo Recognition

Through a series of Freedom of Information Act (FOIA) and state-level public records act requests, EFF has exposed a variety of tattoo recognition programs.

Much of our focus has been in investigating NIST's Tattoo Recognition Program. Our research revealed that NIST scientists had ignored ethical obligations for conducting experiments with images taken from inmates. They received a waiver of these obligations only after the research had been completed. Through direct advocacy and a grassroots campaign, EFF successfully pressured NIST to overhaul its privacy safeguards and to redact sensitive images from public materials.

However, EFF does not believe that NIST has gone far enough and has pushed the government to withdraw its use of tattoo recognition.

In November 2017, we filed a lawsuit against the U.S. Department of Commerce, the U.S. Department of Justice, and the U.S. Department of Homeland Security to force the release of documents, including the names of the institutions that received images of inmates through NIST's program. The lawsuit also seeks to uncover to what extent the FBI influenced the research, which may have triggered additional ethical scrutiny. EFF won access to these records, learning the names of agencies that were using the database. EFF pushed these offices to cease their use of the system. Roughly a third of institutions that we believe requested problematic and exploitive data as part of a government automated tattoo recognition challenge deleted the data or reported that they had never received or used it.

EFF Legal Cases

EFF v. U.S. Department of Commerce, Department of Justice, Department of Homeland Security

For More Information

5 Ways Law Enforcement Will Use Tattoo Recognition Technology (EFF)

Tattoo Recognition Research Threatens Free Speech and Privacy (EFF)

National Institute of Standards and Technology (NIST) - Tattoo Recognition Technology Program

Iris recognition

Iris recognition or iris scanning is the process of using visible and near-infrared light to take a high-contrast photograph of a person's iris. It is a form of biometric technology in the same category as face recognition and fingerprinting.

Advocates of iris scanning technology claim it allows law enforcement officers to compare iris images of suspects with an existing database of images in order to determine or confirm the subject's identity. They also state that iris scans are quicker and more reliable than fingerprint scans since it is easier for an individual to obscure or alter their fingers than it is to alter their eyes.

Iris scanning raises significant civil liberties and privacy concerns. It may be possible to scan irises from a distance or even on the move, which means that data could be collected surreptitiously, without individuals' knowledge, let alone consent. There are security concerns as well: if a database of biometric information is stolen or compromised, it is not possible to get a new set of eyes like one would get a reissued credit card number. And iris biometrics are often collected and stored by third-party vendors, which greatly expands this security problem.

How Iris Recognition Works

Iris scanning measures the unique patterns in irises, the colored circles in people's eyes. Biometric iris recognition scanners work by illuminating the iris with invisible infrared light to pick up unique patterns that are not visible to the naked eye. Iris scanners detect and exclude eyelashes, eyelids, and specular reflections that typically block parts of the iris. The final result is a set of pixels containing only the iris. Next, the pattern of the eye's lines and colors are analyzed to extract a bit pattern that encodes the information in the iris. This bit pattern is digitized and compared to stored templates in a database for verification (one-to-one template matching) or identification (one-to-many template matching).

Iris scanning cameras may be mounted on a wall or other fixed location, or they may be handheld and portable. Researchers at Carnegie Mellon University are developing long-range scanners that could even be used to capture images surreptitiously from up to 40-feet away.

What Kinds of Data Are Collected for Iris Recognition

Iris scanners collect around 240 biometric features, the amalgamation of which are unique to every eye. The scanners then create a digital representation of that data. That numeric representation of information extracted from the iris image is stored in a computer database.

Iris scanning is sometimes used in conjunction with other biometrics, such as fingerprints and face recognition.

Who Sells Iris Recognition Technology

Identification Technologies, Crossmatch, EyeCool, EyeLock, Gemalto, Idemia, Iridian Technologies, Iris Guard, Iris ID, IriTech, NEC, Neurotechnology, Panasonic, SRI International, Tascent, Thales, and Unisys. Many of these companies offer multiple forms of biometric identification technology.

