BRENNAN
CENTER
FOR JUSTICE

Vote YES on Amendment to Strike "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.** Senator Wyden has described it as **"one of the most dramatic and terrifying expansions of government surveillance authority in history,"** and Marc Zwillinger, one of the FISA Court's amici curiae (outside experts appointed to assist the court), has taken the rare step of going public with his concerns about the provision.

How the 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.**

- Almost every U.S. businesses could be described as providing some type of "service." And every business has access to equipment on which communications are routed or stored: phones, computers, wifi routers, or servers. For the large number of businesses that offer wifi to their customers, this equipment will contain their customers' communications as well as their own.
- 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.**
- Moreover, even the small number of exemptions come with a loophole. Even though a hotel could not be required to provide assistance, anyone who provides a service within that hotel and has access to the hotel's communications equipment—such as an IT service provider—could be forced to help the NSA to access the communications transmitted and stored on that equipment.
- 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 defenders of the ECSP provision say—and why they're wrong.

"This is a narrow fix."

- Supporters of this provision have portrayed it 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 issue that prompted this provision may be "narrow," the "fix" is anything but.**
- As Marc Zwillinger, who participated as an amicus 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.

- Zwillinger 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."

"This doesn't change the fact that targets of Section 702 must be foreigners overseas. Nothing in this provision permits the targeting of U.S. businesses or places of worship."

- Such statements are a thinly veiled attempt to mislead members by conflating *targets* of surveillance with entities that can be requires to *assist with surveillance*.
- While the provision does not allow the government to "target" a U.S. business—in other words, to collect and review all of its communications—it *does* allow the government to require almost any business or place of worship to give the NSA access to their communciations equipment (phones, computers, wifi routers), trusting the NSA to extract and remove only the communications of foreign targets. The potential for abuse of such a provision is staggering.

"This change is necessary to address changes in technology over the past 15 years."

- As noted, the provision—on its face—is far broader than needed to address the partciular type of provider (a data center for cloud computing) at issue.
- A similar provision was included in the Protect America Act in 2007; Congress recognized its mistake and removed the provision when it passed Section 702. **A provision that originated in 2007 cannot be a response to changes in technology that have occurred over the past 15 years** (i.e., since 2009).

"We cannot pass this amendment because the bill would have to go back to the House, pushing Congress beyond the April 19 sunset date. Section 702 would temporarily lapse and we would lose valuable intelligence."

- As reported by the *New York Times*, even if Section 702 were to expire, **"the suggestion that the tool itself would simply lapse on April 19 is significantly misleading."** That's because the FISA Court has approved a one-year "certification" that will allow the government to continue conducting Section 702 surveillance until April 2025. Under a provision of the FISA Amendments Act, certifications remain valid until their expiration date, regardless of the sunset.
- Administration officials nonetheless claim that some companies might refuse to comply with directives to turn over targets' communications. They note that a few companies did exactly that after the predecessor to Section 702, the Protect America Act, expired in 2008. But as the *New York Times* article points out, **those companies lost in court.**
- Since then, the law has only gotten stronger on the side of the government; **in passing the FISA Amendments Act in 2008, Congress added language to make clear that FISA Court certifications remain valid until their expiration "notwithstanding any other provision" of the law, including the sunset provision.**
- **Why would companies risk fines of $250,000 per day to launch a legal battle that the government already won 16 years ago?** The administration's claimed fears of noncompliance are vastly overblown and are designed to prevent the Senate from voting to improve this deeply flawed bill. **The Senate must not cave to this pressure; it must take the time it needs to get this right.**

No democracy should allow its government to have this 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.