Weaponized Data via Silencer

March 23, 2026

"Authoritarian regimes have developed strong cyber espionage capabilities that enable their influence and coercion operations," explains a National Intelligence Council "assessment," dated April 7, 2020.

This report goes on to say that the "collection and aggregation of vast quantities of personal data" by commercial enterprises, and the willingness to share this data with third parties, "increases both the likelihood and the impact of data breaches."

The report, which is highly redacted though declassified in late 2022, fingers Iranian hackers as well as foreign governments for having obtained private data on U.S. citizens. In 2013, Russia's Federal Security Service "sponsored a theft of 3 billion accounts" off an American web service, and in 2017 Chinese agents "stole 147 million from a US credit-reporting agency." And more.

Reading on, a sense of *déjà vu* develops. The report calls this technological capacity "digital authoritarian capabilities" — yet our own government has the same.

It accuses China of marshaling "mass surveillance and AI-driven algorithmic tracking of its citizens' behavior at home to inform the use of soft or coercive incentives and disincentives to control them," but that, I'm afraid, is what our government does, too.

Now we learn that all this and more was known by American intelligence agencies during the first Trump administration.

But was kept from him.

That is, "intelligence analysts downplayed China's actions because they had disdain for the 'vulgarian' Trump," explains *Just the News*, and at least one agent kept evidence of possible Chinese interference in the 2020 election from the president because that might have led to "policies against China" that the agent didn't like.

That, right there, we call a *datum*.

This is Common Sense. I'm Paul Jacob.