ICE uses Facebook data to locate and track suspects

Meenakshi Jagadeesan
29 March 2018

In an article published this week, the Intercept has revealed yet another troubling trend in the anti-immigrant measures that are being institutionalized by the US government. Based on a public records request made by reporters, it was found that Immigration and Customs Enforcement (ICE) not only has access to the vast trove of data available on Facebook, but has actually used backend Facebook data to locate and track suspects.

The story details one instance in February-March 2017, when ICE agents were in contact with a detective based in Las Cruces, New Mexico about a particular suspect. The email chain between various agents reveal that ICE could access Facebook data showing the log of when the account was accessed and the IP address corresponding to each login. Responding to the story, a Facebook spokesperson denied that ICE had any unique access to data and that its request for information was "checked for legal sufficiency." In this particular case, "ICE sent valid legal process … in an investigation said to involve an active child predator." Facebook "responded to ICE's valid request with data consistent with our publicly available data disclosure standards."

While the initial version of the Intercept story mentioned that the target was an immigrant, this has been denied by both ICE and Facebook. The story was later amended to state that the documents "reported in the story do not establish the target of the investigation was an immigrant or that the individual was being pursued for immigration violations."

It is possible that the particular instance exposed in this report did not concern an immigrant, though that makes the involvement of ICE questionable. Even if one were to take that seemingly far-fetched claim at face value, it is a matter of record that ICE requested private Facebook data last year to obtain a cellphone number for an unauthorized immigrant in Detroit. The number associated with the immigrant being pursued by ICE was then tracked through a cell site simulator, a powerful surveillance tool used to vacuum up cellphone calls and user location data.

Law enforcement agencies have a broad reach under the "Stored Communications Act" to ask communication service providers, including Facebook, to release information pertinent to ongoing cases. The kind of data that can be accessed by agencies such as ICE is quite extensive and much of it can be obtained without court orders.

Facebook, now under additional scrutiny and pressure to reveal how and with whom it shares information because of the Cambridge Analytica exposé, has released semi-annual transparency reports in the past detailing the number of government requests for user data. While there is no breakdown of which particular law agency has made the requests, the report from last year is quite telling. It reveals that from January 2017 through June 2017, Facebook received 32,716 requests for data from 52,280 users. Facebook notes in its report that it complied with 85 percent of the requests and "approximately 57 percent of legal process we received from authorities in the U.S. was accompanied by a non-disclosure order legally prohibiting us from notifying the affected users."

As Nathan Wessler, staff attorney with the American Civil Liberties Union's Speech, Privacy, and Technology Project, told the Intercept, the subpoenas used by ICE and other agencies are in fact nothing but "a piece of paper that they've prepared ahead of time, a form, and they fill in a couple of pieces of information about what they're looking for and they self-certify what they're looking for is relevant to an ongoing investigation." Most companies tend to comply with

these requests.

Facebook is just one part of the vast array of the spyware apparatus used by immigration enforcement officials. As even the story of the “non-immigrant” suspect shows, ICE did not stop with getting the backend data from Facebook. This data, one agent claimed, could be combined with “IP address information back from T-Mobile,” and that the agency had “sent the phone company an expedited summons for information.” Jen Miller, another agent on the same email chain, is quoted as saying: “I am going to see if our Palantir guy is here to dump the Western Union info in there since I know there is a way to triangulate the area he’s sending money from and narrow down time of day etc.”

Palantir is the $20 billion data-mining firm founded by billionaire Trump campaign supporter Peter Thiel. As reported by Spencer Woodman in the Intercept last year, Palantir received a $41 million ICE contract in 2014, to build and administer Investigative Case Management (ICM), an intelligence system that was considered to be “mission critical” to the agency. The article points out that this system allows ICE agents to access a vast “ecosystem” of data to facilitate both the discovering of targets and then the creation and administering of cases against them.

The system provides its users access to intelligence platforms maintained by numerous agencies, including the Drug Enforcement Administration, the Bureau of Alcohol, Tobacco, Firearms and Explosives, and the Federal Bureau of Investigation. It can provide ICE agents access to information on a subject’s schooling, family relationships, employment information, phone records, immigration history, foreign exchange program status, personal connections, biometric traits, criminal records, and home and work addresses. As young people and teachers throughout the US and the world are increasingly organizing on social media, the use of these platforms by the state spying apparatus will continue to grow.

It is worth noting that this system as well as the general trend to upgrade the federal government’s push to deport immigrants took place not under the current administration, but during the Obama era. The Obama presidency not only oversaw the maximum number of deportations in US history, but also the very conscious and systematic expansion of the surveillance and intelligence gathering network directed at immigrants.

Now, this surveillance network is in the hands of the Trump administration that has made no bones about its rabid anti-immigrant stance and its willingness to continue the abrogation of constitutional rights as well as international humanitarian law.