Dell Cameron

Security
Jun 12, 2023 3:23 PM

The US Is Openly Stockpiling Dirt on All Its Citizens

A newly declassified report from the Office of the Director of National Intelligence reveals that the federal government is buying troves of data about Americans.

The United States government has been secretly amassing a “large amount” of “sensitive and intimate information” on its own citizens, a group of senior advisers informed Avril Haines, the director of national intelligence, more than a year ago.

The size and scope of the government effort to accumulate data revealing the minute details of Americans' lives are described soberly and at length by the director's own panel of experts in a newly declassified report. Haines had first tasked her advisers in late 2021 with untangling a web of secretive business arrangements between commercial data brokers and US intelligence community members.

What that report ended up saying constitutes a nightmare scenario for privacy defenders.

“This report reveals what we feared most,” says Sean Vitka, a policy attorney at the nonprofit Demand Progress. “Intelligence agencies are flouting the law and buying information about Americans that Congress and the Supreme Court have made clear the government should not have.”

In the shadow of years of inaction by the US Congress on comprehensive privacy reform, a surveillance state has been quietly growing in the legal system's cracks. Little deference is paid by prosecutors to the purpose or intent behind limits traditionally imposed on domestic surveillance activities. More craven interpretations of aging laws are widely used to ignore them. As the framework guarding what privacy Americans do have grows increasingly frail, opportunities abound to split hairs in court over whether such rights are even enjoyed by our digital counterparts.

“I’ve been warning for years that if using a credit card to buy an American’s personal information voids their Fourth Amendment rights, then traditional checks and balances for government surveillance will crumble,” Ron Wyden, a US senator from Oregon, says.

The Office of the Director of National Intelligence (ODNI) did not immediately respond to a request for comment. WIRED was unable to reach any members of the senior advisory panel, whose names have been redacted in the report. Former members have included ex-CIA officials of note and top defense industry leaders.

Wyden had pressed Haines, previously the number two at the Central Intelligence Agency, to release the panel's report during a March 8 hearing. Haines replied at the time that she believed it "absolutely" should be read by the public. On Friday, the report was declassified and released by the ODNI, which has been embroiled in a legal fight with the digital rights nonprofit the Electronic Privacy Information Center (EPIC) over a host of related documents.

"This report makes it clear that the government continues to think it can buy its way out of constitutional protections using taxpayers' own money," says Chris Baumohl, a law fellow at EPIC. "Congress must tackle the government's data broker pipeline this year, before it considers any reauthorization of Section 702 of the Foreign Intelligence Surveillance Act," he said (referring to the ongoing political fight over the so-called "crown jewel" of US surveillance).

The ODNI's own panel of advisers makes clear that the government's static interpretations of what constitutes "publicly available information" poses a significant threat to the public. The advisers decry existing policies that automatically conflate being able to buy information with it being considered "public." The information being commercially sold about Americans today is "more revealing, available on more people (in bulk), less possible to avoid, and less well understood" than that which is traditionally thought of as being "publicly available."

Perhaps most controversially, the report states that the government believes it can "persistently" track the phones of "millions of Americans" without a warrant, so long as it pays for the information. Were the government to simply demand access to a device's location instead, it would be considered a Fourth Amendment "search" and would require a judge's sign-off. But because companies are willing to sell the information—not only to the US government but to other companies as well—the government considers it "publicly available" and therefore asserts that it "can purchase it."

It is no secret, the report adds, that it is often trivial "to deanonymize and identify individuals" from data that was packaged as ethically fine for commercial use because it had been "anonymized" first. Such data may be useful, it says, to "identify every person who attended a protest or rally based on their smartphone location or ad-tracking records." Such civil liberties concerns are prime examples of how "large quantities of nominally 'public' information can result in sensitive aggregations." What's more, information collected for one purpose "may be reused for other purposes," which may "raise risks beyond those originally calculated," an effect called "mission creep."

Most Americans have at least some idea of how a law enforcement investigation unfolds (if only from watching years of police procedurals). This idea imagines a cop whose ability to surveil them, turn their phone into a tracking device, or start squeezing records out of businesses they frequent, are all gated behind evidentiary thresholds, like reasonable doubt and probable cause.

These are legal hurdles that no longer bother an increasing number of government agencies.

Access to the most sensitive information about a person was once usually obtained in the course of a “targeted” and “predicated” investigation, the report says. Not anymore. “Today, in a way that far fewer Americans seem to understand, and even fewer of them can avoid, [commercially available information] includes information on nearly everyone,” it says. Both the “volume and sensitivity” of information the government can purchase has exploded in recent years due to “location-tracking and other features of smartphones,” and the “advertising-based monetization model” that underlies much of the internet, the report says.

“In the wrong hands,” the ODNI’s advisers warn, the same mountain of data the government is quietly accumulating could be turned against Americans to “facilitate blackmail, stalking, harassment, and public shaming.” Notably, these are all offenses that have been committed by intelligence agencies and White House administrations in the past. What constraints do exist on domestic surveillance activities are all a direct response to that history of political sabotage, disinformation, and abusive violations of Americans' rights.

The report notes: “The government would never have been permitted to compel billions of people to carry location tracking devices on their persons at all times, to log and track most of their social interactions, or to keep flawless records of all their reading habits. Yet smartphones, connected cars, web tracking technologies, the Internet of Things, and other innovations have had this effect without government participation.”

The government must appreciate that all of this unfettered access can quickly increase its own power “to peer into private lives to levels that may exceed our constitutional traditions or other social expectations,” the advisers say, even if it can't blind itself to the fact that all this information exists and is readily sold for a buck.