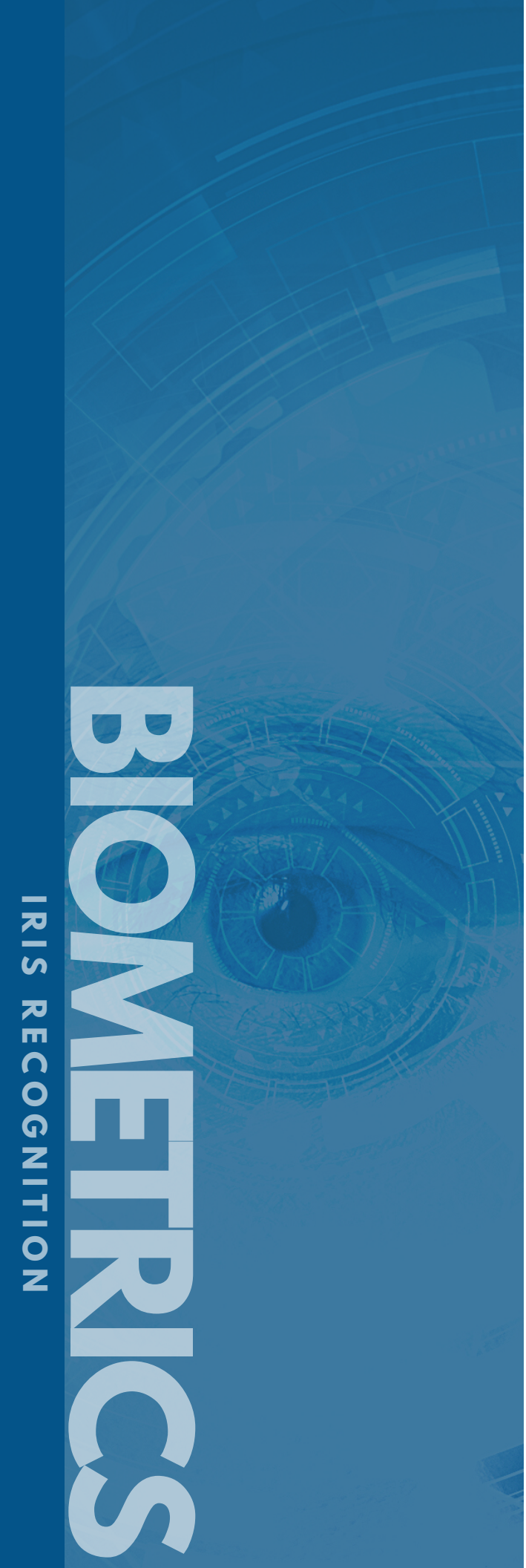

POLICING PROJECT FIVE-MINUTE PRIMERS:

IRIS RECOGNITION

Written by Allen Slater, Policing Project Student Fellow

One of the cornerstones of front-end accountability is the principle that issues of public concern—everything from law enforcement's use of surveillance technologies and data sharing to its use of force and arrest practices—should be the subject of robust engagement between police departments and the communities they serve. But productive public debate requires access to accurate information so that the policies and priorities can be carefully considered.

The Policing Project's biometrics series aims to aid in this purpose by providing basic information on one of the more complex—and rapidly changing—areas of policing: the use of biometric technologies. In each entry in this series we will explore four questions about a particular type of biometric technology:

- **How are police using this technology?**
- **How does the technology work?**
- **How accurate is the technology?**
- **Are there reasons why the public should be concerned?**

Our second entry in this series covers **iris recognition**. Although this technology is being deployed nationwide-from the Southern border to Massachusetts-news coverage and public discussion have not been nearly as high profile as with other biometric technologies.

HOW ARE POLICE USING IRIS RECOGNITION?

Like face recognition, iris scanning technology is primarily used to identify individuals. The FBI began a pilot program in 2013 to incorporate iris identification into its Next Generation Identification system. In addition to authorizing criminal justice agencies to enroll iris images with criminal records or append iris images to existing criminal records, the Bureau's pilot program identified a variety of use cases where police could utilize iris technology.

Local police departments are also utilizing iris recognition in the following ways:

In the field: Some jurisdictions are providing officers with mobile iris recognition devices (like the MORIS, a device sold by BI2 Technologies), which can be used to identify individuals that officers interact with when carrying out their duties (such as during the course of a stop).

Tracking movement within correctional facilities: Incarcerated individuals are often required to submit biometric data, including iris scans, during the booking process. As a result, correctional facilities can use iris identification to identify inmates during movement between facilities, and before release.

NCIC data: An individual iris scan could be used to search against data from the National Crime Information Center (NCIC), which tracks outstanding warrants, sex offender status, and a variety of other information. This capability can provide information to police that a suspect might refuse to provide, such as gang affiliation.

Border Security: The Department of Homeland Security uses iris identification at the border, touting it as a quick, non-contact process that provides a faster and more stable form of identification than fingerprints, which can be damaged to the point of unreliability.

Investigation Searches: Unlike fingerprints, iris images are not left as physical evidence at crime scenes; they are either captured in person or digitally. Thus, their application as an investigative tool is currently limited to circumstances were high resolution videos or photos are available. However, the FBI is currently researching wider practical applications for iris recognition in investigations.

Additionally, both the FBI and biometrics companies working with the police are currently managing databases that contain hundreds of thousands of iris scans — meaning that iris recognition technology is both a useful law enforcement tool, and a profitable investment. Both contexts provide privacy and transparency concerns for the public.

