The Atlantic

Snooping on Foreigners' Facebook Feeds Is Ineffective and Creepy

***The federal government wants visa applicants to cough up their social-media handles*.**

Faiza Patel and Harsha Panduranga

June 14, 2019

Late last month, the State Department rolled out new rules that require nearly all foreigners applying for U.S. visas—about 15 million people each year—to disclose the handles they've used over the past five years on Facebook, Twitter, Instagram, YouTube, Pinterest, Myspace, and 14 other social-media platforms. The program is unlikely to help identify people who pose a threat to the United States. It will, however, empower the U.S. government to scrape up more information than it knows what to do with. Information misconstrued by consular officers or, potentially, computer algorithms could lead to innocent people being sent into bureaucratic limbo or having their visa denied. At worst, social-media data could be used to discriminate on a large scale against particular political or religious views disfavored by Donald Trump's administration and its successors.

The momentum to use social media to screen people coming to the United States has been mounting since December 2015, when media reports falsely claimed that Tashfeen Malik, who with her husband killed 14 people in San Bernardino, California, had pledged allegiance to ISIS in public Facebook posts. In fact, Malik had sent private messages that monitoring Facebook posts wouldn't have caught. Nevertheless, the Department of Homeland Security launched several pilot programs to test the feasibility of such checks. In 2016, it added an optional question requesting social-media handles for travelers applying for visa-free admission to the United States. And the Trump administration has already required the disclosure of social-media handles from roughly 70,000 visa applicants "determined to warrant additional scrutiny."

The new rule, though, vastly expands the universe of people affected. Unfortunately, the State Department has offered little detail about precisely how it will use the millions of identifiers that it is collecting. According to the department's regulatory filings, consular officers could look at social-media accounts to round out other information about an applicant—for instance, what they glean from her interview and application papers. It's not clear whether social-media data will be subjected to some type of automated system meant to flag particular words or identify suspicious connections between people. But Homeland Security—the State Department's main partner in vetting visa applications—has experimented with systems that perform both tasks. Many other questions remain: What will happen to people who are flagged? Will they be notified of a post that troubles a consular officer and given a chance to respond to any concerns? How will any vetting system account for slang, cultural context, and humor? Does the State Department even have the language capacity to systematically review social-media posts?

The department says it needs social-media identifiers to determine whether visa applicants meet the standards for getting a visa, to root out fraud, and to "identify misrepresentations that disguise potential threats." Of course, these are precisely the judgments that consular officers have already been making as part of the robust visa-vetting system that was built after the September 11 attacks. Anybody who has ever applied for a visa to the United States will attest that it involves a rigorous investigation. In addition to providing biographical and biometric information, applicants have to explain—and meticulously document—where they're going, how they will pay for the trip, where they will stay, whom they know in the United States, and more. Before any people who need a visa board a flight for the United States, a consular officer probes their story and checks their information against databases of law-enforcement and intelligence information.

The burden is on applicants to prove that they meet the requirements for getting a visa. If they live in a country where documents are hard to come by, the U.S. government doesn't relax the rules. If they come from a country where forgeries are common, consular officers will be even more vigilant.

Simply put, we already have "extreme vetting" that keeps out those who would do harm: From 2002 to 2016, the Cato Institute has calculated, one deadly terrorist made it through for every 379 million decisions authorizing a foreigner to enter the United States.

Since around 2014, officials have looked at social-media accounts in certain cases. But there is no evidence that such checks have added value. That's according to the government's own assessments on the usefulness of social-media monitoring. A February 2017 report from the Homeland Security's Office of Inspector General found that the social-media-vetting pilot programs that it evaluated "lack[ed] criteria for measuring performance to ensure they meet their objectives." Other internal assessments have shown that officers had difficulty using social media to detect fraud or to pinpoint public-safety or national-security concerns. These findings are in line with the objections to social-media vetting that the Brennan Center for Justice, where the two of us work, and dozens of other organizations and experts have also raised. Scaling up social-media checks will only multiply these problems.

While social-media screening isn't a dependable way to identify threats, it can be used to discriminate. The United States, despite its foundational commitment to free speech, has a long history of excluding people not because they endanger the American public, but because government officials don't like their views. In the past, it barred Charlie Chaplin, Gabriel García Márquez, and future Canadian Prime Minister Pierre Trudeau.

This concern is particularly acute under the Trump administration. Candidate Trump promised an "ideological screening test … [to] screen out any who have hostile attitudes toward our country or its principles." His first homeland-security secretary, John Kelly, went even further when he told Congress, "We want to get on their social media with passwords. What do you do? What do you say? If they don't want to cooperate, then they don't come in." Indeed, the State Department has cited one of the executive orders containing Trump's Muslim ban as a legal ground for its massive expansion of social-media screening. Against this backdrop, it is difficult to take much comfort in the department's assurance that social media "will not be used to deny visas based on … race, religion, ethnicity, national origin, political views, gender, or sexual orientation."

Moreover, the legal basis that the State Department cites means social-media information could be shared with foreign governments. It is not hard to imagine how repressive countries with which the United States shares intelligence—for instance, Saudi Arabia—could use social-media handles to identify and target activists and protesters.

Two years ago, the Supreme Court recognized the importance of social media as "for many … the principal sources for … speaking and listening in the modern public square, and otherwise exploring the vast realms of human thought and knowledge." But when people think the government is watching, they self-censor and avoid saying things that may be regarded as controversial. Regardless of whether a consular official or an algorithm is doing the vetting, the State Department's policy imposes real costs to free expression and democratic engagement across the globe. At a time when these basic freedoms are under attack in many countries, the push to gather and vet what people say online sends the message that America isn't committed to these core principles.