

AI is making it very easy for the government to spy on you. Some lawmakers are worried.

AI's increasing ability to sift through data and track

Americans' locations has some lawmakers reconsidering parts of the Foreign Intelligence Surveillance Act.

By [Jared Perlo](#)

The long-running fight to rein in the government's power to search Americans' phone calls, emails and text messages without a warrant has gained new urgency on Capitol Hill over concerns that AI will supercharge state surveillance.



Subscribe to read this story ad-free

Get unlimited access to ad-free articles and exclusive content.



Privacy advocates warn that if the law enabling warrantless monitoring of Americans is not meaningfully reformed, many citizens could be subject to increasingly invasive AI-powered analysis of communications swept up by foreign intelligence programs as well as commercially available location and behavioral data.

“Imagine instead of doing a query with one person that you turned AI loose on these databases,” Rep. Thomas Massie, R-Ky., said Thursday at a press conference announcing a [new bill to close data-collection loopholes](#). “There’s virtually nothing the government can’t know about you.”

Section 702 of the Foreign Intelligence Surveillance Act (FISA) allows the government to collect the communications of foreigners abroad, but it also enables the government to collect messages, emails and other transmissions from Americans when they contact foreigners. The government can then perform warrantless searches on those emails, messages and other communications. Though the provision was originally passed in 2008, lawmakers must renew it every few years.

A bipartisan coalition of lawmakers has emerged in recent weeks to tackle concerns about AI’s ability to search through the mountains of data procured through Section 702. In March, Rep. Warren Davidson, R-Ohio, and co-sponsors in the House and Senate [introduced a sweeping FISA reform bill](#).

“For years, there have been jaw-dropping abuses of section 702,” Sen. Ron Wyden, D-Ore., a co-sponsor of the Government Surveillance Reform Act, said on the Senate floor last week. “Government officials have searched through 702 data to find Black Lives Matter protesters, political campaign donors, elected officials, even a state judge who complained about police abuses.”



[FOR SUBSCRIBERS](#)

America's law enforcement agencies should be able to harness technology responsibly, Wyden said, "but new tools require new rules. Without new rules, you can count on the executive branch to run roughshod over Americans' privacy rights and constitutional freedoms."

While the FISA renewal process is often fraught, as opposing sides weigh the trade-offs between surveillance and security, this year's fight has been particularly acrimonious. Section 702 was set to expire on Monday, but lawmakers agreed to a 10-day extension to provide more time to debate new protections and safeguards.

The White House [has pushed congressional Republicans](#) to pass an extension of Section 702 without any changes.

In a statement, a White House spokesperson told NBC News: “The Administration continues to have positive conversations and remains open to proposals that Congress can reach consensus on that would reauthorize FISA.”

On Thursday afternoon, House Speaker Mike Johnson, R-La., [introduced a new version of the spy law](#) that would extend Section 702 for three years.

While the new bill added some safeguards, the text did not add a requirement for search warrants sought by some Republicans.

In a statement to NBC News, Wyden said the latest draft was window dressing for the same hollow privacy guarantees: “The latest House FISA bill is a rubber stamp for [President Donald] Trump and [FBI Director] Kash Patel to spy on Americans without a warrant. Don’t fall for fake reforms.”

Thursday’s draft follows [a dramatic midnight mutiny](#) last Friday from a group of 20 House Republicans, many of whom belong to the conservative House Freedom Caucus. Johnson had [called a vote on a longer, five-year extension](#) for Section 702 that was quickly beaten back. A [final vote at 2:07 a.m. on reauthorizing the legislation](#) for 18 months also failed, leading Johnson to agree to the 10-day extension while members hash out a new version.

Even some Democrats who had previously voted in favor of Section 702 in 2024 are now refusing to reauthorize the law without meaningful amendments.

“We must reform FISA to protect our privacy and civil liberties and ensure that Section 702 will not be used to spy illegally on Americans,” said Rep. Jamie Raskin, D-Md., [in a hearing last week](#). Like others, Raskin highlighted

the Trump administration's hollowing out of existing oversight mechanisms, like the Privacy and Civil Liberties Oversight Board, as reasons to ensure stronger safeguards.

"Times have changed since 2024. The watchdogs are gone," said Raskin.

"Those reforms now depend on Trump administration officials to respect the law, which I am afraid is oxymoronic, if not just moronic."

He also noted that many surveillance activities allowed by Section 702 will already continue through March 2027 due to a legislative stipulation extending the authority for months if Congress cannot agree on a longer-term reauthorization.

