

The Washington Post

The Cybersecurity 202: What's making critics most worried about competing House surveillance bills

By Tim Starks and Ellen Nakashima

December 12, 2023



By [Tim Starks](#) and [Ellen Nakashima](#)
with research by [David DiMolfetta](#)

Welcome to The Cybersecurity 202! The ol' pacemaker-hacking story popped up in a TV show I watched recently. I won't say more so as not to spoil things.

Below: China's cyber operatives are breaching critical U.S. infrastructure, and North Korea-linked hackers continue exploiting Log4j vulnerabilities. First:

What's making critics most worried about competing surveillance bills in the House



House Intelligence Committee Chairman Michael Turner (R-Ohio), left, and the committee's top Democrat, Rep. Jim Himes (Conn.), talk to reporters in June. (Ricky Carioti/The Washington Post)

There are two competing House proposals to revise and extend a potent surveillance tool due to expire at year's end — and the opposing sides of the debate have tried to paint each other's bills as fatally flawed.

- On one side, critics say the House Intelligence Committee-approved version would dramatically expand the range of businesses that could be compelled to aid government surveillance, down to coffee shops that provide WiFi service.
- On the other side, critics say the House Judiciary Committee-approved version would delay or inhibit investigations into a range of heinous crimes, such as human trafficking.

That only scratches the surface of the broadsides launched against both bills, which tackle an update and extension of Section 702 of the Foreign Intelligence Surveillance

Act, long touted by national security officials as one of the most powerful surveillance authorities in the government's arsenal and long decried by civil liberties advocates as privacy-invasive.

The House was expected to take up both bills today for an unusual showdown, but the House Rules Committee on Monday ditched a scheduled vote of its own to set up the procedure under which the legislation could move on the House floor. But the House is separately set to vote on a defense policy bill this week that would extend the existing Section 702 authorities through April 19, giving lawmakers more breathing room to settle on a longer-term overhaul.

Let's take a look at one of the largest objections to each major long-term Section 702 proposal.

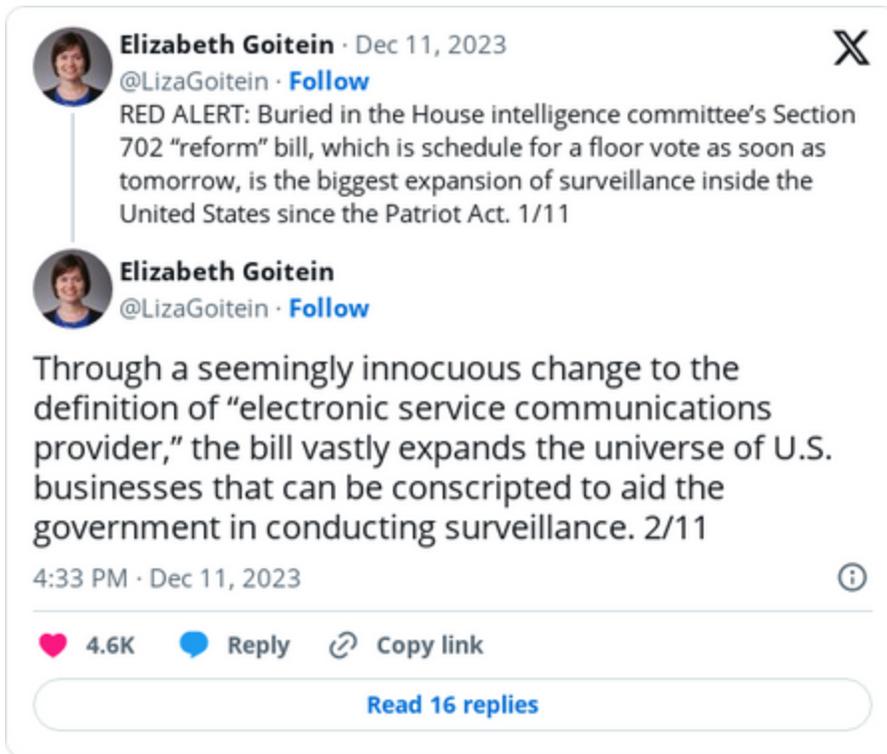
The knock on the Intelligence bill

Under Section 702, the intelligence community can spy without a warrant on the communications of foreign targets located abroad, some of whom might be speaking with people in the United States, with the court-ordered cooperation of electronic communications service providers. The FBI can query the database of communications using identifiers, such as names and phone numbers, for U.S. people and companies.

