



U.S. House of Representatives
Washington, DC 20515

April 10, 2026

Dear Members of Congress:

Every Member of Congress takes an oath to support and defend the Constitution. Our Founding Fathers had the foresight to include warrants in the Fourth Amendment expressly to protect Americans from overreach of the government and now, 239 years later, Congress is actually considering allowing Americans to continue to be investigated by law enforcement without warrant protections.

In 2008, Congress passed Section 702 of the Foreign Intelligence and Surveillance Act (FISA) for the purpose of allowing the National Security Agency (NSA) to target any foreigner abroad and acquire all their communications without a court order. Congress explicitly prohibited the targeting of Americans; however, almost all Americans have had data caught up in the dragnet.

Any future reauthorization of FISA must include requirements to obtain a warrant before searching the 702 database for the contents of Americans' communications. This would not preclude agencies from targeting suspects; no queries on non-U.S. persons would be subject to warrant requirements, and searches of Americans suspected of criminal behavior would still be allowed. Additionally, there are many exceptions to allow for emergency situations.

Thousands of government employees have access to this database and it has even been used to [run personal queries](#) on political donors, activists, prospective tenants, journalists, Members of Congress, and ex-girlfriends. In 2021 alone, [3.4 million](#) (that we know of) warrantless searches were run on Americans. Very few of these were known to the individuals whose communications were searched. While the 2024 reauthorization included some minor reforms, the number of warrantless searches of Americans' data went up by [35% in 2025](#) compared to 2024.

Additionally, we must close the data broker loophole, whereby agencies bypass any existing warrant requirements by simply purchasing Americans' sensitive data from third party data brokers. This data includes search and browsing history, medical data, biometric information, recordings from home assistant devices, and the contents of virtual communications. This is a backdoor to personal information about the lives, relationships, and beliefs of law-abiding citizens; federal agencies should not be able to legally buy their way around the Bill of Rights.

Crucially, the 2024 amendment altering the definition of Electronic Communication Service Providers (ECSP) must be reversed. As passed in 2008, Section 702 defined ECSP as major communications

providers, such as phone companies or search engines, and allowed for seizure of data that had passed through their infrastructure. In 2024, this was expanded to most organizations with infrastructure such as Wi-Fi routers or phone lines. This “Make Everyone a Spy Law” leaves entities such as houses of worship, nonprofits, and most small businesses vulnerable to demands that they turn over their visitors’ data.

Finally, you may have heard inaccurate information surrounding the urgency of the April 20, 2026 date. To clarify, existing FISA Court certifications are authorized for up to a year beyond the April 20 “deadline,” meaning these authorities will not simply disappear overnight.

Public safety must always be protected; but we can do so without watering down our fundamental rights. All of these reforms would be a return to the Founders’ vision of Constitutional liberty, while preserving the original intent of FISA and mechanisms in place to stop threats to the homeland. On behalf of our over 3 million members in all 50 states we ask that you defend the protections afforded under the Constitution by supporting warrant requirements to the 2026 FISA reauthorization.

Sincerely,

A handwritten signature in black ink, appearing to read "Brent Gardner". The signature is written in a cursive, flowing style.

Brent Gardner
Chief Government Affairs Officer
Americans for Prosperity