

Government surveillance erodes trust between citizens and government

 americansforprosperity.org/blog/government-surveillance-erodes-trust-between-citizens-and-government/

May 8, 2025

Taking back control of our privacy: How to rein in FISA abuse

National security should not come at the expense of personal liberties.

Unfortunately, a program meant to protect us from terrorist attacks has become a backdoor mechanism used by the government to snoop on U.S. citizens.

Americans for Prosperity's James Czerniawski, senior policy analyst for technology and innovation, recently testified before the U.S. House Subcommittee on Crime and Federal Government Surveillance. His testimony focused on warrantless surveillance of citizens under Section 702 of the Foreign Intelligence Surveillance Act, or FISA, and recommendations for ending the abuse.

Section 702 of FISA allows the U.S. government to collect the communications of non-U.S. persons around the world. This certainly seems like a reasonable step to prevent another 9/11.

However, in the process of collecting those communications, it also sweeps up vast amounts of data from Americans, and taking a peek at that data without a warrant appears to be irresistible to the national security apparatus.

AFP's James Czerniawski testifying before the U.S. House Subcommittee on Crime and Federal Government Surveillance.

In fact, as James points out in his testimony, Section 702 has become a go-to resource for the government to access Americans' communications without a warrant. Examples of blatant abuse include:

- [The FBI used Section 702 data to conduct 200,000 warrantless searches](#) of American citizens' communications in 2022 alone.
- In 2023, a FISA Court opinion revealed that [the government improperly searched the 702 database 278,000 times](#) between 2016 and 2020. It used the database to spy on people present at the U.S. Capitol on January 6, 2021, and to find information about Black Lives Matter protesters in 2020, among other things.
- It has also been revealed that the government has searched the database to learn about donors to a congressional campaign and [targeted elected officials](#), including a sitting U.S. senator.

The federal government is clearly abusing Section 702. And this abuse is contributing to an erosion of trust between the American people and the security apparatus charged with protecting them.

Past surveillance reform attempts have been failures.

As James laid out in his testimony, Congress has tried its hand at surveillance reform in the past, including attempts to reform Section 702.

Back in 2020, Congress couldn't agree on how to reform a program authorized under the PATRIOT Act, so they just let the snooping authority expire. That tactic didn't work.

Instead of stopping their surveillance tactic, intelligence agencies continued their activities in secret under the authority of an executive order.

In another instance, Congress attempted to reform Section 702 by simply codifying the FBI's internal guidelines. But that didn't stop them from violating their own guidelines at least 4,000 more times.

There are better reforms.

If Congress is serious about reining in abusive warrantless searches under Section 702, James suggested three areas for congressional focus.

- **Closing the backdoor search loophole.** Under Section 702, U.S. intelligence agencies are allowed to search billions of international communications to find and review American citizens' phone calls, text messages, and emails. Seventy-six percent of Americans believe the government should obtain a warrant before searching international communications for conversations involving those present in the U.S.
- **Closing the data broker loophole.** Under current law, government agencies can purchase location information, internet records, and other sensitive data about people in the U.S. from data brokers. They can then use this information to subject them to surveillance via other technologies. Eighty percent of Americans believe Congress should close this loophole.
- **Strengthening third-party oversight at the FISA Court.** FISA Court can appoint third-party consultants — experts in privacy, constitutional rights, or surveillance law — to advise them when considering novel questions. But their role is limited. Expanding it would be a significant improvement to due process and the protection of citizens' civil liberties.

We live in a dangerous world. But protecting our constitutional rights and national security are not mutually exclusive goals.

As James Czerniawski testified, AFP stands ready to work with Congress to reform government surveillance laws and practices to protect citizens' privacy.