Why is the US government using social media to monitor the public?

Kevin Reed
24 June 2019

A series of recent reports—based on documents obtained from Freedom of Information Act (FOIA) filings and other leaked information—have revealed that the Department of Homeland Security (DHS) is violating the First Amendment right to free speech and assembly by gathering social media data for surveillance purposes and targeting organizations and individuals for harassment, intimidation, deportation and arrest.

Among the facts revealed by these reports are:

• DHS is using increasingly sophisticated methods for collecting and analyzing social media data to monitor political protests and demonstrations against US government policies.

• These methods are being used to target left-wing and oppositional political organizations and individuals in the name of "national security" and "public safety."

• DHS is working with private security firms to scrape individual social media information including profile photographs, organizational affiliations, event activity and page roles.

• Once individuals and organizations have been targeted by DHS through their social media activity, their identities and dossiers are merged with other big data resources of the surveillance state including those of the Departments of Justice, State, Defense and the CIA.

ICE's "Anti-Trump Spreadsheet"

On March 6 of this year, the *Nation* published a report—based on documents obtained in a FOIA request—that shows how the Immigration and Customs Enforcement agency (ICE) used social media intelligence to track a series of protests in the summer of 2018. These demonstrations were organized to promote immigrant rights, oppose the deportation policies of the Trump administration and protest the politics of the National Rifle Association (NRA).

In one case, the *Nation* report says, the Homeland Security Investigations arm of ICE distributed an email with an attachment containing the headline "Anti-Trump Spreadsheet 7/31/2018" to a DHS representative and an undisclosed list of others on the eve of protests against racism and xenophobia in New York City.

The spreadsheet provided detailed information about demonstrations opposed to the immigration policies of the Trump administration taking place between July 31 and August 17. It included the names of groups participating in the demonstrations and the number of individuals who had signed up on Facebook to attend it.

Among the organizations listed were the Young Progressives of America, Refuse Fascism NYC, NYC Says Enough, the New Sanctuary Coalition and Rise and Resist. The *Nation* report says the documents show how ICE "has been keenly attuned to left-leaning political activity" and "highly aware of organizations and advocates opposed to their controversial agency, which includes detaining and deporting undocumented immigrants."

The *Nation* reported on another incident on July 24, 2018 where the deputy director of ICE's New York Field Office sent an email to top local ICE officials with information copied from the Facebook event page of a demonstration scheduled to take place two days later. The information included the name of the event, the number of people who signed up on Facebook to attend it and the names of the sponsoring organizations such as the Legal Aid Society and the New Sanctuary Coalition.

The *Nation* quoted from the July 24 ICE email, "This e-mail is to inform you of a planned protest at the ERO [ICE Enforcement and Removal Operations] NYC Area. … The protest is being coordinated by approximately 40 different groups located throughout the NYC area."

In response to these revelations, the New Sanctuary Coalition and other groups filed a lawsuit against ICE for violating the First Amendment by targeting prominent immigrant rights activists for surveillance, arrest and deportation. The lawsuit says that ICE specifically targeted individuals for deportation in order to suppress their political speech.

CBP's San Diego target list

In March, NBC 7 San Diego obtained and published a series of leaked Customs and Border Protection (CBP) slides showing the agency maintained a secret database of 59 individual activists, journalists and social media influencers associated with the Migrant Caravan that was making its way to the US-Mexico border in late 2018. The leaked document, called "San Diego Sector Foreign Operations Branch: Migrant Caravan FY-2019, Suspected Organizers, Coordinators, Instigators and Media," was dated January 9, 2019.

The published list contained head shots—including many gleaned from Facebook profiles—along with dossiers of the individuals, 40 of whom were US citizens. According to the NBC 7 report, "The individuals listed include ten journalists, seven of whom are US citizens, a US attorney, and 48 people from the US and other countries, labeled as organizers, instigators or their roles 'unknown.' The target list includes advocates from organizations like Border Angels and Pueblo Sin Fronteras."

The NBC 7 report said that among those profiled in the document, "Some had alerts placed on their passports, keeping at least two photojournalists and an attorney from entering Mexico to work." Other reports about the incident said that 43 of those on the list had alerts placed against their names so that they would be tagged for questioning and stopped for additional screening by US border agents. Among the information scraped from their social media accounts was their "role" in Facebook pages set up to support those in the caravan such as administrator or editor.

In one case, Nora Phillips, a US attorney who specializes in legal aid to migrants, refugees and deportees in Tijuana was listed in the database and has since been denied entry to Mexico because an alert was placed on her passport. Phillips and two other lawyers say that border agents placed

them on the target list to retaliate and harass them for defending asylum seekers and being publicly critical of CBP practices.

