No Hiding

More police departments are using facial recognition to help solve crimes.

PHOTO CREDITS

WATCH A VIDEO about facial recognition in China & Ecuador at UPFRONTMAGAZINE.COM

Your Face?

But as the use of the technology grows, so do privacy concerns. BY JOE BUBAR

MASKOT/GETTY IMAGES (TEENS); SAUL LOEB/AFP/GETTY IMAGES (SURVEILLANCE)

It was all caught on camera. In 2017, a woman entered a store in Cornelius, Oregon, stashed a $130 pair of boots in her purse, and walked out.

The Washington County Sheriff's Office pulled images of her face that had been captured by the security cameras. They uploaded the images to their newest crime-solving tool: a facial recognition system. Within seconds, the system came up with a digital lineup of potential matches. When a deputy spoke to one of these women the next day, she confessed to the crime and was charged with theft. The case might have never been cracked in the past. Now, it was solved in only a day.

That's just one of many recent examples of police departments using facial recognition to help solve crimes. They've been able to crack a variety of cases, from shoplifting to assaults and mass shootings.

But the growing use of this technology is fueling a heated debate. Some are calling it a breakthrough in policing. Civil liberties advocates don't see the technology that way. They say it isn't always accurate and could lead to wrongful arrests, especially of people of color. They also argue that the use of facial recognition is an invasion of privacy. And they fear it could be used for mass surveillance. That means it might help the police and government agencies secretly watch people.

"This is the most pervasive and risky surveillance technology of the 21st century," says Alvaro Bedoya, director of Georgetown Law's Center on Privacy & Technology (C.P.T.).

Those concerns led San Francisco to take action. Last spring, the city became the first in the U.S. to ban the police and other city agencies from using facial recognition. San Francisco's police department hadn't used facial recognition yet. The move was largely precautionary, but it could spark similar legislation elsewhere. In fact, other cities are already considering bans.

The Fourth Amendment protects against unreasonable searches and seizures.

But many people argue that facial recognition is a powerful and efficient tool for keeping people safe. It could also be used for finding missing people. Instead of banning the technology, they say cities should create rules for how it's used.

"It is ridiculous to deny the value of this technology in securing airports and border installations," says Jonathan Turley, a constitutional law expert at George Washington University in Washington, D.C. "It is hard to deny that there is a public safety value to this technology."

A Breakthrough in Policing?

You're probably already familiar with facial recognition. It's used to tag friends on Facebook, unlock iPhones, and add filters on Snapchat.

It's becoming increasingly common in police departments too. Although it's difficult to say exactly how many use the technology, a 2016 C.P.T. study offers at least one estimate. It found that at

Facial recognition for law enforcement on display at a tech conference in Washington, D.C.

least a quarter of state and local police departments have the ability to run facial recognition searches.

Typically, police upload an image of someone to a computer with facial recognition software. The image could come from a phone. It could also come from any of the many cameras that we pass by each day. You can spot these cameras on buildings, on street corners, or in businesses and stores. The software scans the image and compares it to a database of known people. That might include a collection of mug shots from previous arrests. Thirty-one states also allow police to access driver's license photos, according to the C.P.T. study (*see "How Facial Recognition Works," facing page*).

The technology can search through databases of millions of people in mere seconds. Police say it saves them valuable time. In New York City alone, it led to nearly 1,000 arrests in 2018. Facial recognition has been helpful to police in other parts of the country. It helped lead to the arrest of a trio of suspected jewel thieves and people who the authorities said were trying to enter the U.S. under fake names. And it aided police in catching a man who killed five people in a mass shooting at the offices of a Maryland newspaper in 2018.

Last December, police in Pennsylvania used the technology to nab a man who they say had assaulted a 15-year-old back in 2016. "If it wasn't for facial recognition, it would still be an open case," says Michael Zinn, an officer in York, Pennsylvania.

A map of all the cameras that Detroit's police can access. The cameras are hooked up to a facial recognition system that works in real time.

Biases & Mass Surveillance?

But there are concerns about the technology's accuracy. The Massachusetts Institute of Technology recently conducted a study looking into these concerns. They studied the facial recognition systems created by I.B.M., Microsoft, and Amazon. They found that the three systems were much better at identifying the gender of white men's faces than that of darker-skinned or female faces.

We often think of computers as objective. But it's actually not uncommon for people's biases to creep into technology. In this case, experts point to the people who trained the systems. These programmers typically used databases that contained more white people than people of color. As a result of these flaws, some people worry that African Americans, women, and others might be wrongly identified and arrested.

But police departments say they don't rely on facial recognition as definitive evidence. They claim that it's only used to get leads they might not otherwise have discovered. And all three companies say they've improved their systems.

But even with better accuracy, there are broader privacy concerns. Civil liberties advocates point out that these systems are often being used without people's knowledge or consent. They argue that it violates the Fourth Amendment's ban on unreasonable searches and

Taylor Swift reportedly used facial recognition at a concert to identify stalkers.

FACING THE FUTURE

From stadiums to schools, more and more places are experimenting with facial recognition.

When fans at a recent Taylor Swift concert at the Rose Bowl stadium in Los Angeles walked up to a kiosk playing videos of the pop star, they had no idea their picture was being taken. But a hidden camera in the kiosk reportedly sent images of their faces to a command center in Nashville, where facial recognition software cross-referenced the photos with a database of people who'd been identified as potential stalkers of the singer.

