CBP is Doubling Down on Biometrics

Transparency

Through a new website, the agency aims to educate and update travelers on how it uses the NIST-approved facial-recognition technology.

Kate Macri
Fri, 10/16/2020 - 16:08

U.S. Customs and Border Protection's new facial recognition technology not only helps detect imposters, but also it helps create a contactless environment for CBP agents and passengers entering the U.S. during the COVID-19 pandemic. Among the tech's aims include enhancing security, health and safety at U.S. ports of entry.
“Once we're finished with the deployment strategy, by mid-January we should be at 25 different locations, and three ports of entry for the cruise passenger environment,” CBP Office of Field Operations Deputy Executive Assistant Commissioner Diane Sabatino told GovernmentCIO Media & Research.

Sabatino said CBP wants to reassure passengers that the agency takes every precaution to ensure transparency and privacy with the new facial recognition technology, which is why the agency recently launched a new biometrics-focused website providing updates and news to discuss how the agency uses the tech.

The facial recognition mechanism is not the first time CBP has used biometrics to validate passengers entering the U.S. In 2004, the agency used fingerprinting to verify passenger identity. Before facial recognition technology, CBP officials would compare a passenger's face to his or her ID.

Now, facial recognition technology eliminates that step, and passengers only need to pause to have their picture taken and compared to a federal database of passport and visa photos.

The technology is based only on the NEC algorithm, which is one of the 189 face-comparison algorithms evaluated by NIST. NEC is a leader in the facial recognition technology space for federal use.

“We have worked with NIST to review the algorithm, it's the gold standard according to their review and documentation,” Sabatino said. “[If there are] mistakes, we'd simply advise the officer there's no match, but when we get that no match, we revert to that process for comparison we use today where there is that manual verification by the officer.”

Critics of the technology worried it would misidentify people based on race, but Sabatino clarified that there has not been any significant differences based on demographics. "We haven't seen that challenge with respect to this particular algorithm that we're using. It's at 97 to 98% accuracy,” she added.
Even though security is the primary goal of the technology, the facial recognition mechanism shaves anywhere from 20 to 30 seconds off the verification process and is entirely touchless — a bonus for CBP officers and travelers during the COVID-19 era.

Sabatino clarified that if a passenger doesn’t match with a photo in the database, that doesn’t mean CBP denies entry into the U.S. A human is still involved in the process.

“It doesn't automatically result in the officer thinking there's something wrong with the individual,” she said. “That officer would do that manual comparison [of the passenger’s ID] and proceed with a primary interview. I do want to point out that even though we've incorporated biometrics into the processing, it's not replacing the human interaction that occurs at the point of entry.”

Sabatino said the facial recognition technology is also more accurate and reliable than a CBP officer making a visual comparison of the passenger’s face to his or her ID. Passengers with privacy concerns surrounding the facial recognition system can also choose to opt out, she added.

“The entry/exit program uses the tech only at a time and place where a passenger would expect to have to present themselves for ID verification,” she told GovernmentCIO Media & Research. “We have engaged with privacy groups to address CBP's application of the tech, and the images themselves are templatized. There's no reverse engineering of the photo for use outside of CBP. With U.S. citizens, it's deleted within 12 hours, and we use a secure cloud-based environment. There's no biographic data attached to the images, it's simply templatized information with respect to the image that is shared and the info that is already shared with us on file.”

A CBP spokesperson also told GovernmentCIO Media & Research that the agency constantly scans the cloud-based, private network storing the photos for vulnerabilities and cybersecurity threats.
“We have published over 10 privacy assessments that are available on the [CBP biometrics] website, and we're very tuned into the concerns about the new technology,” Sabatino said. “[We’re trying to make] sure people understand about their ability to opt out. It's also why the website is so important — to be as transparent as possible.”