BRENNAN CENTER FOR JUSTICE

The Senate Must Stop "One of the Most Dramatic and Terrifying Expansions of Government Surveillance Authority in History"

The Reforming Intelligence and Securing America Act (RISAA), as amended in the House, authorizes **the largest expansion of surveillance on domestic soil since the Patriot Act.** The potential for abuse of this new authority is staggering, and the Senate must not permit it to become law.

How the House ECSP provision works. Under current law, the government conducts Section 702 surveillance with the compelled assistance of **"electronic communications service providers,"** such as Verizon and Gmail, that have direct access to Americans' communications. The government obtains orders from the FISA Court requiring the companies to provide assistance, generally by turning over the communications of designated targets.

RISAA vastly expands the universe of entities that can be compelled to provide assistance to include providers of *any* service, as long as they have access to the equipment on which communications are transmitted. **This category sweeps in an enormous range of U.S. businesses that provide wifi to their customers and therefore have access to routers or other equipment on which communications transit.**

- Although the provision exempts hotels, libraries, restaurants, and a handful of other establishments, **the vast majority of U.S. businesses—department stores, barber shops, laundromats, hardware stores, dentist's offices, fitness centers—would be fair game. So would the commercial landlords that lease the office space where tens of millions of Americans go to work every day, including the offices of journalists, lawyers, nonprofits, and others.**
- Unlike Verizon or Gmail, most of these businesses would lack the ability to isolate and turn over individual communications. They would therefore be forced to give the NSA direct access to the equipment itself, and to all the communications routed or stored on that equipment—including countless communications between and among Americans. **The NSA would be on the "honor system" to pull out and retain only the communication of foreign targets.**

What the government says. The administration and intelligence committee members have portrayed this as a "narrow" fix to a FISA Court ruling that the government could not compel assistance from a specific type of provider—reportedly, a data center for cloud computing. **But while the *problem* may be "narrow," the *fix* is anything but.**

- As the FISA Court amicus who participated in that FISA Court case explained: **"[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."** The provision is not just overbroad; it's *deliberately* overbroad, to conceal its true purpose.
- The same FISA Court amicus warned that **"[t]he breadth of the new definition is obvious."** Even though the definition exempts a few types of businesses, "**scores of businesses that did not receive a specific exemption remain within its purview."** The provision even encompasses "delivery personnel, cleaning contractors, and utility providers."
- Senator Ron Wyden, who has a history of issuing prescient warnings about surveillance overreach (such as the NSA's bulk collection of Americans' phone records), stated that **this provision "represents one of the most dramatic and terrifying expansions of government surveillance authority in history."**

No democracy should allow its government to have such an Orwellian power. Even if the current administration does not plan to make full use of this authority, a future administration surely will. **The Senate should vote to remove this provision, and if the provision is not removed, the Senate should not pass RISAA.**

For questions about Section 702, contact Liza Goitein at goiteine@brennan.law.nyu.edu or Noah Chauvin at chauvinn@brennan.law.nyu.edu.