



US govt expands warrantless surveillance of Americans

October 26, 2017

The US government, without court or congressional review, may have broadened a legal interpretation of which citizens are subjected to physical or digital surveillance to include “homegrown violent extremists,” according to newly released documents.

A new manual permits the collection of information about Americans, citizens and green card holders, for counterintelligence purposes “*when no specific connection to foreign terrorist(s) has been established,*” according to training slides created last year by the Air Force Office of Special Investigations (AFOSI).

The manual used in training presentations was obtained by Human Rights Watch (HRW) through a Freedom of Information Act request.

HRW requested the manual after leaked documents indicated that under Executive Order 12333, the US had vacuumed up the communications of potentially all telephone calls in countries including Mexico and Philippines.

“If you are in El Paso, Texas and have called your mother in Juarez, Mexico, US intelligence agencies probably have a record of your call,” stated HRW. *“They can use this data to map social networks and share it for law enforcement purposes.”*

The expanded powers relate back Executive Order 12333, signed by former President Ronald Reagan in 1981 and modified under the George W. Bush administration. It establishes how US intelligence agencies such as the CIA are allowed to pursue foreign intelligence investigations. The order also allows surveillance of US citizens in certain cases, including on activities defined as counterintelligence.

Previously the DoD’s manual said the US government had to show a target was working on behalf of the goals of a foreign power or terrorist group. The practical effect of the expanded

definition on how the US government gathers intelligence is not clear. Surveillance experts worry the increased monitoring lacks sufficient oversight.

“What happens under 12333 takes place under a cloak of darkness,” Sarah St. Vincent, a surveillance researcher at HRW, told Reuters. *“We have enormous programs potentially affecting people in the United States and abroad, and we would never know about these changes,”* without the documents.

Among the slides is a list of shooting attacks, examples being San Bernardino, California in December 2015 and Orlando, Florida in June 2016, that would fall under the *“homegrown violent extremist”* category.

The shooters had declared allegiance to the Islamic State (IS, formerly ISIS/ISIL) shortly before or during the attacks, but investigators found no actual links to the terrorist organization that has carried out shootings and bombings of civilians around the world.

Military counterintelligence agencies are also allowed to investigate both active duty and US civilian personnel as long as there is a potential case connected to the military, DoD senior intelligence oversight official Michael Mahra told Reuters.

The disclosure comes as US intelligence officials are pushing to renew the controversial spying program, allowing agencies to conduct bulk surveillance on internet users.

Section 702 of the Foreign Intelligence Surveillance Act gives US intelligence agencies permission to spy on and store internet data and communications of foreign people living outside the US. The George W. Bush-era legislation’s authorization is set to expire on December 31, if Congress does not renew it. The Senate Intelligence Committee is expected to privately vote on a bill to reauthorize the law this week, despite requests for a public debate.

While that process is underway, a bipartisan group of lawmakers has introduced the first legislative proposal to restrict law enforcement’s access to data collected by the National Security Agency’s (NSA) warrantless internet surveillance program.

The Republican and Democratic leaders on the House Judiciary Committee unveiled the *“USA Liberty Act”* Wednesday. The legislation would renew Section 702 of the Foreign Intelligence Surveillance Act (FISA), which authorizes the collection, use, and dissemination of electronic communications and metadata.

A discussion draft of the bill, obtained by the Cato Institute, adds some restraints on law enforcement’s ability to access Americans’ data. The bill would also extend the surveillance authority, which is set to sunset at the end of this year, until 2023.