How Law Enforcement Uses Iris Recognition

The Federal Bureau of Investigation added iris recognition to its Next Generation Identification (NGI) System in December 2020. Since then, the FBI has encouraged local policing and prison agencies to utilize and contribute samples to its Iris Recognition program. Its database of more than 1.3 million samples is based on contributions from federal, state, and local law enforcement. The Texas Department of Criminal Justice was among participating agencies, contributing more than 110,000 iris samples from incarcerated individuals.

The U.S. military has used iris scanning devices to identify detainees in Iraq and Afghanistan. For example, the handheld biometrics recorder SEEK II allows military personnel to take iris scans, fingerprints, and face scans and port the data back to an FBI database in West Virginia in seconds, even in areas with low connectivity. As is often the case with cutting-edge surveillance technologies developed for use in foreign battlefields, similar iris scanning technology has since been deployed by police departments across the U.S.

The New York City Police Department was among the first police departments to begin using iris recognition. The department installed BI2 Technologies' mobile MORIS (Mobile Offender Recognition and Information System) in the fall of 2010. Although New York City's use of iris scanning in jails was supposed to be voluntary, there have been reports of arrestees being held longer for declining iris photographs. The NYPD also uses iris recognition in identity verification when an individual is arraigned.

Prisons, such as the Rhode Island Department of Corrections, and agencies, like the Tennessee Bureau of Investigation, have also begun using the technology. An EFF survey of California law enforcement agencies in 2015 found that sheriff offices in Orange County and Los Angeles County had plans to implement iris scanning technology.

Iris recognition devices have been installed in every sheriff's department along the U.S.-Mexico border. The vendor BI2 offered these sheriffs free three-year trials of its stationary iris capture devices to be used in inmate intake facilities, and it has said it would eventually provide mobile versions as well. The iris templates generated with the mobile app can be compared against hundreds of thousands of other iris templates in less than 20 seconds. The scans will be added to BI2's private database, which already has close to a million iris scans collected from over 180 law enforcement jurisdictions across the country.

The B12 database is housed by a third-party vendor in an undisclosed location in San Antonio, Texas, and in three other disaster backup facilities. A BI2 executive told The Intercept that it is the largest database of its kind in North America.

The Department of Homeland Security utilizes the Homeland Advanced Recognition Technology (HART) System, the agency's primary biometric database, which is accessible to DHS components, law enforcement partners, and international entities. HART includes access to a 1-to-Many iris database, allowing users to compare an iris to a dataset of individuals' biometric records containing iris images. Customs and Border Protection employs at least four iris scanners at checkpoints and has begun

have tested iris recognition as a means of limiting access to authorized students, family, and faculty.