HOW DOES IRIS RECOGNITION TECHNOLOGY WORK?

The iris is the colored portion of the eye that controls how much light enters the pupil. It is made up of a complex network of features that create a random texture that, absent disease or injury, is consistent throughout a person's life. This stands in contrast to other biometrics, like faces and fingerprints, which can be altered by age or manual labor, making them less reliable in comparison.

In addition to being consistent over time, a person's iris image is relatively unique. Current evidence suggests there is less than a 1 in 10 billion chance that two irises have even a thirty percent similarity.

An iris identification requires a near-infrared spectrum camera, which typically operates at distances up to one yard (3 feet). Physical contact is not required. This camera takes a detailed image of the boundaries and textures of the iris, excluding eyelashes and eyelids. A program then maps the iris image using more than 200 distinct features. The specific capabilities of these programs vary between manufacturers, and some may use more points, or different points of comparison than others, but mapping is an activity that all programs undertake. After mapping the iris, the program converts that image into a unique code to be read by an algorithm.

That encoded image then undergoes a specialized test that looks for the amount of difference (not similarity) between that image and all of the iris images in the iris database. Any images that are not different enough must be from the same iris. Focusing on *differences* allows iris recognition algorithms to work faster than other biometric technologies, like facial recognition, which measures how *similar* two images are.

HOW ACCURACY OF IRIS RECOGNITION TECHNOLOGY?

Current research suggests that iris scanning technology, if properly operated, can be fairly accurate. In April 2018, the Department of Commerce's National Institute of Standards and Technology (NIST), published its evaluation of a large number of iris recognition systems and found the following using a sample size of 160,000:

- When it comes to **one-to-one** matching (that is, using iris scanning to *confirm* a claimed identity – for example, as a security clearance procedure), the best performing versions of the technology produced a false negative rate of 1 in 175, and a false positive rate of 1 in 100,000. In the real world, this means that a system would mistakenly reject 1 in 175 valid users, and mistakenly grant access to 1 in 100,000 unauthorized users.

- When it comes to **one-to-many** matching (that is, using iris scanning to *identify* an unknown person – such as an officer in the field), the best performing versions of the technology produced a false negative rate of 1 in 150, and a false positive rate of 1 in 1000. In the real world, this means that a system would mistakenly not identify 1 in 150 people actively in a law enforcement database, and mistakenly positively identify to 1 in 1000 people.

The average time that a program took to cycle through 160,000 irises was 11 milliseconds, and under certain circumstances, slowing the process down increased the overall accuracy of the program. Evaluators concluded that the largest variable in iris recognition accuracy is the software being used, but there are other factors that can impact the performance of these systems.

Demographic variations in subjects are one factor that can cause issues (though the effects are not as pronounced as they are in facial recognition). NIST's evaluation found that algorithms tended to perform best on whites and worst on Asians; in some instances, the performance difference was noticeable, and in others, negligible. Evaluators conceded that bias in the testing data may have been the culprit here—over

ten times more data was used from whites compared to Asians during testing. The impact of gender was too inconsistent to draw conclusions during the NIST's evaluation.

Scholars have also demonstrated on multiple occasions that certain ocular illnesses can impair the accuracy of iris recognition systems; the technology is particularly sensitive to conditions that obstruct the iris or cause geometric distortions in eye tissue. Research has also shown that under certain circumstances, contact lenses can impair the accuracy and performance of iris recognition programs — because two-thirds of the millions of Americans who wear contacts are women, this flaw holds a significant risk for them.

WHY SHOULD THE PUBLIC CARE ABOUT IRIS RECOGNITION?

As with all biometric identification technologies, iris scanning raises privacy concerns. Because this technology is largely unregulated, there remain unanswered questions about how long iris scans can be stored, whether scans can be shared with third parties, and what standard of cause law enforcement needs to scan or search an iris database.

Further complicating these issues are the roles played by large companies in the collection and storage of iris recognition data. BI2 Technologies, one of the leading private vendors of iris recognition technology, started a three-year-long giveaway of its software to law enforcement in 2017. The company has acquired nearly a million iris scans as a result.

It is also worrisome that companies like BI2, Palantir, Amazon, and others are investing significant resources to collect and store the biometric data (including iris scans) of undocumented immigrants and asylum seekers. Not only are these collection efforts particularly concerning for those communities, they are also concerning for local law enforcement officials who do not feel they should play a role in immigration enforcement. Even leaving this context aside, there are those who might rightfully ask what limit there are on private companies' ability to share and monetize those iris scans.

The real-world impact of iris recognition technology depends, in part, on how the technology itself advances. At the moment iris scanners are only effective at about 1 yard (3 feet). This limitation generally means that iris scanners must be used out in the open, with the knowledge and cooperation of the person being scanned. But long-range iris scanning capabilities are an ongoing project and may not be too far off. For example, at the CyLab Biometrics Center at Carnegie Mellon University, researchers created a system that can capture an iris from a reflection in a car's mirror up to twelve meters (36 feet) away. If effective, long-range iris scanners could potentially be used in ways similar to face recognition, raising some of the same civil liberties concerns.

Moreover, as with face recognition, there is no federal regulatory framework for iris recognition technology, meaning that both law enforcement and private entities are able to operate largely as they please when it comes to iris scanning. To protect individual privacy rights and to move our law enforcement community towards democratic policing, the public must be informed about biometric technologies like iris recognition, and engage in the discussion about how they will be used.