Social Media Surveillance

In recent years, the federal government has ramped up its efforts to monitor the social media accounts of immigrants and nonimmigrants seeking to enter the United States. In late 2016, the U.S. Department of Homeland Security (DHS) began requesting foreign travelers arriving through the Visa Waiver Program, which allows citizens of 38 countries to travel and stay for up to 90 days without a visa, to provide their social media handles voluntarily.[i] In May 2017, the U.S. State Department issued an emergency notice of new proposals to increase screening and information collection from "a subset of visa applicants worldwide," targeting individuals from predominantly Muslim countries impacted by President Trump's travel ban.[ii] Later that year, in October 2017, the Trump administration announced the implementation of enhanced vetting and screening procedures, such as social media checks, for refugees from 11 countries previously identified as posing a "higher risk" to the United States, including the aforementioned countries.[iii]

In May 2019, the State Department began requiring the nearly 15 million people who apply for visas to enter the country each year to register all social media handles used in the past five years on their application forms.[iv] Most recently, in September 2019, DHS issued a proposal to collect social media information from Visa Waiver Program applicants and applicants for immigration benefits – a plan that, if implemented, would ask an estimated 33 million people per year to provide social media handles used in the past five years.[v]

Decoding Social Media with Algorithms

Social media surveillance represents a tool in the Trump administration's strategy for closing off the United States to particular visitors, especially Muslims, which has manifested in "extreme vetting" policies and multiple iterations of a travel ban.[vi] Four DHS agencies participate in social media surveillance efforts for visa vetting purposes: U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), the Transportation Security Administration (TSA), and U.S. Citizenship and Immigration Services (USCIS).[vii]

Agency employees manually review social media posts, but, according to experts at the Brennan Center for Justice, at least CBP, ICE, and USCIS use algorithmic tools (though the full scope of DHS' efforts is unknown.)[viii] For example, the data mining firm Palantir designed CBP's Analytical Framework for Intelligence to identify non-obvious links between individuals or entities based on addresses, travel-related information, Social Security numbers, or other information, such as social media data. However, little is known "about the validity of [CBP's techniques for analyzing social media information] or whether [these techniques are] using discriminatory proxies."[ix] In addition, ICE partnered with the data mining firm Giant Oak, which provides social media monitoring support for PATRIOT, a visa applicant screening program, and LeadTrac, a management system for vetting overstay leads.

The Brennan Center for Justice's experts point to DHS' social media monitoring pilot programs as evidence of the flawed nature of social media surveillance. In February 2017, DHS' Office of Inspector General audited an ICE program and five USCIS programs, which were piloted the year before, and concluded that DHS had failed to establish mechanisms to measure their effectiveness.[x] Moreover, upon evaluating its own programs, USCIS found that out of the 12,000 refugee applicants and 1,500 immigration benefit applicants screened, social media information was helpful only in "a small number of cases" and "had a limited impact on the processing of those cases – specifically in developing additional lines of inquiry."[xi] In summary, DHS' pilot programs failed to "reliably match social media accounts to the individual being vetted, and even where the correct accounts were found, it was difficult to determine 'with any level of certainty' the 'authenticity, veracity, [or] social context' of the data, as well as whether there were 'indicators of fraud, public safety, or national security concern.'"[xii]

The Dangers of Social Media Surveillance

As DHS agencies gain access to a growing collection of personal information extracted from social media accounts, they may use it to subject religious minorities and communities of color to enhanced vetting and surveillance. Muslims are particularly vulnerable to such forms of targeting, given the Islamophobic nature of the Trump administration's immigration rhetoric and policies, namely the travel ban. Among DHS' pilot programs, at least two targeted Syrian refugees, one targeted both Syrian and Iraqi refugees, and at least two used an analytical tool tailored to Arabic speakers.[xiii]

Social media surveillance could also have a chilling effect on online expression. According to one study, awareness or fear of government surveillance of the internet had a substantial chilling effect among both Muslims and broader samples of internet users.[xiv] Thus, as individuals wishing to visit or immigrate to the United States realize that they will need to disclose their social media handles, they may censor themselves in order to improve their chances of obtaining visas. Even the social media content produced by individuals who already live in the country under visas could be subjected to scrutiny, as well as their online communications with U.S. citizens.[xv]

