What You Need to Know About Facial Recognition at Airports

The New York Times

By Elaine Glusac Feb. 26, 2022

Customs officials aim to save time and increase security by ramping up the use of facial recognition. But what about privacy? A biometrics specialist weighs in.

As Americans get more comfortable traveling during the pandemic, international travelers may find a new identification system used by the U. S. Customs and Border Protection agency (C.B.P.) on their return home in the form of biometric facial recognition. Following a directive by Congress's 9/11 Commission to increase border security by using biometrics, C.B.P. began ramping up the technology in 2018 in a program called Simplified Arrival. Among other biometric measurements available, including iris scans and fingerprints, the agency selected facial recognition, which uses a computer algorithm to compare a picture taken in person at airport immigration or another border checkpoint to the traveler's passport picture or visa.

"We've automated a manual process," said Diane Sabatino, the deputy executive assistant commissioner for C.B.P., who is overseeing the biometric program.

Some privacy advocates have questioned the use of the technology. Addressing equity, Senators Roy Blunt, Republican of Missouri, and Jeff Merkley, Democrat of Oregon, sent a letter to the agency in January requesting more information "to ensure that flagged individuals are treated in a safe, fair and noninvasive manner given the imperfection of facial recognition software."

The following are excerpts from an interview on the issues with Ms. Sabatino, edited for length and clarity.

Why was facial recognition chosen over other forms of biometrics?

When we looked at different biometric technology — fingerprints, iris and facial scans — we landed with facial because it is such a simple process. Travelers present themselves and their documentation and pose for a quick photo in seconds. The officer has the data they need based on a discussion with the traveler about the purpose of the trip and ultimately can make a decision about whether further examination is needed. We can now leverage technology that's better at making comparisons. The officer is still the ultimate decision maker. Travelers can opt out.

What are the benefits of using the technology?

It's a streamlined process. One benefit is helping officers be more efficient at determining the intent of travel. It's also better at identifying potential impostors. And the third piece we hadn't contemplated was the added health benefits. We have a security enhancement at a time and place where individuals are already expected to present themselves for identity verification, and now we're adding touchless travel and limiting the spread of pathogens. It wasn't something we were contemplating when we developed it, but it certainly made sense.

How much time will a traveler typically spend at inspection?

Manual verification lasts 10 to 30 seconds, depending on environmental factors. Someone outside at a land border could be more challenged because of the lighting. As we automate and refine facial recognition technology, we're taking two to three seconds to verify the match. The match is one tool in the entire process. That tool doesn't make the decision to admit or require further examination. It is the officer and the totality of the circumstances. The priority is security.

How many impostors has the technology identified?

Since deployment, in about the first three years, primarily in the air passenger environment and somewhat in maritime, we have identified about 300 impostors using the technology. That doesn't mean we would not have otherwise identified them. In the last year, at pedestrian land crossings at the southern land border, it caught about 1,000 to 1,100.

Critics fear digital systems will be used for surveillance. How are you ensuring privacy?

Our business use case is in identifying individuals at a time and place where they would normally expect to present themselves for identity verification. We are not grabbing images and scraping social media. Individuals are presenting a passport and we have a repository to tap into and build galleries in advance of their arrival using U.S. passport photos and photos of those who have applied for visas. So we build these galleries in the airport and maritime environments based on information already provided for identity verification. We match it to the information we have.

And we're making sure there's secure encryption. When a gallery is created, that photo isn't attached to any information and can't be reverse engineered to be compromised. The design is based on the privacy measures we knew had to be in place. Images for U.S. citizens are retained less than 12 hours and often times much less.

How are you handling the threat of unconscious bias in the programming, which could lead to higher rates of errors for some groups, including people of color?

That's certainly something we're very tuned into. We have partnered with the National Institute of Standards and Technology to provide information on the program. Our high-

performing algorithms show virtually no demonstrable difference when it comes to demographics.

How are travelers notified that they can opt out?

We post signage at all ports of entry. Individuals opting out need to notify the officer at inspection. It would then revert to the manual process.

Is the technology at all border checkpoints?

We have it rolled out in pedestrian lanes at land borders. In the air environment, we're covering about 99 percent with Simplified Arrival. The land border is the final frontier. We just completed a 120-day pilot in the car lanes at Hidalgo, Texas, and we'll be evaluating the outcome. At cruise terminals, we're in the 90 percent range. We're working with nine major carriers at eight ports of entry, including Miami, Port Canaveral and Port Everglades, all in Florida.

How do you address biometric skeptics?

We welcome the scrutiny from privacy advocacy groups. We want to be able to tell and share the story about the investment we've made with respect to privacy. There are so many myths and so much misinformation out there, conflating what we do with surveillance. Anytime new technology is rolled out, there are always legitimate concerns. We welcome those questions. They help us answer better when we are building out these systems.