As of May 24, four separate requests from members of Congress for detailed information about the target database—including a recent letter from US Senators Kamala Harris (D-CA), Richard Blumenthal (D-CT), Tom Udall (D-NM) and Elizabeth Warren (D-MA) to DHS Acting Secretary Kevin McAleenan—had no response.

Social media intel from private security firms

On April 29, the *Intercept* published a report—based on documents obtained by the America Immigration Council through a freedom of information request—showing that a private intelligence firm gathered and provided to DHS social media information on people preparing to participate in more than 600 demonstrations across the country at the end of June 2018.

According to the *Intercept* report, LookingGlass Cyber Solutions of Reston, Virginia scraped social media information of individuals in the days leading up to the protests against the Trump administration's policy of separating migrant children from their families at the border. This information was shared with DHS and then distributed through "fusion centers" nationwide to local law enforcement.

According to the DHS website, fusion centers operate as "focal points for the receipt, analysis, gathering, and sharing of threat-related information between federal; state, local, tribal, territorial (SLTT); and private sector partners."

The *Intercept* said the documents showed that a LookingGlass "Threat Analyst" emailed the finished intelligence report to a "LookingGlass Shared Services" web address on June 28, two days before the protests were to take place. The analyst's report included the following summary: "LookingGlass has compiled a spreadsheet for State Fusion Centers detailing over 600 planned 'Family Separation Day Protests' across the US on June 30. These originated from Cyber Threat Center (CTC) and are broken out by City and State; they provide physical location and the Facebook event ID."

A DHS official confirmed the role of LookingGlass in social media analytics saying, "In this particular instance, a private sector entity shared unsolicited information it collected through publicly available channels with DHS I&A [Office of Intelligence and Analysis] on protests that were scheduled to take place near Federal facilities."

The claims of "unsolicited" private sector participation notwithstanding, the involvement of firms like LookingGlass—a global provider of "360° cybersecurity and intelligence" with former CIA and US military-intelligence representatives on its executive team—indicates that corporate-military entities are involved in perfecting methods of harvesting social media information for DHS.

Brennan Center report on social media monitoring

On May 22, the Brennan Center for Justice of the NYU Law School published an extensive report entitled, "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." This document substantiates the facts in the above reports from the *Nation*, NBC 7 San Diego and the *Intercept* and provides critical details about the scale and scope of the social media data gathering operations of DHS.

The Brennan Center document analyzes how DHS and its agencies—CPB, TSA, ICE and US Citizenship and Immigration Services (USCIS)—are "vacuuming up social media information" from a variety of sources and using it "to evaluate the security risks posed by foreign and American travelers."

Among the key findings of this important report are:

• Social media information is being collected from travelers, including Americans, even when they are not suspected of any connection to illegal activity

• Social media checks extend to travelers' family, friends, business associates and social media contacts

• DHS is continuously monitoring some people inside the US and plans to expand these efforts

• DHS is increasingly seeking and using automated tools to gather and analyze social media data

• Social media information collected by DHS is shared with other law enforcement and state security agencies under broad standards

The Brennan Center report analyzes how DHS gathers basic traveler information through the Electronic System for Travel Authorization (ESTA)—where foreign travelers must complete an online application—and then connects it up with social media data and other "link analysis" to make an evaluation of the "national security threat" or "potential risk to the homeland" of individuals.

When an individual is applying for a visa waiver (permission to travel to the US for 90 days or less without a visa), for example, their social media information is stored in the CBP's Automated Targeting System (ATS). The ATS data and other information are then fed "into a number of other watch lists, such as the FBI's Terrorist Screening Database and TSA Watch Lists, as well as analytical products on trends and threats."

All of this information—about the applicant, their family and friends—is disseminated to a series of agencies including the Departments of Justice and State, the National Counterterrorism Center (NCTC) and the CIA and Department of Defense through an organization called the National Vetting Center (NVC).

The NVC was established under the Trump Administration on February 6, 2018. According to the DHS website, "The NVC is a collaborative, interagency effort to provide a clearer picture of threats to national security, border security, homeland security, or public safety posed by individuals seeking to transit our borders or exploit our immigration system."

Social media data scraping and warrantless searches

The Brennan report also reveals that as of March 2018, the State Department has begun collecting "social media identifiers" on all 15 million individuals who apply for visas each year. These identifiers are being scraped from 20 different social media platforms including the most widely used in the US (Facebook, Twitter, Instagram, etc.) as well as others that are popular in China, Russia, Belgium and Latvia.

The CPB also uses warrantless searches of personal electronics at the border to gather social media information. By using powerful handheld devices called Universal Forensic Extraction Devices (UFEDs), CBP staff is copying "in a matter of seconds the entirety of a device's memory, including all data from social media applications both on the device and from cloud-based accounts like Facebook, Gmail, iCloud and WhatsApp."

