April 24, 2026

Dear Speaker Johnson, Minority Leader Jeffries, Majority Leader Thune, Minority Leader Schumer:

As privacy and civil liberties advocates, we write to express the need for critical reforms to protect Americans' privacy rights and guard against surveillance abuse as part of any extension of Section 702 of the Foreign Intelligence Surveillance Act ("FISA 702"). FISA 702 — a warrantless surveillance authority that collects the private communications of a huge number of Americans — is set to expire on April 30. It is essential that Congressional action on this issue close loopholes that are exploited to circumvent court approval.

FISA 702 has been repeatedly misused to deliberately pull up Americans' private communications, and despite changes to the law enacted in 2024 broad misconduct continues: Over the past two years the government has used filter tools to run queries for Americans' communications while avoiding requirements to audit those queries for misconduct.[1] This means we do not even know how many queries for Americans' communications have occurred over the past two years, and that malicious queries could be occurring without ever being audited or addressed.

To protect Americans from surveillance abuse, the following two measures are critical policies to include in any extension of FISA 702:

1) Close the Backdoor Search Loophole: The most significant danger from FISA 702 surveillance is warrantless U.S. person queries. These queries enable government personnel to conduct "backdoor searches," circumventing the need for court approval to deliberately seek out and read Americans' communications. U.S. person queries have been repeatedly misused: Peaceful protesters, campaign donors, lawmakers, Congressional staff, and journalists have all been subject to improper FISA 702 queries in recent years. Self-policing by agencies has failed to stop these harms in the past, and cannot be trusted to prevent them in the future. The only way to reliably protect Americans is to establish a warrant rule, and require U.S. person queries to be approved by a judge based on a probable cause standard. An effective model for doing so can be based on the Protect Liberty Act (H.R. 7816), the SAFE Act (S. 3893), or the Government Surveillance Reform Act (H.R. 7901; S. 4082). These proposals contain a robust warrant requirement, as well as carefully tailored exceptions that account for the limited scenarios where U.S. person queries have provided value. Unfortunately the proposal brought to the House floor last week — which only reiterated longstanding requirements for a warrant to *target* Americans — fails to address this issue, as do other proposals that would allow warrantless queries absent probable cause.

2) Close the Data Broker Loophole: Intelligence agencies and law enforcement should only be able to collect Americans' sensitive records with court approval. Yet all too often this basic protection is evaded by exploiting the Data Broker Loophole, with agencies ignoring courts and instead buying Americans' data. Electronic location records, communications metadata, web browsing activity,

[1] Charlie Savage, *New York Times*, "U.S. Says Wiretap Program Thwarted Attack on 2024 Taylor Swift Concert," April 9, 2026, https://www.nytimes.com/2026/04/09/us/politics/section-702-surveillance-fisa.html ("In 2024, the Justice Department became aware of how that function sometimes let analysts see collected messages of Americans who had been in contact with the foreign target. But those views were not being logged or counted as queries for an American's information, so the reported numbers were off, and there was no way to go back and audit them for compliance with heightened limits. The F.B.I. deactivated the function. In referring to the newly identified problem in this year's ruling …. the person familiar with the matter said that it was similar to the problem with the F.B.I. filtering tool, and that the newly disclosed issue applied across the intelligence community, including another tool being used by the bureau").

transaction and purchase records, online search data, and many other forms of data can reveal individuals' most intimate beliefs, activities, and interactions. The government should not be able to to collect and stockpile this sensitive information en masse with no restraints other than a price tag. The Data Broker Loophole undermines one of the most significant FISA reforms Congress has enacted this century: In 2015 Congress voted overwhelmingly to ban domestic bulk collection, requiring that collection of Americans' data be individualized, and based on evidence and investigative need. But by exploiting the Data Broker Loophole the government engages in precisely the type of bulk collection Congress enacted FISA reforms to prohibit. Closing this loophole is vital to ensuring prior FISA reforms are upheld, and that Americans' data is safe from unfettered collection. H.R. 7816, S. 3893, and H.R. 7901/S. 4082 contain provisions that solve this issue as well.

The government's exploitation of these loopholes to stockpile and misuse Americans' most intimate communications and information already presents immense risks, and the emerging use of AI technologies to effortlessly sift through vast quantities of data will supercharge those risks to an unprecedented degree.

We urge you to use this moment to advance commonsense measures that will shield Americans from surveillance abuse, and protect their privacy, civil rights, and civil liberties. We are eager to work with you in support of this goal, and advancing these vital reforms. If you have any questions, please contact Jake Laperruque at jlaperruque@cdt.org.

Sincerely,

Access Now
ACLU
Advocacy for Principled Action in Government
Asian Americans Advancing Justice | AAJC
Asian American Federal Employees for Nondiscrimination
Asian Law Alliance
Brennan Center for Justice at NYU School of Law
Center for Democracy & Technology
Center for Security, Race and Rights
CLEAR
Committee to Protect Journalists (CPJ)
Common Cause
Consumer Choice Center
Defending Rights & Dissent
Demand Progress
Due Process Institute
Electronic Privacy Information Center (EPIC)
Fight For The Future
Free Press Action
Freedom of the Press Foundation
Global Network Initiative
Korean American Center
Lawyers' Committee for Civil Rights Under Law

The Leadership Conference on Civil and Human Rights
Muslim Advocates
National Association of Criminal Defense Lawyers
National Immigrant Justice Center
New America's Open Technology Institute
Muslims for Just Futures
Pacific Asian Counseling Services
The Project for Privacy and Surveillance Accountability
Project On Government Oversight
Reporters Committee for Freedom of the Press
Reporters WIthout Borders (RSF)
Restore The Fourth
Surveillance Technology Oversight Project (S.T.O.P.)
X-Lab
The 1990 Institute