the ct mirror

Extreme digital vetting moves forward under new name

George Joseph

November 26, 2017

The Department of Immigration & Customs Enforcement is taking new steps in its plans for monitoring the social media accounts of applicants and holders of U.S. visas. At a tech industry conference last Thursday in Arlington, Virginia, ICE officials explained to software providers what they are seeking: algorithms that would assess potential threats posed by visa holders in the United States and conduct ongoing social media surveillance of those deemed high risk.

The comments provide the first clear blueprint for ICE's proposed augmentation of its visa-vetting program. The initial announcement of the plans this summer, viewed as part of President Donald Trump's calls for the "extreme vetting" of visitors from Muslim countries, stoked a public outcry from immigrants and civil liberties advocates. They argued that such a plan would discriminate against Muslim visitors and potentially place a huge number of individuals under watch.

ICE officials subsequently changed the program's name to "Visa Lifecycle Vetting." But, according to the ICE presentation, the goal of the initiative — enhanced monitoring of visa holders using social media — remains the same.

Speaking to a room of information-technology contractors, hosted by the Government Technology & Services Coalition, Louis Rodi, deputy assistant director of ICE Homeland Security Investigations' National Security Program, said the agency needs a tool equipped with "risk-based matrices" to predict dangers posed by visa holders, with the social media of those considered a threat under continuous surveillance throughout their stay in the U.S.

"We have millions and millions and millions of people coming every year, and subsequently departing, so we have to be smart about it," said Rodi to a room of representatives from companies like Microsoft, Accenture, Deloitte and Motorola Solutions. "And I'm sure there are tools out there that can help."

For this targeted group of visa holders, ICE's online monitoring of public social media posts would be large-scale and non-stop. "Everything we're dealing with is in bulk, so we need batch-vetting capabilities for any of the processes that we have," said Rodi. Alysa Erichs, ICE Homeland Security Investigations' acting deputy association director for information management, told attendees that ICE hopes to get automated notifications about any visa holders' social media activity that could "ping us as a potential alert."

ICE spokeswoman Carissa Cutrell stressed to ProPublica that the Department of Homeland Security has not actually begun building any such program. "The request for information on this initiative was simply that — an opportunity to gather information from industry professionals

and other government agencies on current technological capabilities to determine the best way forward," Cutrell wrote in an email. The program would require clearance from numerous DHS units, including the Privacy Office and the Principal Legal Advisor, before it could be implemented, according to a federal official who spoke on the condition of anonymity.

In his speech, Rodi referred to meetings ICE has had with companies but did not mention any frontrunners. The major tech companies present at the conference, including Microsoft, Accenture and Deloitte, either declined to comment or didn't respond to ProPublica's request to comment about their level of interest in providing technology for the vetting program. Microsoft has opposed Trump's immigration policies, and several Microsoft researchers have publicly called for ICE to stop spying on visitors' social media.

ICE is already monitoring some social media at eight Homeland Security Investigation posts internationally, Rodi said, and the plan is to expand to more sites. In response to a question posed by ProPublica from the audience, he stated that the department was open to other social media monitoring techniques, such as link analysis (which helps authorities map out applicants' online connections), so long as they solely rely on public posts.

The ICE officials emphasized the Trump administration's strict stance. "This administration is big on immigration enforcement, so we're not going to look the other way like we have in the past when we have overstays," said Rodi. "Maybe it's an administrative violation — it's still a crime. These people need to pay. They can't get away with it."

Some analysts argue that gathering social media data is necessary. ICE already has a tool that searches for connections to terrorists, according to Claude Arnold, a former ICE Homeland Security Investigations special agent, now with the security firm Frontier Solutions. But, he said, potential terrorist threats often come from countries, such as Iraq or Syria, that provide little intelligence to U.S. authorities. As a result, in Arnold's view, social media information is all the more important.

Privacy advocates take a darker view. "ICE is building a dangerously broad tool that could be used to justify excluding, or deporting, almost anyone," said Alvaro Bedoya, executive director of Georgetown Law's Center on Privacy & Technology. "They are talking about this as a targeted tool, but the numbers tell a different story."

Bedoya noted that the program outline originally anticipated that the monitoring would identify 10,000 high-risk visa holders a year. That suggests the pool of people under social media surveillance would be many orders of magnitude larger. (ICE officials did not address this point at the conference.)

Last week, a coalition of academics and technologists warned in a public letter that ICE's interest in using big data algorithms to assess risk is misguided, given how rare it is for foreign visitors to be involved in terrorist attacks in the U.S. That means there's little historical data to mine in hopes of using it to design a new algorithm. The letter cited a Cato Institute analysis that found that the likelihood of an American dying in a terrorist attack on U.S. soil in any given year was 1 in 3.6 million in the period between 1975 and 2015.

Cathy O'Neil, one of the signatories to that letter and author of "Weapons of Math Destruction," told this reporter in August that any algorithm a company proposes would come built-in with some very human calculations. "At the end of the day, someone has to choose a

ratio," she said. "How many innocent false positives are you going to keep out of the country for each false negative?"

Thus far, social media monitoring of visa applicants has not identified any potential threats that wouldn't have turned up in existing government databases, Rodi acknowledged. "We haven't found anything that would preclude someone from getting a visa through social media alone," he said. "But, you never know, the day may come when social media will actually find someone that wasn't in the government systems we check."

That argument doesn't placate those who believe ICE's vetting is already exhaustive. Social media surveillance would be difficult to carry out without collecting collateral data on thousands of American citizens in the process, said Rachel Levinson-Waldman, senior counsel to the Brennan Center's Liberty and National Security Program.

"Generally, with surveillance technologies, they are adopted for national security purposes overseas, but are then brought stateside pretty quickly," she said, citing practices first honed overseas, such as intercepting cellphone calls. "So once there's some kind of dragnet surveillance tool or information collection tool in place for one purpose, slippage can happen, and it will expand and expand."