



## **Late-night reports suggest CIA collecting more data on Americans**

Chris Mills Rodrigo

February 11, 2022

A late-night release of government reports on two Central Intelligence Agency programs has revealed that the organization is most likely collecting more data on American citizens than previously known.

The revelations have prompted calls from civil rights organizations and privacy hawks in Congress for legislative action to strengthen protections for Americans.

Both reports conducted by the Privacy and Civil Liberties Oversight Board (PCLOB), a watchdog created after 9/11 to ensure counter-terror investigations did not jeopardize privacy or civil liberties, looked into two programs conducted under Executive Order 12333 authority.

The Reagan-era presidential directive established a framework for data collection by the intelligence community during foreign missions.

When Edward Snowden almost a decade ago revealed the extent of warrantless bulk data collection by the government, Congress responded by banning collection under a separate statute focused on domestic activities, the Foreign Intelligence Surveillance Act (FISA).

While Congress left EO 12333 alone, civil liberties experts were concerned that intelligence agencies could still be collecting American data despite the new restrictions on FISA, especially since in the digital era data is far less restricted by borders.

“With the revolution in communications technology, our communications, our data, floats all over the world, on its way to where it's going and gets stored all over the world,” said Elizabeth Goitein, co-director of the Liberty and National Security Program at the Brennan Center for Justice at NYU Law.

“Under Executive Order 12333 in general the government is not allowed to target particular Americans or U.S. persons,” she continued. “But it hardly matters anymore because if the

government can conduct bulk surveillance and bulk collection overseas it's going to pick up American's data in the process.”

The redacted reports, called “Deep Dives” by the PCLOB, are the first time those fears have been officially confirmed.

“Most Americans probably think and assume that government surveillance affecting their own information and data is subject to oversight by Congress and the courts,” Goitein explained. “And they have reason to assume that because there are laws that would seem to indicate as much — but there are loopholes in those laws that the government could be exploiting and these reports confirm that that's exactly what the government is doing.”

The only clues to what program was evaluated in “Deep Dive II” come from a partially declassified letter from Sens. Ron Wyden (D-Ore.) and Martin Heinrich (R-N.M.) and a set of recommendations from PCLOB staff. The rest of the report, which was delivered to the Senate Intelligence Committee in March 2021, was held back by the CIA to “protect sensitive tradecraft methods and operational sources.”

The lawmaker's letter suggests that the program involved collecting bulk data “entirely outside the statutory framework that Congress and the public believe govern this collection.” The letter, dated April of last year, calls for the full report to be declassified.

The PCLOB staff recommendations revealed that despite the CIA releasing guidelines for data collection in 2017 it had not implemented those standards in the unknown program.

Surveillance experts who spoke with The Hill speculated that the program could involve the purchasing of international phone records, given that reporting in 2013 found the CIA doing exactly that with AT&T, or data from third-party brokers.

“Based on the legal arguments the government has made elsewhere it is possible that this is another telephone metadata dragnet... or web browsing information or even location information,” Sean Vitka, policy counsel at Demand Progress, told The Hill.

The other report, “Deep Dive 1,” is less heavily redacted and focuses on a program targeting potential sources of ISIS funding with connections to Americans.

Based on CIA staff interviews conducted in 2015, the PCLOB gleaned some details about the agency's acquisition, processing and dissemination of financial data.

One standout revelation from that report, according to the Cato Institute's Patrick Eddington, is the sheer number of requests for the unmasking of United States' persons information in the investigation. A CIA staff member was asked how many of those requests were received in a year and although the number is redacted it appears to be several digits.

“So you begin to get I think, just from that alone, the sense that you're talking about minimally thousands of requests, maybe tens of thousands of requests,” Eddington, who formerly worked

for the CIA, told The Hill. “I find it really tough to believe that there are literally tens of thousands or hundreds of thousands of people in this country who are engaged in financial transactions that were designed to benefit ISIS.”

That suggests that the CIA collected information on far more people as part of the program than was required by the security threat the agency was responding to.

“If you're a person who either has financial assets or gives money to entities overseas, you should be concerned about this,” Eddington said. “When data on Americans gets funneled around other different agencies, they can have really negative effects.”

For example, if an American traveler’s data were swept up in the investigation, a Transportation Safety Administration official could see their name in a report on ISIS funding and add them to a no fly list even if that person has no connection to terrorism at all.

The reports released this week are almost sure to spur some action from Congress.

“FISA gets all the attention because of the periodic congressional reauthorizations and the release of DOJ, ODNI and FISA Court documents,” Wyden and Heinrich said in a joint statement. “But what these documents demonstrate is that many of the same concerns that Americans have about their privacy and civil liberties also apply to how the CIA collects and handles information under executive order and outside the FISA law.”

Privacy experts who spoke to The Hill argued that at a minimum, in order to bring EO 12333 activities under the law, Congress should require that agencies depending on the statute acquire a specialized warrant before collecting data on Americans.

“Congress really has not legislated to any significant degree to create protections for Americans in the context of 12333 surveillance and yet this spying is incredibly broad and sweeps up huge amounts of Americans data,” Patrick Toomey, a senior staff attorney at ACLU's National Security Project, told The Hill. “It raises the same kinds of privacy concerns that Congress has set out to address under FISA by establishing a legal framework that requires court approval before intelligence agencies can obtain or access American’s information.”

Improving both transparency and Congressional oversight is also seen as essential.

While the CIA said in a statement Thursday that it has kept the intelligence committees in both chambers up to date on its intelligence operations, Wyden and Heinrich said that the bulk collection program was kept from “the public and Congress” until the PCLOB report was delivered last spring.

“I do think that the intelligence community learned a lesson after the Snowden disclosures and realized that they needed to be more transparent in order to earn back the Americans trust,” Goitein told The Hill. “Why they would throw that all away for this program is a head scratcher, because now we’re right back to where we were in 2013.”

