

US government collecting social media accounts of visitors to country

E.P. Milligan
31 December 2016

The US government has begun requesting foreign travelers to submit their social media information to Customs and Border Protection (CBP) before traveling into the country. The practice is claimed to be part of broader efforts to identify potential “terrorist threats.”

The request is part of the online Electronic System for Travel Authorization, a visa waiver application that many visitors must complete. The choices include Facebook, Twitter, Google+, Instagram, LinkedIn, and YouTube, as well as additional space for applicants to volunteer other lesser-known platforms.

Privacy rights activists have pointed out that there are few guidelines about how the information could be used by CBP or shared with other agencies. In effect, the practice represents an infringement on the First and Fourth Amendments, protecting freedom of expression and protection from unreasonable searches and seizures. This represents yet another development of a broader process of the erosion of democratic rights, as the US government assumes ever more increasingly the character of a police state.

While the CBP instituted the practice last week, the agency has claimed that—for now—it will not bar entry to applicants who decline to provide their social media information. The US Federal Register states that “collecting social media data will enhance the existing investigative process and provide Department of Homeland Security (DHS) greater clarity and visibility to possible nefarious activity and connections by providing an additional tool set which analysts and investigators may use to better analyze and investigate the case.”

The US government approves roughly 10 million visa applications a year and had 77.5 million foreign visitors in 2015 alone. The scooping up of such a vast amount of data will in effect lead to the creation of the largest

government-controlled database of its kind virtually overnight.

The ACLU and the Center for Democracy and Technology have cautioned that the practice could potentially provide the state with “gateways into an enormous amount of [users’] online expression and associations, which can reflect highly sensitive information about that person’s opinions, beliefs, identity and community.”

The groups also warned that government surveillance will “fall hardest on Arab and Muslim communities, whose usernames, posts, contacts and social networks will be exposed to intense scrutiny.”

The Internet Association, a group representing companies such as Facebook, Google and Twitter, argued the policy violates freedom of expression.

Internet privacy group Access Now pointed out that while the DHS claims the data collection is not mandatory, most applicants will not know that they have a choice at all. It is also likely to serve as a dangerous precedent upon which the government could implement further information probes.

Nathan White of Access Now stated: “The process to enter the US is confusing, and it’s likely that most visitors will fill out the card completely rather than risk additional questions from intimidating, uniformed officers—the same officers who will decide which of your jokes are funny and which ones make you a security risk.”

The DHS is believed to already have the ability to perform limited scans of social media data. The idea was first floated by the government following the San Bernardino killings in California, in which social media profiles factored into the investigations alongside a locked iPhone 5C.

Fifteen years after the bogus “War on Terror” began,

the United States has curtailed basic democratic rights and conducted mass illegal surveillance on the population. What is more, in every major terrorist attack on both US and European soil, the perpetrators have been known by intelligence agencies.

Clearly, the increasing surveillance of the population has done little to prevent terrorist threats. In reality, the impetus behind authoritarian measures has far more to do with strangling social opposition.

The most notorious and far-reaching anti-democratic measures were revealed by whistleblower Edward Snowden, who uncovered massive government spying of US citizens as well as foreigners through the illegal collection of cellphone metadata. He has been forced into exile over fear of arrest or even assassination.

The US government has already made enormous efforts to track the movements of citizens and foreigners alike. In early 2015, information obtained through the Freedom of Information Act revealed that the US Drug Enforcement Administration (DEA) has been tracking the movements of millions of Americans through a national license plate reader program.

The DEA operates a National License Plate Recognition program, started in 2008, that connects its license plate readers with other law enforcement agencies. Under the guise of the “War on Drugs,” the federal government is moving quickly to create a centralized database of all drivers’ movements throughout the country.

A report released by the ACLU in July 2013, called “You Are Being Tracked,” detailed a massive system of automatic license plate readers in use throughout the United States. Small, high-speed cameras mounted on police cars, road signs, bridges, and elsewhere capture thousands of license plates per minute.

Drivers’ information is kept for years or even indefinitely, with little to no protection for personal privacy rights. The information also can be shared with any other government agency regardless of whether or not it pertains to the “War on Drugs.”

An undated document shows the DEA has already deployed at least 100 license plate readers across the US, and that its database already held more than 343 million records. A 2010 document demonstrates that the agency had installed 41 plate reader monitoring stations in Texas, New Mexico and California alone.

The DEA uses the collected information to data mine

in order to “identify travel patterns” of specific individuals “of high interest,” helping to track and even predict their movements. The report does not specify what constitutes a person of “high interest.” It goes on to describe how the system monitors drivers in real time, with the ability to notify law enforcement officers immediately when a certain plate is spotted.



To contact the WSWWS and the Socialist Equality Party visit:

wsws.org/contact