That's part of a growing trend: Facial recognition is being used in more and more places, and not just by the police.

At a terminal at Hartsfield-Jackson Atlanta International Airport, passengers flying with Delta Air Lines no longer have to show their passports when checking in and going through security. Instead, they can simply look at a screen with facial recognition software that compares their faces to passport photos in a database.

And as of this year, Lockport City School District in New York is using a facial recognition system that can spot people carrying guns, as well as anyone who isn't supposed to be on campus, such as students who've been suspended.

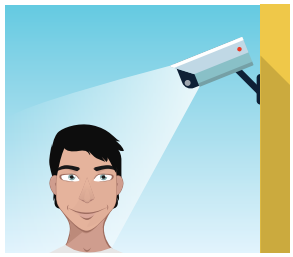
Proponents of facial recognition point to these examples as just a few of the ways that the technology can keep us safer and make our lives easier. But others argue that there's a risk in having it in so many places.

"It's psychologically unhealthy when people know they're being watched in every aspect of the public realm, on the streets, in parks," Aaron Peskin, a San Francisco city supervisor, told the Associated Press. "That's not the kind of city I want to live in."

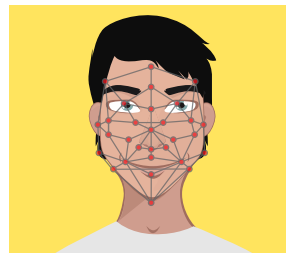
CITY OF DETROIT OPEN DATA PORTAL/PROJECT GREEN LIGHT (MAP); JIM WEST/ALAMY STOCK PHOTO (CAMERA); KEVIN MAZUR/TAS18/GETTY IMAGES (TAYLOR SWIFT)

HOW FACIAL RECOGNITION WORKS

Half of all Americans have their images, such as a driver's license photo, stored on at least one facial recognition database searchable by law enforcement agencies. Here's how those photos can be used to identify a suspect.



1. CAPTURING
A camera collects an image of an unknown person's face. Cameras can be mounted on traffic lights, on buildings, or inside businesses.



2. EXTRACTING
Software identifies facial features in the image and defines them as a set of values. These data points make up the person's unique facial profile.

3. COMPARING
The facial profile is compared with those of known faces, which can number in the tens of millions, stored in a database.

4. MATCHING
The software decides whether the original image likely matches any picture in the database. If it does, the person may have been identified.

seizures. They also fear the U.S. could become a surveillance state. In other words, they're worried that the government will use this technology to keep close watch over its citizens.

A worst-case scenario already exists in China. There, roughly 200 million cameras track and identify citizens in real time. The technology is used to keep people in line and catch lawbreakers. The government also uses facial recognition systems to monitor the Uighurs, a largely Muslim minority. China has exported this surveillance technology. They've given it to many other countries, including Zimbabwe, Ecuador, and Pakistan. Experts worry that some of these nations are using the technology to track political opponents.

It might not be long before police departments across the U.S. begin using real-time facial recognition systems. This is detailed in a recent report by Clare Garvie, a researcher at Georgetown University who studies facial recognition. It shows that law enforcement agencies in Chicago, Detroit, and other cities are already moving quickly to install them.

In Detroit, the police have a million-dollar system. It allows them to screen hundreds of private and public cameras set up around the city. That includes cameras in gas stations, fast-food restaurants, churches, apartment buildings, schools, and other places. The faces caught by these cameras can be searched in real time against Michigan's driver's license photo database.

'There is a public safety value to this technology.'

Detroit's police department says the system isn't currently in use. Still, civil liberties advocates argue that being able to observe and identify people at a distance could threaten their basic rights. That might even include the First Amendment right to free speech. People might be too fearful to attend a protest, for example, if they think they're being watched. Civil liberties proponents also worry that in the wrong hands, the technology could be used to monitor marginalized groups, such as minorities or immigrants.

This technology "provides government with unprecedented power to track people going about their daily lives," says Matt Cagle, a lawyer with the American Civil Liberties Union of Northern California. "That's incompatible with a healthy democracy."

Even some people involved with the companies creating this technology are speaking out against it. In May, many Amazon shareholders called on the company to stop sales of its facial recognition system, Amazon Rekognition, to government agencies unless its board concludes that the technology doesn't contribute to human rights violations. But Amazon says it's not going to pull Rekognition from the shelves.

Privacy vs. Safety

Many people say there needs to be more transparency about how the police are using facial recognition.

"There is a fundamental absence of transparency around when and how police use face recognition technology," says Garvie of Georgetown.

Its use is advancing so rapidly that it's outpacing Congress's ability to legislate it. That's why there are currently few limits on how the police can deploy facial recognition. It's possible that the Supreme Court will one day have to weigh in on this issue.

Ultimately, the question is: How much of our privacy are we willing to give up to feel safe? Aaron Peskin, a San Francisco city supervisor, says the city's ban on facial recognition use by the police is an attempt to strike the right balance.

"There are many ways to make our society secure without living in a security state," he told the Associated Press. "And we have very good policing, but we don't want to live in a police state." •

With reporting by Julie Bosman, Serge F. Kovaleski, Natasha Singer, and Farhad Manjoo of the New York Times.

BEATRIZ GASCON J/SHUTTERSTOCK.COM (FACE); DACIAN G/SHUTTERSTOCK.COM (CAMERA)