Senator Chuck Grassley
Chairman
Senate Judiciary Committee
224 Dirksen Senate Office Building
Washington, DC 20510

Senator Dick Durbin
Ranking Member
Senate Judiciary Committee
224 Dirksen Senate Office Building
Washington, DC 20510

Senator Tom Cotton
Chairman
Senate Select Committee on Intelligence
211 Hart Senate Office Building
Washington, D.C. 20510

Senator Mark Warner
Ranking Member
Senate Select Committee on Intelligence
211 Hart Senate Office Building
Washington, D.C. 20510

June 18, 2026

Dear Chairman Grassley, Ranking Member Durbin, Chairman Cotton, and Ranking Member Warner:

Section 702 of the Foreign Intelligence Surveillance Act (FISA) authorizes warrantless surveillance of foreign individuals abroad.[1] Though designed to target foreign nationals, Section 702 contains a loophole that allows agencies to search through Americans' private communications that are "incidentally" collected, known as the "backdoor search loophole." While Section 702 expired by its terms on June 12, members of Congress are actively considering how to reauthorize and reform the law.

As the government adopts new AI technologies, FISA Section 702 and other federal privacy loopholes pose a growing threat to civil liberties. AI can aggregate and analyze seemingly innocuous information, assembling it into a detailed portrait of Americans' private lives.

As Congress considers FISA's surveillance program reauthorization, Members of Congress from both parties are raising alarms about a reauthorization that doesn't address these loopholes and the growing threats from AI.[2] Without meaningful reform, AI risks supercharging mass surveillance and eroding our democracy.

There is a path forward. Congress must include a warrant requirement for accessing Americans' communications content and close the data broker loophole.

---

[1] Electronic Frontier Foundation, "Backdoor Search," Electronic Frontier Foundation, accessed June 4, 2026, https://www.eff.org/pages/backdoor-search.

[2] Mia McCarthy, Jordain Carney, and Calen Razor, "'Get a warrant': FISA fights resurface," *Inside Congress*, *Politico*, May 28, 2026, https://www.politico.com/newsletters/inside-congress/2026/05/28/get-a-warrant-fisa-fights-await-congress-00940300. ; Andrew Desiderio and Laura Weiss, "Dems threaten FISA over Pulte," Punchbowl News, June 3, 2026, https://punchbowl.news/article/senate/pulte-dems/.

Although FISA Section 702 was created to monitor foreign nationals, FISA-enabled surveillance inevitably sweeps up vast amounts of sensitive data belonging to Americans as well due to Americans' communication with foreign targets. Each year, intelligence agencies conduct thousands of warrantless searches of Section 702 information for the purpose of finding and reviewing Americans' phone calls, emails, and text messages.[3]

The "data broker loophole" in the Electronic Communications Privacy Act similarly allows the government to buy Americans' sensitive electronic data without obtaining a warrant.

These practices predate AI, but with it, the scope and scale of surveillance will reach unprecedented levels.[4] Research shows that AI can compress in seconds what would take a human investigator hours.[5] Through inference, pattern matching, and data fusion, AI-enabled re-identification can assemble granular portraits of individuals' lives, making data analysis faster, cheaper, and easier than ever before.[6]

FISA's June 12 expiration presents an opportunity. Any FISA Section 702 extension should include a warrant requirement for searches of Americans' communications and reforms to stop the government from buying sensitive data it would otherwise need a warrant to obtain.

Americans should not have to surrender their constitutional rights because surveillance tools have become faster, cheaper, and more powerful. If Congress fails to act now, AI will not just expand existing privacy violations, but will make them harder to detect, easier to scale, and far more dangerous to democracy.

Sincerely,

Americans for Responsible Innovation
Brennan Center for Justice at NYU School of Law
Center for Democracy & Technology
Common Cause
Consumer Action
Consumer Federation of America
Demand Progress
Defending Rights & Dissent
Electronic Privacy Information Center (EPIC)
Free Press Action

---

[3] Office of the Director of National Intelligence, Office of Civil Liberties, Privacy, and Transparency, Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities: Calendar Year 2025 (Washington, DC: ODNI, April 2026), https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2022/3608-statistical-transparency-report-regarding-national-security-authorities-calendar-year-2021.

[4] Darrell M. West, "How AI can enable public surveillance," *Brookings*, April 15, 2025, https://www.brookings.edu/articles/how-ai-can-enable-public-surveillance/.

[5] Simon Lermen et al., "Large-Scale Online Deanonymization with LLMs," preprint, submitted February 24, 2026, arXiv:2602.16800.

[6] Barry Friedman and Danielle Keats Citron, "Indiscriminate Data Surveillance," Virginia Law Review 110, no. 6 (October 2024): 1351, https://virginialawreview.org/articles/indiscriminate-data-surveillance/.

National Action Network
National Hispanic Media Coalition
Restore The Fourth Action
TechEquity Action
The Leadership Conference on Civil and Human Rights