According to the Brennan Center report, 30,200 people had their devices scrubbed in this manner at the border without a warrant in 2017. Although a subsequent lawsuit blocked these intrusions by CPB, a modification to the procedure still allows warrantless copying of device data if there is evidence of a vaguely defined "national security concern."

The report also outlines the network infrastructure that has been erected by CBP for gathering and processing big data components from multiple sources. The CPB Intelligence Records System (CIRS) stores a "wide variety of information on individuals, including many who are not suspected of any criminal activity." The CIRS gathers "commercial data, and information from public sources such as social media, news media

outlets and the internet."

This information gathering operation is exempt from certain requirements of the Privacy Act, such that the CIRS data "may be ingested, stored, and shared regardless of whether it is accurate, complete, relevant or necessary for an investigation. There is no public guidance on quality controls for information" in the CIRS.

Third-party data mining tools

The data from the ATS and CIRS are then integrated into a master database known as the Analytical Framework for Intelligence (AFI). According to the DHS website, the AFI has big data mining tools that provide "enhanced search and analytical capabilities to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk."

The AFI database is used for a host of law enforcement purposes and the analytics and data mining tools that access it are provided by third party private entities. One of these firms, Palantir, is a longtime contracting partner of the government and previously provided services to the National Security Agency in a massive public surveillance program.

The report describes the way Palantir analytics tools take "personal information about people that Palantir ingests from disparate sources—such as airline reservations, cell phone records, financial documents, and social media — and combines [it] into a colorful graphic that purports to show software-generated linkages between crimes and people."

Another private company called Babel Street provides software that specifically scans social media platforms. The Brennan Center report says that Babel Street's precise role is unknown, but "CPB likely uses Babel Street's web-based application Babel X, which is multilingual text-analytics platform that has access to more than 25 social media sites, including Facebook, Instagram and Twitter."

What is the Department of Homeland Security?

Since its establishment on November 25, 2002 by then-President George W. Bush, DHS has grown into a massive state apparatus of thirteen operational and support agencies with 240,000 employees and an annual budget of more than $45 billion. Founded in the aftermath of the September 11, 2001 terrorist attacks—with overwhelming bipartisan support from the Democrats and Republicans—DHS reorganized the previously separate departments of the Customs Service, the Coast Guard and the US Secret Service under one office. It was the largest federal government reorganization since the end of World War II.

From the beginning, DHS was established as a domestic instrument for suppressing democratic rights in concert with the militarism and illegal wars fought by US imperialism in the Middle East and elsewhere. Among its primary functions is to carry through the mandate of the Patriot Act of 2001—also passed with overwhelming bipartisan support and renewed in 2011 by then-President Barak Obama—which sanctions a host of undemocratic measures, including indefinite detention and warrantless searches, wiretapping and electronic surveillance, all in the name of "national security."

During the Trump administration, DHS has shifted focus away from "the war on terror" as it had been utilized over the previous fifteen years. With the reorientation of foreign policy toward the conflict with US rivals Russia and China, DHS has been redirected towards enforcing Trump's racist Muslim refugee ban, policing the manufactured "crisis" at the southern border and cracking down on migrants seeking asylum in America.

Understood within this context, the inclusion of social media information gathering and analytics as part the repressive apparatus of DHS is entirely in line with the attack on democratic rights and increasingly xenophobic and authoritarian character of the Trump administration.

While organizations such as the Brennan Center, the *Nation* and the *Intercept* have brought to light the use of social media data by DHS and its affiliates, their objections are largely based on appeals to Democrats and Republicans in Washington, D.C. and the courts to stop it. These appeals are frequently combined with criticism of the "ineffective" nature of social media data gathering as a law enforcement methodology.

The use of social media data by DHS and other federal, state and local police agencies exposes as a sham the professed opposition of various Democratic and Republicans Party politicians to "privacy violations" by the social media and technology corporations. As long as social media information is being gathered and used secretly by the state, the parties of the ruling elite have no problem with such violations.

Behind the campaign against "fake news" on social media platforms—and the growing calls for a government break-up of all the big technology companies—is a drive to censor online political content. With workers and young people internationally using social media to plan, organize and coordinate a wave of demonstrations and strikes, the ruling elite is working on the one hand to subordinate all online content to its interests and on the other to spy on the political activity of the public in order to suppress growing social opposition to the capitalist order.

The violation of free speech and assembly rights by the intelligence and surveillance state cannot be fought by appeals to the capitalist political parties and politicians. The defense of basic democratic rights can only be mounted in a coordinated struggle of the working class internationally on the basis of the fight for socialism.