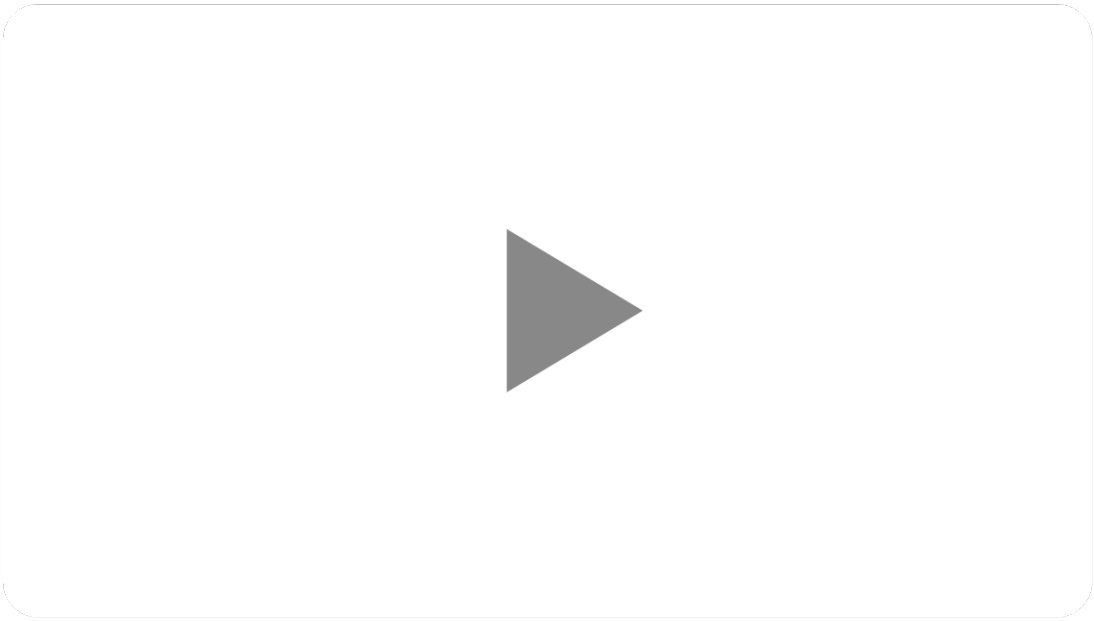
Threats Posed by Iris Recognition

Perhaps the biggest threat of iris scanning is the danger of a national database that can track people covertly, at a distance or in motion, without their knowledge or consent. This raises significant civil liberties and privacy concerns which increase as iris data are collected from more and more people. It may be possible for law enforcement officers to use long-range iris scanners on people simply glancing in their rear view mirror after being pulled over. At some point, it's possible that every person could be identified at any place, even if they are not suspected of committing a crime.

There also are grave concerns with local law enforcement sharing biometric data to help federal immigration agencies such as the U.S. Immigration and Customs Enforcement (ICE), which has direct access to many law enforcement databases.

No biometric is foolproof. A 2009 research study showed that patients with acute iris inflammation (also known as iritis or anterior uveitis) caused current iris recognition systems to fail. A 2012 report from the National Institute of Standards & Technology (NIST) showed that iris recognition technology used to identify an individual in a crowd was inaccurate 1 to 10% of the time. Quality problems were due to poor subject presentation (e.g., a closed eye, rotated iris or off-axis gaze), problems with the capture environment (such as motion or defocus blur, reflections due to excessive ambient lighting or broken LEDs), image processing or storage (such as image compression or corruption), and unusual characteristics inherent in the individual (such as an abnormal pupil shapes). The miss rates (or false negative error rates) for single irises ranged from 2.5% to 20% or higher.

It is also possible to trick or bypass iris scanners. In 2012, security researchers at the Universidad Autonoma de Madrid were able to recreate images of irises from digital codes stored in security databases. Hackers with the Chaos Computer Club in Germany were able to bypass the iris-based authentication in Samsung's Galaxy S8 smartphone (despite the company's claims of "airtight security,") by simply taking a digital photograph of the owner's face in night shot mode, printing it out, superimposing a contact lens on the image, and holding the image in front of the locked phone.



And then there is the issue of data security. It's unclear what steps, if any, law enforcement agencies are taking to secure the sensitive biometric data they collect. Databases of iris biometric are a honeypot of sensitive, highly personal data that will be targeted by criminals. Data breaches and hacks happen. Law enforcement can also be careless with the equipment used to collect and store this data. In one example, a military device used to scan individuals' irises was sold on eBay with the information still on it.

Biometric information is a special risk because it's not possible to revoke, cancel, or reissue an eyeball if digital biometric information is stolen or compromised. Making the risk of data breach even greater, law enforcement often stores its iris biometrics on databases operated by vendors and other private third parties. This also gives companies access to and control over criminal justice data, which many of their employees can access remotely.

Suggested Additional Reading:

The Biometric Frontier: "Show Me Your Papers" Becomes "Open Your Eyes" as Border Sheriffs Expand Iris Surveillance (The Intercept)

How Iris Recognition Works (Cambridge University)

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

Five Minutes Primers: Iris Recognition (Policing Project)

IREX 10: Identification Track (National Institute of Standards and Technology)

Most recently updated October 1, 2023