# The CIA Got Caught Spying On Americans Again. It's Time For Congress To Make Them Stop

**The CIA's surveillance authorities need to be sharply curtailed and the market for third-party data restructured or eliminated entirely.**

BY: RACHEL BOVARD

FEBRUARY 17, 2022

Nearly a decade ago, Edward Snowden dropped a series of bombshell revelations on the world, chief among them revealing the presence of the PRISM program: a constitutionally dubious surveillance program under which the National Security Agency, Federal Bureau of Investigation, and Central Intelligence Agency gather and search through the emails, internet calls, photos, and chats of Americans without obtaining a warrant, usually through the backdoor of America's major tech companies.

In response, Congress passed the USA Freedom Act in 2015, a bill that amended the Foreign Intelligence Surveillance Act (FISA) to ban the bulk collection of Americans' telephone records and internet metadata under Section 215 of the PATRIOT Act. In its place, Congress authorized more targeted measures subject to transparency, declassification, and reporting requirements.

But based on recently released information from the Senate Intelligence Committee heads Sen. Ron Wyden, D-Ore., and Sen. Martin Heinrich, D-N.M., the CIA received Congress's directive and apparently responded with a big, fat LOL.

The pair of senators announced last week they had pressured the CIA into releasing a partial de-classification of two Privacy and Civil Liberties Oversight Board (PCLOB) reports, "Deep Dives," both of which suggest the CIA is collecting more data on American citizens than even Congress is aware of.

To accomplish this, the CIA cites authority under Executive Order 12333, a broad-based, Reagan-era presidential directive that established a framework for data collection by intelligence agencies during foreign missions. The CIA is technically prohibited from collecting data on Americans, but given the bulk nature of modern surveillance – where all kinds of identifiable information is swept up in giant dragnets – the data of Americans is invariably captured.

Intelligence agencies are required to take steps to protect domestic information, including redacting the names of any Americans from reports unless they are deemed relevant to the investigation, a process called "unmasking."

Deep Dive I, the first PCLOB report partially declassified by the senators, focuses on a program targeting potential sources of ISIS funding with connections to Americans and suggests that data from American citizens is being unmasked at a high rate. Former CIA analyst and Cato Institute scholar Patrick Eddington put it this way:

*The report also notes that requests by CIA and non-CIA elements for the unmasking of [U.S. Person] data or identities is common and seemingly on a large scale . . . If you look at the redacted portion on the number of unmasking request, the redaction encompasses at least 8 and perhaps as many as 10 numeric characters – potentially a huge number.*

"I find it hard 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," he later told The Hill. Moreover, according to the PCLOB report, analysts are not required to provide a justification for initiating queries on U.S. citizens.

**The CIA May Still Be Spying Via Third Parties**

The second report, "Deep Dive II," was left almost entirely classified but raises potentially even greater concerns, namely that an undisclosed data repository on American citizens exists, as the senators put it, "entirely outside the statutory framework that Congress and the public believe govern this collection."

Given the redactions, it's hard to know exactly how this bulk data is being collected. But prior reporting on bulk data collection from the government can inform reasonably educated speculation that this program may involve the government purchasing data from the third-party commercial market.

Hundreds of times a day, popular smartphone apps broadcast their location, demographic information, and unique phone-ID numbers to an industry of online data brokers and advertising companies, which resell them to other firms – and to the government.

In 2013, it was revealed that the CIA was paying AT&T more than $10 million a year under a "voluntary contract" (that is, not under subpoena or court order) to exploit the company's database of phone records, including international calls made by Americans. The U.S. military, law enforcement arms, the Internal Revenue Service, and even a National Guard unit tasked with carrying out drone strikes have all purchased various data sets from data brokers.

You can see the appeal. There is currently nothing illegal about purchasing a person's minute and intimate details, which are used to inform everything from political campaign targeting to product advertising. For the government, it is an easy way to circumvent constitutional protections when gathering details on Americans.

While data brokers promise these details are anonymous, late last year a Catholic newsletter was able to purchase app data from the dating app Grindr, cross-reference it with other publicly available information, and identify and out a gay Catholic priest.

**Time to Reform the Intelligence Community**

At the very least, the Wyden/Heinrich disclosures make clear how much oversight and reform is needed over the intelligence community's capabilities and ongoing actions.

But such efforts between Congress and the IC are rarely cooperative, and sometimes downright adversarial. The intelligence community has long exuded arrogance toward congressional attempts at oversight of their activities. In 2013, Wyden asked then-Director of National Intelligence James Clapper in an open congressional hearing if the NSA collected "any type of data at all on millions or hundreds of millions of Americans."

"No," Clapper responded. "Not wittingly."

Just months later, Snowden revealed the NSA's access to the bulk data of Americans through U.S. tech companies and millions of call records from telecom providers. Clapper was later forced to apologize to the Senate Intelligence Committee for his "clearly erroneous" statement.

A year later, rather than responding to the post-Snowden era with a more cooperative attitude toward congressional oversight and, where possible, transparency, the CIA responded by hacking the computers of Senate investigators examining the agency's role in perpetrating torture.

But the IC has had numerous allies on Capitol Hill. During the FISA reauthorization debate in 2020, Sen. Richard Burr, R-N.C., seemed to scoff at the exercise itself, noting that under EO 12333, the NSA "can do all of this without Congress's permission, without guardrails . . . that authority exists."

In lieu of this, Congress should be *more* aggressive in its oversight and statutory reform, not less. This includes ignoring the inevitable fear-mongering that intelligence agencies and Department of Defense regularly engage in whenever Article I attempts to assert itself. These are the same people, after all, who told us Kabul wouldn't fall, swore there were nuclear weapons in Iraq, repeatedly told bald-faced lies to Congress about the status of the war in Afghanistan, and call anything they don't like "Russian misinformation" in an effort to protect the politically powerful and discredit dissent.

But Congress must also update the rules about commercial data brokerage, which exists in a largely lawless space. Sen. Ron Wyden, Sen. Rand Paul, R-Ky., and 18 other senators introduced the Fourth Amendment Is Not For Sale Act, which would close the legal loophole allowing data brokers to sell American's personal information to law enforcement and intelligence agencies without court oversight.

Rep. Warren Davidson's, R-Ohio, office confirmed to The Federalist that his office will soon introduce the It's Your Data Act, which will restrict third-party data collection and sharing, and ban the sale of such data to the government.

All of these efforts begin what will be an uphill but necessary climb for Congress: getting control of the massive and largely accountable surveillance activities of the federal government. This is the work of the legislature. As Wyden and Heinrich noted, “it is critical that Congress not legislate without awareness of a . . . CIA program, and that the American public not be misled into believing that the reforms in any reauthorization legislation fully cover the IC’s collection of their records.”