November 13, 2026

The Honorable Charles E. Schumer
Democratic Leader
U.S. Senate

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

The Honorable Richard J. Durbin
Democratic Whip
U.S. Senate

The Honorable Katherine Clark
Democratic Whip
U.S. House of Representatives

The Honorable Pete Aguilar
Democratic Caucus Chairman
U.S. House of Representatives

Re: Protecting Americans from Warrantless Surveillance and Weaponization of Government

Dear Leaders Schumer and Jeffries, Whips Durbin and Clark, and Caucus Chairman Aguilar:

We write to urge you to make protecting Americans' privacy and reining in surveillance an urgent congressional priority. The unprecedented assault on privacy by the Trump administration underscores a fundamental reality: civil liberties cannot depend on who occupies the White House.

For years, Congress has debated the government's surveillance powers primarily through the lens of Section 702 of the Foreign Intelligence Surveillance Act (FISA). Reforming those authorities remains a critical first step, but federal surveillance capability now extends far beyond FISA. Federal agencies can access or acquire extraordinarily sensitive information about all of us through commercially-available purchased data, automated license plate readers and other location-tracking technologies, facial recognition and biometric systems, financial records, and vast databases maintained by government agencies and private companies.

These capabilities do not exist in isolation. Communications surveillance, location tracking, financial information, facial recognition, biometrics, commercially acquired data, and increasingly powerful tools for aggregating these government databases together create a surveillance ecosystem that Congress has never comprehensively addressed. Weaponized, this ecosystem would allow for any individual in the United States, or any of our communities, to be targeted at such a level that it shatters the ability for the free exercise of constitutional rights.

Congress must take action now, and must not extend any surveillance powers, like FISA, without doing so.

Increasingly sophisticated data analysis and artificial intelligence tools make it possible to aggregate these disparate sources and draw conclusions about individuals' movements, relationships, associations, beliefs, and activities on a scale unimaginable when many of our existing privacy laws were written.

As evidenced by the backlash against Flock and automated license plate readers, Americans of all political leanings see that surveillance has gone too far, and are rightfully outraged at the expansion of surveillance happening at the federal, state, and local levels. Addressing the escalating danger to our privacy, civil liberties, and constitutional rights requires more than responding to individual abuses after the fact. It requires limiting the very surveillance infrastructure that makes abuse possible.

The Trump administration has shown its willingness to use the machinery of the federal government in ways that threaten political dissent and civil liberties. National Security Presidential Memorandum 7, for example, directs a government-wide effort involving Joint Terrorism Task Forces and instructs federal agencies to investigate not only alleged acts of political violence but funding mechanisms, organizational structures, and supporting networks. A tool that was designed to stop legitimate terrorist threats is now being used to target advocacy organizations that challenge government policy. This is merely one example of the executive branch asserting powers to baselessly target its perceived political opponents.

Whatever one's views of this administration, the broader lesson is clear: Congress should not allow or fund invasive surveillance powers that remain practically unconstrained, especially as artificial intelligence capabilities expand at a dramatic rate. The assumption that officials will always use them responsibly has been proven dangerously wrong.

President Trump has essentially made this point himself. Pushing this spring for a “clean” extension of Section 702, he acknowledged that a separate FISA authority, not the provision he wanted extended, had been “illegally and unfortunately used against me” during the Russia investigation, and said he was willing to accept that risk again in exchange for not reforming FISA at all. This administration is not the guardrail Congress should be relying on. Democrats must not allow the last act of the Republican trifecta to be giving this administration—or any administration—warrantless surveillance powers to spy on Americans.

The danger is compounded by the government's growing ability to obtain information from private sources that historically would have required judicial process. Purchasing commercially

available data and surveillance technology lets agencies acquire sensitive information about people in the United States without a warrant.

Networks of automated license plate readers can create detailed records of individuals' movements across communities and jurisdictions, and questions about access and accountability have grown more urgent as these networks expand. Even Flock Safety, the largest automatic license plate reader vendor, acknowledges that local agencies can establish one-to-one data-sharing relationships with federal agencies.

We urge Democratic leadership to advance legislation that:

- **Broad surveillance reform that includes strengthening transparency and accountability across government.** Congress and the public need meaningful information about the surveillance technologies federal agencies deploy, the amount of taxpayer dollars spent, the data they acquire, how those systems are used, and the mechanisms available to identify and remedy abuse.

- **Protects individuals' communications from warrantless searches.** Congress should require a warrant or other appropriate court order before intelligence and law enforcement agencies search Section 702 databases for individuals' communications, subject to carefully defined emergency exceptions.

- **Closes the data-broker loophole.** Federal and state agencies should not be permitted to purchase sensitive information that they would otherwise need a warrant or court order to compel directly.