Under the House Intelligence Committee bill, critics say, a modified definition of what constitutes such a provider includes any provider — not just an electronic communications provider — that has access to **“equipment that is being or may be used to store such communications.”**

That means, as the Electronic Frontier Foundation's director of federal affairs, **India McKinney**, wrote last week, that “the HPSCI bill would expand that definition to include a much broader range of providers, including those who merely provide hardware through which people communicate on the Internet.”

Here's **Elizabeth Goitein**, co-director of the liberty and national security program at the Brennan Center for Justice, expounding on the potential ramifications:



The top Democrat on the Intelligence panel, Rep. **Jim Himes** (Conn.), rejected the criticism in a statement.

“The allegation that the FISA Reform and Reauthorization Act of 2023 expands the program’s reach to target Americans is categorically false,” he said.

- The criticized section “is a narrow modification intended to modernize the statute to ensure it remains relevant to ever-evolving communication technologies,” he continued.
- “As with all portions of Section 702, the government is only permitted to use the authority to target specific foreign targets based overseas, and all of the protections built into the statute by Congress and enforced by the FISA Court will remain in place,” Himes said. “Arguments otherwise are either misinformed or disingenuous.”

A committee aide, who spoke on the condition of anonymity under ground rules set by the panel, said, “This is a narrow change of the definition that will help us better get after some of our highest-priority intelligence targets.”

- The aide said it was “ridiculous” to suggest that the bill would cover someone who comes to a residence to repair WiFi, and about the idea of the bill covering WiFi and coffee shops, the aide said, “It is impossible for me to imagine a scenario where that would be permissible under any range of provisions of 702” and 702-related functions.

The Intelligence Committee provision was spurred by FISA Court and FISA Court of Review decisions, recently declassified, which held that a provider that had been served with a 702 order was not covered under the current definition in the law and thus did not need to comply, said a senior Justice Department official, who spoke on the condition of anonymity under ground rules set by the department. The court of review’s 2023 decision suggested that the government could ask Congress to close “any unintended gap in coverage.” And that is what the government is seeking to do through the Intelligence Committee’s bill, the official said.

“The problem emerges because of the manner in which companies facilitate and store communications today wasn’t anticipated when 702’s definition of ‘electronic communication service provider’ was first put into place,” the official said.

U.S. officials are reluctant to be too specific about what types of companies or service providers they are seeking to have covered, because, they say, the information is classified and disclosing it could help adversaries seeking to avoid surveillance.

Nonetheless, the provision could be read to cover commercial landlords and data centers, for instance, argued **Marc Zwillinger**, an attorney at the ZwillGen law firm who counsels clients on subjects like FISA.

The DOJ official pushed back on the notion. An entity that exists solely to store information such as corporate records — not communications — would not be covered by the provision, the official said.

Further, the official said, nothing in the Intelligence bill changes the overall requirement that the government must be targeting or seeking the communications of a foreigner located overseas.

Still, Zwillinger told us, “This change opens the door to a wider range of collection than would be possible today.”

The knock on the Judiciary bill

Meanwhile, the House Judiciary Committee’s bill has faced criticism that it would keep law enforcement from using information on U.S. persons acquired under 702 “as evidence against such person in any criminal, civil, or administrative proceeding or used as part of any

criminal, civil, or administrative investigation,” as the bill states, except for a subset of threats such as cyberattacks.

That leaves off a list of other crimes — including kidnapping and child exploitation — where 702-acquired data could otherwise be used in a prosecution, observed a senior congressional aide who opposes the Judiciary bill and spoke on the condition of anonymity because of the sensitive nature of the legislation. And the bill says “it may not be used as part of any investigation,” the aide said, “which means if you stumble across this and want to go and get a warrant, or you want to go and find it a different way, you’re not allowed to because you found this information and you’re not allowed to be able to know that exists.”

A coalition of groups representing law enforcement such as the National District Attorneys Association and the National Association of Police Organizations have criticized another portion of the bill for similar reasons. The legislation would prohibit data brokers from selling consumer data to law enforcement and federal agencies. The law enforcement groups say that would delay their investigations into grave crimes.

Spokespeople for Judiciary Committee Republicans didn’t respond to a request for comment on concerns over how the measure handles criminal information. Nor did representatives for the bill’s sponsor, Rep. **Andy Biggs** (R-Ariz.), who instead responded generally elsewhere to the debate over his legislation:

