



## **A.I. Heralds End Of the Passport Line... and Start Of A Privacy Row**

Molly Fosco

October 15, 2018

Because an artificial intelligence mistake could mean imprisonment for an innocent person or entry for a genuine threat.

From critical care to cyber security, 5G data speeds and AI could change lives. OZY's Fifth Generation Intelligence series tells you how.

After a grueling 10-hour flight, you finally land back home in the United States. But your relief is short-lived as you remember the endless customs line you'll soon encounter. As you approach the dreaded entrance, you stop in your tracks. There's no line. Everyone ahead of you walks up to a machine that takes their picture and asks them a few questions. Within seconds, they're free to go, except for one guy who is picked out by the machine as suspicious. Welcome to the future of border patrol — and to a revived security-versus-privacy debate in a new arena.

U.S. Customs and Border Protection first tested facial biometric technology for exit verification in June 2016 at Hartsfield-Jackson Atlanta International Airport. They've since expanded biometric exit verification to 15 U.S. airports. The agency began biometric entry verification at JFK in July 2018 and has since then expanded that to 13 other U.S. airports. The idea is the same both for entering and exiting passengers: to more quickly recognize suspicious travelers. The Department of Homeland Security has partnered with the University of Arizona's BORDERS program to develop an AI-based screening system that can identify suspicious behavior more accurately than humans can. And information technology company Unisys in March 2018 unveiled a new AI-based system called LineSight that can more efficiently screen travelers as they go through customs.

These technologies promise to significantly reduce waiting times at immigration counters and allow officials to focus on a smaller set of identified suspects instead of every person entering the country. They're gaining traction at a time when America's already stretched border-security apparatus is under heightened pressure because of President Donald Trump's demands for stricter policing of the southern border and his travel ban from several Muslim-majority countries. Help from technology makes sense. But machine learning used to predict human behavior has been found to be biased in a number of ways, including against Black defendants in the courtroom, ProPublica found in 2016. Organizations like the Electronic Frontier Foundation are concerned that facial recognition and AI software will misidentify innocent people at global borders too. The consequences of a machine not identifying a genuine threat who learns to game

the software may prove even graver than the harassment of an innocent individual — it could allow a potential terrorist in.

Researchers building these technologies, on the other hand, insist that their platforms are fundamentally superior to human screening because, unlike officers, they can't get bored, tired or distracted, and they lack the biases and preconceived opinions of humans.

“Humans are notoriously poor at detecting lies and other telltale signs of malintent,” says Dr. Jay Nunamaker, director of the BORDERS program.

The debate over whether humans or machines are better at identifying threats isn't academic. Today, Americans are just as worried about terrorism as they were in the years following 9/11, according to data gathered by Gallup, *USA Today* and CNN in 2016. About 45 percent of people surveyed said they fear that they or their family will be victims of terrorism — a figure that has not wavered much since 2001. A similar fear is growing abroad in Western Europe, which has seen a rise in fatal terrorist attacks since 2013, according to the Global Terrorism Database. The Cato Institute found in 2016 that the threat of foreign terrorism in the U.S. is quite small. Still, advanced technology is attractive to government agencies stretched because of pressures to increase policing under Trump.

The University of Arizona first began their formalized BORDERS program under the Department of Homeland Security in 2008 and has since developed the Automated Virtual Agent for Truth Assessments in Real-Time (AVATAR), an embodied border security agent powered by artificial intelligence. This bot collects cues based on body language, voice, use of language, eye movement and heart rate to determine if someone is lying. And while the BORDERS technology is not yet used by any government security agency, Nunamaker says it will be eventually. “It takes time for society to accept new approaches,” Nunamaker says, “but technology is the answer if we're going to improve security.”



---

U.S. Customs and Border Protection officer Julio Corro, right, helps a passenger navigate one of the new facial-recognition kiosks at a United Airlines gate before boarding a flight to Tokyo on Wednesday, July 12, 2017, at George Bush Intercontinental Airport in Houston.

SOURCE [DAVID J. PHILLIP/AP](#)

Unisys is of a similar mind. The company's LineSight technology uses AI to analyze travel information like ticket purchases, data from immigration organizations and cargo documents from [airlines](#) and ships to assess whether someone should be admitted to a country or questioned further. "It doesn't wait until you get to the border; it's processing information as you book your ticket and make your travel plans," says John Kendall, director of border security programs at Unisys. LineSight has not been deployed yet, but Unisys does supply U.S. Customs and Border Protection with some of their current software, as well as Australia and parts of Europe, and plans to market this new system to their existing customers. Nunamaker and Kendall are confident in the abilities of their programs to flag suspicious border traffic more efficiently than human agents. And what's more, says Kendall, LineSight will be able to very quickly

identify people who pose no threat — which is the majority of travelers around the world — making the often excruciatingly slow process of going through customs much faster. “It will reduce the number of false alarms and be better at detecting the real threats: human traffickers,” says Kendall.

The CBP is expanding its biometric facial-recognition program for passengers entering the U.S. beyond airports, to sea and land ports too. In August, the agency began testing facial-comparison technology for inbound and outbound vehicle travelers at the Anzalduas International Bridge Port of Entry in Texas, and in September, for pedestrian travelers entering the U.S. at the Port of San Luis, Arizona. This is in addition to the 15 airport sites for biometric exit and 14 airport sites for biometric entry. The system compares photos taken at the point of entry to a person’s travel documents and verifies a match. The government’s goal is to eventually use biometrics as part of a complete process in which travelers no longer need to use their passports or boarding documents. “It will replace the manual review process,” says John Wagner, deputy assistant commissioner at CBP, “and help agents determine whether people are who they claim to be.”

But for some, advanced [border](#) technology itself raises too many red flags. The Electronic Frontier Foundation (EFF) is concerned that the government collection and storage of traveler data for biometrics is a threat to individual privacy. Jennifer Lynch from EFF says the CBP’s biometrics system are not very accurate under certain circumstances, and she’s concerned about similar potential discrepancies in other platforms like LineSight. “There’s no way to take the bias out of the system,” she says.

The organizations developing border security technology argue that their machines err less than human agents. But unlike other man-versus-machine debates, here there’s personal liberty and terrorist threats on the line. One slip-up could prove costly. This debate won’t be resolved anytime soon.