May 9, 2024

The Honorable Merrick Garland
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530-0001

The Honorable Avril Haines
Director of National Intelligence
Office of the Director of National Intelligence
Washington, D.C. 20511

Dear Attorney General Garland and Director Haines:

The undersigned organizations write to urge you to exercise your discretion to declassify, or otherwise make public, information revealing the type of service provider at issue in the Foreign Intelligence Surveillance Court (FISC) case that gave rise to the new definition of "electronic communications service provider" (ECSP) in the Reforming Intelligence and Securing America Act (RISAA). Without such a public disclosure, the ECSP definition is likely to remain dangerously overbroad, significantly increasing the chance of surveillance abuses.

History of the ECPS provision

The new ECSP definition, passed by the House as an amendment to RISAA in a highly rushed process, sparked widespread alarm. On its face, the new definition would permit the NSA to compel almost any U.S. business to assist with Section 702 surveillance, as most businesses provide some type of "service," and all businesses have access to equipment on which communications might be routed or stored (such as phones, computers, and wifi routers). Because many U.S. businesses would lack the ability to isolate and turn over the communications of specific targets, they could be forced to give NSA personnel direct access to their communications equipment. Senator Ron Wyden described this sweeping provision as "one of the most dramatic and terrifying expansions of government surveillance authority in history."

As the *New York Times* reported, the purpose of the new definition was to address a FISC decision holding that data centers for cloud computing did not qualify as "electronic communications service providers." Rather than simply add data centers to the existing definition, however, the administration deliberately proposed much broader language in order to conceal the type of provider at issue, as this information was (and remains) classified. The administration thus pushed for—and the House passed—a staggeringly broad new power.

When the bill moved to the Senate, concerned Senators made a powerful case for stripping this new definition from the bill. Senator Mark Warner, who chairs the Senate Select Committee on Intelligence, admitted that the provision "could have been drafted better." He nonetheless urged his colleagues to pass the bill without amendment, as amending the bill would cause Congress to miss the April 19th deadline for reauthorization. He promised, however, to work with concerned members to try to narrow the provision using an upcoming legislative vehicle, such as the Intelligence Authorization Act or the National Defense Authorization Act. Based on this promise, the Senate passed the bill.

Unfortunately, even though the true purpose of the provision is now widely known to the public, it nonetheless remains classified. As a result, while congressional leaders might be willing to narrow the new definition somewhat, they are unlikely to agree to a revision that specifically names data centers. Yet the alternative is to draft a provision that is imprecise and therefore could be exploited to include additional types of providers beyond data centers. Although this administration issued a written commitment to apply the new definition only to the type of provider at issue in the FISC decision, that commitment cannot and will not bind future administrations.

The Case for Declassification

Deliberately writing overbroad surveillance authorities and trusting that future administrations will decide not to exploit them is a recipe for abuse. And it is entirely unnecessary, as the administration can—and should—declassify the fact that the provision is intended to reach data centers.

The executive order governing classification allows agency heads or senior agency officials to declassify information as a matter of discretion if "the public interest in disclosure outweighs the damage to the national security that might reasonably be expected from disclosure." E.O. 13526 §3.1(d). In this case, there is an overriding public interest in avoiding overbroad or imprecise surveillance authorities. Unnecessarily expanding the universe of U.S. companies that may be compelled to assist the NSA in conducting Section 702 surveillance not only creates a burden on those companies; it also broadens the scope of "incidental" collection of Americans' information and creates significant new opportunities for abuse.

On the other side of the equation, declassifying this information would cause little if any national security harm. The *New York Times* has already revealed that the relevant FISC case addressed data centers for cloud computing. In the Senate debate over this provision, multiple Senators either stated or implied that the provision was intended to address data centers. Senator Warner himself confirmed this information in his remarks on the floor, when he described the FISC case that gave rise to the provision:

> Now, why has this suddenly now become such an issue? Well, one of those communications providers—remember I talked about clouds, data centers, how these networks come together and how network traffic is intertangled at these data centers? One of these entities that controlled one of those new enterprises that didn't exist in 2008 said: Well, hold it. You can't compel us to work with the American government because we don't technically fit the definition of an electronic communications service provider. And the fact was, the company that raised that claim won in court. So what happened was, the FISA Court said to Congress: You guys need to close this loophole; you need to close this and change this definition. So that is where a lot of this debate has come from.

This is not a situation where official confirmation of information that has already been made public could lead to national security harms. Any foreign target who might alter their behavior upon learning that data centers may be served Section 702 directives has already done so. There is no reason why foreign adversaries would wait for official confirmation before acting on information disclosed by a respected national security reporter and confirmed by several senators, including the Senate intelligence committee chairman.

It is hard to imagine a stronger case for discretionary declassification. We urge you to live up to the principles of transparency you have both espoused on past occasions and declassify this widely-known information, so that Congress may pass responsible and appropriately tailored surveillance legislation.

Sincerely,

Access Now

American Civil Liberties Union (ACLU)

Asian Americans Advancing Justice / AAJC

Asian American Federal Employees for Nondiscrimation (AAFEN)

Brennan Center for Justice at NYU School of Law

Center for Democracy & Technology

Defending Rights & Dissent

Due Process Institute

Electronic Frontier Foundation

Electronic Privacy Information Center (EPIC)

Fight for the Future

Freedom of the Press Foundation

FreedomWorks

Government Information Watch

MPower Change

Muslims for Just Futures

Project for Privacy & Surveillance Accountability (PPSA)

Project On Government Oversight

Restore the Fourth

X-Lab