GlobalResearch
Center for Research on Globalization

U.S. Intelligence Has Amassed ‘Sensitive and Intimate’ Data on ‘Nearly Everyone’

A newly declassified report confirms that the government has unprecedented insight into our lives through smartphones, cars, web browsing, and other tech.

By Lauren Leffer
Global Research, June 15, 2023
Gizmodo

Region: USA
Theme: Intelligence

***

When it comes to data privacy in our present, hyper-connected age, many of your worst fears and biggest anxieties are probably correct.

Yes, smartphones and our manifold other devices collect an incredible array of information on our habits, choices, and movements at all times.

Yes, all of this information is compiled by companies to sell for profit.

Yes, the U.S. government is among the many clients buying up that data.

And yes, it represents a significant and persistent threat to your civil liberties and safety, as confirmed in a newly released report from the Office of the Director of National Intelligence (ODNI)—the top dog among all of our nation’s spy agencies.

The declassified document, made public on Friday, was completed in January 2022, following 90 days of assessment by an advisory panel. It was commissioned by Avril Haines, the director of national intelligence in the Biden Administration, at the behest of Oregon Senator Ron Wyden. Haines agreed to look into the issue of how U.S. intelligence uses commercially available data during her confirmation hearing, and now the result of that inquiry is fully on display.

The newly released report affirms a mounting bevy of evidence that government agencies—from Immigration and Customs Enforcement to the Pentagon—are compiling vast stores of for-sale data.

Taken altogether, the information that the government is easily able to purchase from data brokers rivals anything that's been available to intelligence agencies in the past—even through warrants, wiretaps, and Fourth Amendment due process.

> "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 that is of a type and level of sensitivity that historically could have been obtained, if at all, only through targeted (and predicated) collection," write the report authors. All that data "can reveal sensitive and intimate information about individuals," the 48-page account emphasizes. "It could be used to cause harm to an individual's reputation, emotional well-being, or physical safety."

Though this data may be "anonymized" by brokers and sold in bulk, it does not stay anonymous in the hands of U.S. spy agencies. The government report affirmatively cites a 2019 New York Times investigation that found deanonymizing commercially available information (CAI) takes mere minutes.

"Information that previously did not exist in the public domain about US citizens now is widely available on the open market, raising privacy questions particularly when it comes to US government use of such data," an ODNI official familiar with the matter told Gizmodo in a phone call.

- Through location tracking, your phone knows where you sleep every night.
- Via cookies, your web browser tracks the sites you visit.
- Financial data confirms what you buy and when.

Health apps, smartwatches, and motion tracking can keep tabs on everything from when you're physically active to how you're feeling physically and mentally.

The government report states that religious practice, political views, travel, medical info, social associations, purchase history, "speech activities" and even sexual behavior are all things that can be inferred from CAI. It references widely publicized controversies like the outing of Catholic priests enabled via purchasable data from Grindr and the government's buy-up of data from a Muslim prayer app.

"While each data broker source may provide only a few data elements about a consumer's activities, data brokers can put all of these data elements together to form a more detailed composite of the consumer's life," notes the report. Though a simple commercial transaction, government agencies can access that same composite—and they do.

The Defense Intelligence Agency, for instance, amasses information on peoples' social media activity.

The military spy org also maintains a global location tracking database, per the newly public document, though it claims that specific authorization is required to query that database and that it's rarely accessed. The Department of Defense, Coast Guard, Navy, CIA, FBI, National Security Agency, Department of Homeland Security, and even the Treasury Department are among the other agencies noted as purchasing and using CAI.

Yet within and across each of these organizations, little of their CAI activities are tracked.

Intelligence agencies across the U.S. government don't have a solid understanding of how they are collecting and using purchased data.

Because all of this data is considered publicly available, there are almost no standards or restrictions on how this info should be acquired, used, or kept secure.

None of the publicly available commercial data is currently classified as sensitive in an official capacity, though it undoubtedly is, according to the report.

The ODNI recommends that all of this needs to change, to protect peoples' privacy, freedom, and welfare. "The intelligence community is working to develop additional standards and procedures for commercially available information," the agency official emphasized on the phone.

But new standards and firm suggestions might not be enough. "Even subject to appropriate controls, CAI can increase the power of the government's ability to peer into private lives to levels that may exceed our constitutional traditions or other social expectations," the authors write.

Not to mention the risk such data poses when malicious actors or "adversarial foreign governments" decide to take advantage of it. CAI "can be purchased by anyone including our adversaries," the ODNI official said. "Such information also raises counterintelligence risk for the intelligence community."

U.S. intelligence agencies, companies, and anyone else willing to pay can reap untold information rewards from the data economy. It's a system the government may have long dreamed of, but could never have built on its own. Through tacit acceptance of invasive tech into our daily lives, we did this to ourselves, the report implies.

"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," the ODNI writes, in the declassified document. "Yet smartphones, connected cars, web tracking technologies, the Internet of Things, and other innovations have had this effect without government participation."

Though not everyone places the blame on consumers. "This review shows the government's existing policies have failed to provide essential safeguards for Americans' privacy, or oversight of how agencies buy and use personal data," Senator Wyden wrote in a Monday statement. "If the government can buy its way around Fourth Amendment due-process, there will be few meaningful limits on government surveillance," he said—urging executive and legislative action.

Wyden and other senators introduced an act in 2022 intended to ban data brokers from selling location, health, and other sensitive information. It has yet to progress.

*

Note to readers: Please click the share button above. Follow us on Instagram and Twitter and subscribe to our Telegram Channel. Feel free to repost and share widely Global Research articles.

Featured image is from Gabo_Arts (Shutterstock)

Articles by: Lauren Leffer