June 1, 2026

The Honorable Mike Johnson
Speaker of the House
U.S. House of Representatives

The Honorable John Thune
Majority Leader
U.S. Senate

The Honorable Steve Scalise
Majority Leader
U.S. House of Representatives

The Honorable Chuck Schumer
Democratic Leader
U.S. Senate

The Honorable Hakeem Jeffries
Democratic Leader
U.S. House of Representatives

Re: 45-day Extension of Section 702 of the Foreign Intelligence Surveillance Act

Dear Speaker Johnson, Majority Leaders Scalise and Thune, and Democratic Leaders Jeffries and Schumer:

With Section 702 of the Foreign Intelligence Surveillance Act (FISA) set to expire in 11 days, Congress is preparing to once again consider the terms for reauthorization. This 45-day extension followed several failed attempts to pass no-reform reauthorization proposals. Until now, Congressional leadership has always permitted floor votes on meaningful reforms as part of the FISA reauthorization process; refusal to allow such votes this year has led to this impasse. Congress must advance real, commonsense reforms to Section 702 of FISA, including closing the backdoor search and data-broker loopholes, before the 45-day extension lapses.

Our broad, bipartisan civil society coalition is deeply concerned by recent efforts to reauthorize Section 702 without meaningful improvements to protect Americans from warrantless surveillance, or even allow votes on such reforms. The three-year proposal that passed the House did not include a "warrant requirement"—it only restated existing law. The earlier five-year reauthorization proposal was not a reform package. In fact, it would have actually made it easier for the government to use FISA data against Americans in court. The "clean" 18-month extension did nothing to protect Americans from being spied on through government purchases of sensitive personal information from data brokers and offered no other meaningful reforms to stop the ongoing and well-documented abuses of 702. None of these proposals attempted to put real guardrails in place to shield Americans from warrantless and AI-powered mass surveillance.

Three bills—the **Government Surveillance Reform Act of 2026 (GSRA),** introduced by Sens. Lee and Wyden and Reps. Davidson and Lofgren; the **Security and Freedom Enhancement**

Act of 2026 (SAFE Act), introduced by Sens. Lee and Durbin; and the **Protect Liberty and End Warrantless Surveillance Act of 2026 (Protect Liberty Act),** introduced by Rep. Biggs—would all reauthorize Section 702 of FISA while making crucial reforms to protect Americans' privacy and civil liberties. Without these basic reforms, any reauthorization of Section 702—short-term or otherwise—would leave the communications and other private information of law-abiding Americans vulnerable to government access and abuse. The reforms include:

Requiring a Court Order for U.S. Person Queries: Although the warrantless surveillance authorized by Section 702 may only target foreigners outside the United States, Americans' phone calls, text messages, and emails are inevitably swept in. The SAFE Act, the Protect Liberty Act, and the GSRA would require the government to obtain a warrant or FISA Title I order to access Americans' private communications obtained under Section 702, with reasonable exceptions for emergencies, consent, and certain cybersecurity-related queries. This reform is crucial not only to protect Americans' Fourth Amendment rights but also to prevent continued abuse of U.S person queries, or searches of Section 702 data for Americans' information. Such queries have been used in recent years to improperly search for the communications of 19,000 donors to a congressional campaign; members of Congress and their staff; multiple U.S. government officials, political commentators, and journalists; and protesters on both the left and right.

The 18-year history of the Section 702 program has proven that nothing short of a court order will protect Americans' rights. Most recently, Congress sought to increase internal agency oversight of U.S. person queries when it reauthorized Section 702 in 2024, but the FBI systemically evaded the new statutory requirements by quietly using a so-called "advanced filter function" to conduct queries and wrongly treating those queries as exempt from the law. This response by the FBI confirms the necessity of independent judicial oversight and the insufficiency of relying on executive branch agencies to police themselves.

Closing the Data Broker Loophole: Numerous federal agencies—including the FBI, DHS, and DOD—are evading constitutional and statutory privacy protections by purchasing Americans' sensitive data from data brokers. This data includes geolocation information, communications metadata, and internet browsing history—information that can reveal intimate details about Americans' private lives. Recent reporting indicates that DOD seeks to use artificial intelligence to analyze these troves of data, unlocking new potential for the government to expose Americans' movements, associations, and habits at scale.

The government should not be permitted to buy its way around the Fourth Amendment or the laws Congress has passed to safeguard Americans' rights. During the 2015 FISA reauthorization, Congress banned domestic bulk collection of Americans' data on a broad bipartisan basis, yet the government now exploits the data broker loophole to engage in exactly the type of broad, indiscriminate collection that Congress sought to prohibit. A bipartisan majority of the House

passed the Fourth Amendment is Not For Sale Act, standalone legislation to close this loophole in 2024. The SAFE Act, the Protect Liberty Act, and the GSRA would take significant steps toward protecting Americans' privacy by limiting law enforcement and intelligence agencies' ability to purchase certain sensitive information from third-party sellers, while preserving their ability to obtain that information using a warrant, court order, or subpoena, as provided by law.