Privacy advocates [have long sought](#) to require warrants for searches of Americans' data swept into the databases powered by Section 702 and curated by data brokers. At the same time, many national security proponents and experts in the intelligence community argue that such restrictions would impede law enforcement efforts and pose severe national security risks.

The CIA and other intelligence agencies have also weighed in on the Section 702 debate, highlighting the authority's importance to American security efforts. "To be clear, the US Government cannot use Section 702 to target Americans' electronic communications for

Collection," a [CIA handout says](#), adding that the law [helped prevent a terror attack at a Taylor Swift concert in Austria](#). "Section 702 is the most extensively overseen US intelligence collection tool, with built-in protections for Americans' privacy and civil liberties."

However, civil liberties advocates note that Americans' data is often collected even when they are not explicitly targeted and that agencies then run searches on Americans once this data is obtained.

“Section 702 is so vast that it incidentally collects Americans’ information,” said Jason Pye, vice president of the Due Process Institute, a bipartisan nonprofit that advocates for fairness in the legal system. “The FBI can then search for a person, for an American, without a warrant. That’s what we’re trying to solve.”

Alongside the sharp exchanges about Section 702, lawmakers are also debating whether to introduce new restrictions on the government’s ability to purchase data from third-party data brokers. These brokers collect and curate commercially available data on Americans gleaned from advertisements and other tracking technologies, along with information from public records.



Experts sound alarm as new AI-generated videos of Iran war spread across social media

Brokers sell their data to paying customers — including government agencies — who can then search these databases to track Americans' precise locations, internet browsing activity, travel history, known associates and family members, and even purchase history and transaction patterns.

The directors of the [National Security Agency](#) and [the FBI](#) have acknowledged that the agencies buy data on Americans from third-party brokers to use in their investigations. Yet experts say that the rise of AI could allow government agencies to conduct more — and more accurate — searches of commercial data and information contained in Section 702 databases.

“The technology allows basically a panopticon,” said Brendan Steinhauser, CEO of the nonprofit Alliance for Secure AI, which aims to educate Americans about risks from AI, and a leading conservative voice on the technology. “You can just have AI finding the patterns, aggregating data and allowing the government to build this enormous surveillance state that threatens our civil liberties.”

In late March, Wyden sent a letter to America's leading AI companies to understand whether they would allow the government to use their technology to surveil Americans, including through the collection of bulk commercial data or intelligence data that might inadvertently include Americans' information.

Wyden's office said only Anthropic and Google replied, with no reply from OpenAI or xAI.

The companies' replies, shared exclusively with NBC News, note the lawmaker's concerns but largely avoid details about how the companies allow government users to analyze foreign intelligence data.

“We recognize that complex challenges can be posed by the intersection of rapidly advancing AI and government operations,” wrote Anne Wall, Google's

head of U.S. federal government affairs and public policy. "As we navigate this landscape, our teams maintain a deep respect for the privacy and civil liberties of individuals."

In the response from Anthropic, the company's head of North America government affairs, Brian Peters, said it was committed to protecting civil liberties and had designed its usage policy to ban "unauthorized surveillance or tracking of individuals." Peters said Anthropic barred "analysis of the product of bulk domestic collection," appearing to reference the practices of commercial data brokers.

However, referring to Wyden's Section 702 concerns, Peters said Anthropic had granted an exception "to a small number of national-security customers, permitting the use of our models for foreign intelligence analysis in accordance with applicable law." Peters said that Anthropic's AI systems could be used to analyze this foreign intelligence information, even if it "includes incidentally collected U.S.-person information."

Anthropic, developer of the popular Claude family of AI models, made a public stand earlier this year after expressing concerns about how the Pentagon would use its systems, particularly regarding the use of AI for domestic mass surveillance.

"We support the use of AI for lawful foreign intelligence and counterintelligence missions," Anthropic CEO Dario Amodei [wrote in a statement in late February](#). "But using these systems for mass domestic surveillance is incompatible with democratic values. AI-driven mass surveillance presents serious, novel risks to our fundamental liberties."

Pye, of the Due Process Institute, said Americans across the political spectrum should realize the power of AI-fueled surveillance. "Some of these AI systems, with the data that's available, they can essentially track where

you're coming, where you're going, where you work, how much you earn,  
who you know, political affiliations, Facebook pages, Twitter accounts," Pye  
added.

"I think this is really concerning, particularly in this very heightened, very  
polarized, hyperpartisan political atmosphere."

SHARE

ADD NBC NEWS TO GOOGLE