- **Establishes rigorous safeguards for location data.** Congress should set clear limits on federal acquisition, querying, retention, and sharing of location data and ban use of automatic license plate readers, including data obtained indirectly from state and local agencies or private vendors.

- **Protect our biometric data by ending facial recognition and biometric surveillance.** Congress must ban generalized and suspicionless surveillance by facial recognition and biometric surveillance technology. Congress must subject any use of these technologies to clear legal standards, accuracy requirements, auditing, transparency, and accountability.

- **Limits the aggregation and repurposing of collected information.** Information collected by one agency or for one governmental purpose should not become available across the federal government for unrelated investigative or surveillance purposes.

Congress should ban such data sharing and require transparency around interagency data sharing and the use of private contractors and artificial intelligence to combine or analyze government datasets.

- **Protects financial and digital privacy.** Government access to financial records and digital records such as email should be governed by meaningful legal process and should not become a means of investigating lawful political, religious, charitable, or associational activity absent individualized suspicion and a warrant.

These reforms would revive a basic principle: powerful investigative tools should be directed at people reasonably suspected of wrongdoing, not used to build a persistent surveillance architecture around the American people.

Many of these concerns have historically united members of both parties. Though Speaker Johnson and Majority Leader Thune now seek to avoid any debate over or votes on meaningful privacy protections, Congress has repeatedly considered bipartisan reforms of warrantless searches under Section 702 and government acquisition of commercially available data. FISA represents a critical opportunity for Congress to catch up to the accelerating evolution of surveillance technology.

Many Americans have rightly warned about the danger of weaponizing federal power against political opponents, journalists, protesters, immigrants, advocacy organizations, and other targeted communities. Privacy protections cannot not depend on whether Americans trust the current president. They should be strong enough to protect Americans regardless of who occupies the White House.

We urge you to make comprehensive surveillance and privacy reform a priority, and to firmly oppose the Trump administration's surveillance agenda until such reform is enacted.

Sincerely,

AAPI NJ
Access Now
Advocacy for Principled Action in Government
All in Wisconsin Fund
American Federation of Teachers
Arab American Institute (AAI)
Asian Americans Advancing Justice | AAJC
Autistic Women & Nonbinary Network
Center for Digital Democracy

Center for Organizing
Church Women United in New York State
Citizens for Responsibility and Ethics in Washington (CREW)
Color Of Change
Common Cause
Concerned Citizens for Nuclear Safety
Consumer Choice Center
Council on American-Islamic Relations (CAIR)
Courage California
Defending Rights & Dissent
Demand Progress
Democracy Defenders Action
Democratic Messaging Project
dmarcian, Inc.
Due Process Institute
Earth Ethics, Inc.
Economic Action Maryland Fund
Eisenhower Media Network
Electronic Privacy Information Center (EPIC)
Emgage Action
Empowering Pacific Islander Communities (EPIC)
Environmentalists Against War
Fayetteville Police Accountability Community Taskforce
Free Press Action
Free Speech For People
Freedom of the Press Foundation
Frontera Federation
Gate 15
Genesee Valley Citizens for Peace
Government Information Watch
Holy Spirit Missionary Sisters, USA-JPIC
Indivisible
Indivisible Auburn, WA
Indivisible Eastside, WA
Indivisible EMF — Edgewood, Milton, & Fife, WA
Indivisible Monroe County, Illinois
Indivisible Redmond, Oregon
Indivisible Santa Fe
Indivisible Washington's 8th District
Jewish Climate Action Network, MA

Kino Border Initiative (KBI)
Leaders of Kenosha
Long Beach Alliance for Clean Energy
Make the Road States
MAS PACE GLA
Muslims for Just Futures
National Hispanic Media Coalition
National Organization for Women
NJ Appleseed Public Interest Center
Nonviolence International
North American Climate, Conservation and Environment (NACCE)
Northern Indivisible
Northwest Indivisible
Oakland Privacy
Organize for Peace
Peace Action
People Power United
Progressive Leadership Alliance of Nevada
Project on Government Oversight
Project South
Public Citizen
Rachel Carson Council
Reporters Without Borders (RSF)
Restore The Fourth - Action
ReThinking Foreign Policy
RootsAction
Sapiens First
Secure Justice
Snake River Alliance
Spin Film Impact
The Leadership Conference on Civil and Human Rights
The Restaurant Opportunities Center of Pennsylvania (ROC PA)
The Sikh Coalition
The Tech Oversight Project
UltraViolet Action
UnidosUS
Union of Arab American Women Club
Veterans For Peace, Chapter 23, Rochester, NY
Voices for Progress
Whistleblower & Source Protection Program (WHISPeR) at ExposeFacts

William E. Morris Institute for Justice
Win Without War
Wisconsin Muslim Civic Alliance
X-Lab
Yankee National Party

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