Furthermore, the accumulation of personal information at the hands of the federal government raises privacy concerns. When DHS shares social media information with other law enforcement and security agencies, it does so under broad standards and often does not place limits on re-dissemination.[xvi] Moreover, the systems used sometimes violate the department's own data retention rules. These facts are especially troubling in light of a CBP data breach that occurred in June 2019, during which hackers stole photographs that the agency had taken of travelers and vehicle license plates at border crossings – potentially compromising the information of as many as 100,000 people.[xvii]

Regarding the issues of free expression and privacy, the Brennan Center for Justice, Knight First Amendment Institute at Columbia University, and Simpson Thacher & Bartlett LLP filed a lawsuit on behalf of two U.S.-based documentary filmmaker associations, alleging that the aforementioned May 2019 State Department rule's social media identifier registration requirement, as well as related policies permitting the broad retention and dissemination of identifiers, violate the First Amendment and the Administrative Procedure Act.[xviii] As this lawsuit proceeds, it is critical for advocacy and civil society organizations to understand why the

practice of social media surveillance is ineffective and discriminatory at worst, and to continue to scrutinize these methods as agencies begin to rely more heavily on emerging technologies within our country's immigration system.

[i] Tony Romm, "U.S. government begins asking foreign travelers about social media," Politico (Dec. 22, 2016), https://www.politico.com/story/2016/12/foreign-travelers-social-media-232930.

[ii] "Timeline of Social Media Monitoring for Vetting by the Department of Homeland Security and the State Department," Brennan Center for Justice (Jun. 25, 2019), https://www.brennancenter.org/our-work/research-reports/timeline-social-media-monitoring-vetting-department-homeland-security-and.

[iii] *Ibid.*

[iv] Sandra E. Garcia, "U.S. Requiring Social Media Information From Visa Applicants," *The New York Times* (Jun. 2, 2019), https://www.nytimes.com/2019/06/02/us/us-visa-application-social-media.html.

[v] "Timeline of Social Media Monitoring for Vetting by the Department of Homeland Security and the State Department," Brennan Center for Justice (Jun. 25, 2019), https://www.brennancenter.org/our-work/research-reports/timeline-social-media-monitoring-vetting-department-homeland-security-and.

[vi] Harsha Panduranga, Faiza Patel, and Michael Price, "Extreme Vetting and the Muslim Ban," Brennan Center for Justice (Oct. 2, 2017), https://www.brennancenter.org/our-work/research-reports/extreme-vetting-and-muslim-ban.

[vii] Faiza Patel, Rachel Levinson-Waldman, Sophia DenUyl, and Raya Koreh, "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security," Brennan Center for Justice (May 22, 2019), https://www.brennancenter.org/sites/default/files/2019-08/Report_Social_Media_Monitoring.pdf.

[viii] *Ibid.*

[ix] *Ibid.*

[x] Rachel Levinson-Waldman, "Government surveillance of social media related to immigration more extensive than you realize," The Hill (May 29, 2019), https://thehill.com/opinion/immigration/445766-government-surveillance-of-social-media-related-to-immigration-extensive.

[xi] Faiza Patel, Rachel Levinson-Waldman, Sophia DenUyl, and Raya Koreh, "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security," Brennan Center for Justice (May 22, 2019), https://www.brennancenter.org/sites/default/files/2019-08/Report_Social_Media_Monitoring.pdf.

[xii] *Ibid.*

[xiii] *Ibid.*

[xiv] Elizabeth Stoycheff, Juan Liu, Kai Xu, and Kunto Wibowo, "Privacy and the Panopticon: Online mass surveillance's deterrence and chilling effects," New Media & Society (Oct. 8, 2018), https://journals.sagepub.com/doi/pdf/10.1177/1461444818801317.

[xv] DJ Pangburn, "A lawsuit would reveal how the Trump administration spies on social media," Fast Company (Jan. 18, 2019), https://www.fastcompany.com/90294039/a-lawsuit-would-reveal-how-the-trump-administration-spies-on-social-media.

[xvi] Faiza Patel, Rachel Levinson-Waldman, Sophia DenUyl, and Raya Koreh, "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security," Brennan Center for Justice (May 22, 2019), https://www.brennancenter.org/sites/default/files/2019-08/Report_Social_Media_Monitoring.pdf.

[xvii] "Hackers have stolen photos of travelers taken by the US border agency," MIT Technology Review (Jun. 11, 2019), https://www.technologyreview.com/f/613660/hackers-have-stolen-photos-of-travelers-taken-by-the-us-border-agency/.

[xviii] "Doc Society v. Pompeo," Brennan Center for Justice (Dec. 5, 2019), https://www.brennancenter.org/our-work/court-cases/doc-society-v-pompeo.