

## RISAA's Surveillance Expansion: A Dangerously Broad "Fix" to a Narrow Fact Pattern

The Reforming Intelligence and Securing America Act (RISAA) includes what Senator Wyden [describes](#) as **"one of the most dramatic and terrifying expansions of government surveillance authority in history."** This provision would allow the government to compel a vast range of U.S. businesses to assist the NSA in Section 702 collection. As FISA Court amicus Marc Zwillinger [explains](#), everyday businesses could be required to give the NSA access to all of the communications transmitted or stored on their phones, computers, servers, or wifi routers, which the NSA would then scan for foreign targets (mimicking the controversial "upstream" program).

In an effort to quash the growing alarm over this provision, the administration and intelligence committee leaders are circulating information about the provision that is either inaccurate or highly misleading:

***Statement:** "The provision is exceedingly narrow in both intent and effect—designed to respond to a very specific fact pattern."*

**Response: The fact pattern may be narrow, but the "fix" is extremely—and deliberately—broad.**

The purpose of the provision is to respond to a FISA Court opinion holding that a particular type of provider—[identified](#) by the *New York Times* as a data center for cloud computing—does not qualify as an "electronic communications service provider," and therefore cannot be compelled to assist the NSA in conducting Section 702 surveillance.

The administration, however, did not want to publicly reveal the type of provider at issue. Rather than draft an amendment specific to data centers, the administration deliberately drafted an amendment that sweeps much more broadly, so that no one could infer the true purpose. As [stated](#) by Marc Zwillinger, the FISA Court amicus who participated in the case giving rise to this provision: **"[T]he amendment doesn't narrowly close the gap.... Because they won't name the specific type of provider they want to cover, they are drafting overly broad language that will be interpreted to cover a variety of services, not the limited specific service they claim to need it for."**

Specifically, the provision allows the government to compel assistance, not just from electronic communications service providers (e.g., Google or Verizon), but from *"any other service provider who had access to equipment that is being or may be used to transmit or store wire or electronic communications."* **Almost every business in the United States fits this definition.** Most businesses provide some kind of service, and every business will have access to equipment (such as wifi routers or telephones) on which communications are transmitted or stored. **It would be hard to imagine a broader scope of entities.**

***Statement:** The provision "includes language to explicitly exclude" "providers who cater to users inside the U.S."*

**Response:** The definition excludes exactly four types of entities; the vast majority of U.S. businesses are *not* excluded. As Zwillinger [points out](#): **"The breadth of the new definition is obvious from the fact that the drafters felt compelled to exclude such ordinary places such as senior centers, hotels, and coffee shops. But for these specific exceptions, the scope of the new definition would cover them—and scores of businesses that did not receive a specific exemption remain within its purview."** Businesses not excluded by the definition include such commonly visited places as barber shops, laundromats dentist's offices, and—perhaps most alarmingly—commercial landlords who rent out the office space where tens of millions of Americans go to work every day.

**Statement:** *“Nothing in this [provision] changes the core principle of Section 702, which is that it can be used only to obtain the electronic communications of foreign nationals abroad.”*

**Response:** This is true, but it misses the point. Under current law, the government can compel a narrow range of electronic service providers, like Google and Verizon, to turn over foreign targets’ communications. Under this provision, countless U.S. businesses that provide wifi to their customers could be required to give the NSA access to *all the communications transmitted on their equipment*—including enormous volumes of wholly domestic communications—trusting the NSA to extract and remove only the communications of foreign targets.

**Whatever “narrow” fact pattern the administration is seeking to address, a law that allows the NSA to compel almost any U.S. business to provide the agency with wholesale access to its customers’ communications is NOT the solution.**

*For questions about Section 702, contact Liza Goitein at [goiteine@brennan.law.nyu.edu](mailto:goiteine@brennan.law.nyu.edu) or Noah Chauvin at [chauvinn@brennan.law.nyu.edu](mailto:chauvinn@brennan.law.nyu.edu).*