Fixing the Definition of "Electronic Communication Service Provider": The Section 702 reauthorization legislation passed in 2024 included a provision that was intended to allow the government to compel the cooperation of one particular type of company when conducting surveillance under Section 702. Because the type of company was, and still remains, classified, the provision was deliberately written in broad language to obscure the type of company at issue. The unintended consequence is that the provision gives the NSA access to the communications equipment of a huge array of businesses and commercial locations, vastly expanding the universe of Americans' communications that can be "incidentally" collected and creating enormous potential for abuse.

When the expanded definition was adopted, Senator Mark Warner, then the chair of the Senate Select Committee on Intelligence, acknowledged the problem and pledged that he would work with colleagues to fix it after the bill's passage. To date, however, Congress has failed to address the admittedly overbroad expansion. The SAFE Act, the Protect Liberty Act, and the GSRA all include language that would amend the definition of "electronic communication service provider" to prevent the government from enlisting ordinary American businesses in its surveillance under Section 702.

Strengthening Amici Provisions: *Amici curiae* play an important role in ensuring the FISA Court hears a perspective other than that of the government in cases implicating Americans' privacy and civil liberties. However, *amici* are still left out of too many important cases and are unable to access all the materials necessary to do their job. All three bills would address some of the current limitations on *amici's* effectiveness, ensuring that Americans' privacy and civil liberties interests are adequately represented before the FISA Court and improving the Court's ability to conduct meaningful oversight of FISA surveillance. These provisions are taken from the so-called "Lee-Leahy amendment," a measure that passed the Senate in 2020 by a vote of 77-19.

The commonsense reforms in the Government Surveillance Reform Act, the Security and Freedom Enhancement Act, and the Protect Liberty and End Warrantless Surveillance Act serve to protect Americans' constitutional rights while preserving the core national security value of Section 702: the ability to collect information about foreign threats. Congress must be permitted to vote on these reforms, which have longstanding bipartisan support in Congress and are widely favored by constituents. According to recent polling, Americans are overwhelmingly on the side of reform—only 12 percent of Americans want FISA extended as-is, 76 percent want Congress

to close the backdoor search loophole, and 80 percent want Congress to close the data broker loophole.

The Foreign Intelligence Surveillance Court recently recertified the Section 702 program, so collection will not lapse until March 2027, giving Congress time to thoughtfully approach reauthorization. Congress must not abandon Americans' constitutional rights and instead should reject any extension that does not include key bipartisan reforms that would protect Americans' privacy and civil rights and liberties. We urge Congress to use the remainder of the 45-day extension to engage in good faith negotiations on reforms, only advance real reform proposals, and stop passing short-term extensions that delay what the American people need: a Section 702 reauthorization that continues to protect our national security, but also respects our Fourth Amendment rights.

Sincerely,

AAPI New Jersey
Access Now
Advocacy for Principled Action in Government
American Civil Liberties Union
Antiwar.com
APA Justice
Arab American Institute
Asian Americans Advancing Justice | AAJC
Autistic Women & Nonbinary Network
Brennan Center for Justice
Center for Democracy and Technology
Church Women United in New York State
Citizens for Responsibility and Ethics in Washington (CREW)
Color Of Change
Common Cause
Connecticut Voices for Children
Consumer Choice Center
Courage California
Defending Rights & Dissent
Demand Progress
Due Process Institute
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Fight for the Future
Free Press Action

Freedom of the Press Foundation
Government Information Watch
Holy Spirit Missionary Sisters, USA_JPIC
Indivisible
Indivisible Auburn WA
Indivisible Eastside (WA)
Indivisible EMF — Edgewood, Milton, & Fife, WA
Indivisible Plus Washington
Indivisible Washington's 8th District
Japanese American Citizens League
Jewish Climate Action Network
Law Enforcement Action Partnership
Libertas Institute
Long Beach Alliance for Clean Energy
Lucy Parsons Labs
MPower Change Action Fund
Muslims for Just Futures
National Fair Housing Alliance
National Organization for Women
NETWORK Lobby for Catholic Social Justice
North American Climate Conservation and Environment (NACCE)
Northwest Indivisible
NTEN
Oakland Privacy
OCA Silicon Valley
OpenMedia
Oregon Consumer League
P Street
Peace Action
People Power United
Project for Privacy and Surveillance Accountability
Project on Government Oversight
Project South
Reporters Without Borders (RSF)
Restore The Fourth
RootsAction
Snake River Alliance
Stop AAPI Hate
Surveillance Technology Oversight Project
Thai Community Development Center (Thai CDC)

The Alliance for Secure AI
The Eisenhower Media Network
The Leadership Conference on Civil and Human Rights
The Sikh Coalition
The Southern Poverty Law Center
UltraViolet Action
UnidosUS
United Church of Christ Media Justice Ministry
United for Peace and Justice
Wikimedia Foundation
Wisconsin Muslim Civic Alliance
X-Lab
Zero Hour

cc: Members of the House of Representatives and Members of the U.S. Senate