Congress of the United States

Washington, DC 20515

March 26, 2026

The Honorable Tulsi Gabbard
Director of National Intelligence
Washington, D.C. 20511

Dear Director Gabbard:

We write to urge you to let the American people know what, if any, impact the use of commercial Virtual Private Network (VPN) services can have on their privacy rights against warrantless surveillance by U.S. intelligence agencies.

Heeding the advice of federal agencies such as the Department of Defense, Federal Bureau of Investigation, National Security Agency, and Federal Trade Commission, millions of Americans use commercial VPN services, which purport to protect their privacy by hiding the customer's IP address, and consequently their country, as the source of their internet traffic. While VPN services can protect against some privacy and security threats, their use by Americans has the potential to impact their privacy rights against warrantless government surveillance.

VPNs hide the IP address of a user's phone or computer from websites and apps, which can otherwise be used to approximate the user's location, and in some cases, uniquely identify them. Commercial VPNs do this by sending their customers' web and app data through servers that the companies operate, hiding the true origin. A single VPN server will typically be used by hundreds, if not thousands of users concurrently from countries around the world, and their internet traffic will be comingled, all appearing to originate from the same IP address. VPN companies operate servers around the world and allow their users to choose which servers they use. Some users may intentionally use VPN servers from other countries to, for example, attempt to access region-controlled content, such as live sports.

VPNs are far more effective at hiding a user's true location and country than enabling a user to convincingly impersonate a specific country. This is because cybersecurity companies maintain and sell lists of the IP addresses of commercial VPN servers, which other companies, including streaming platforms, subscribe to. By subscribing to a list of commercial VPN servers, a company may be able to determine that a visitor to their website or app is likely a VPN user, but cannot identify where in the world that user is actually located. Not all companies subscribe to these lists and restrict access to VPN users, but some do. Consequently, major streaming platforms like Netflix will block region-restricted content to users accessing the service from a known VPN server, because the company cannot identify the country in which the user is located.

But the use of VPNs may also significantly impact Americans and their rights as it relates to U.S. government surveillance. The U.S. intelligence community's authority to target Americans for surveillance is strictly regulated under the Foreign Intelligence Surveillance Act (FISA). Surveillance

of Americans' communications generally requires a court order authorized by a judge on the Foreign Intelligence Surveillance Court. In contrast, Section 702 of FISA permits the warrantless targeting of foreigners overseas, while Executive Order 12333 permits both the targeting of foreigners overseas and bulk, indiscriminate surveillance of foreigners' communications. While statutory law and the Attorney General-approved guidelines governing surveillance under EO 12333 make distinctions between the privacy protections afforded to U.S. persons and those denied to foreigners, there remain questions about how the government should treat the data of people whose identity, citizenship, or location is unknown to the government.

Under both Section 702 and EO 12333, the government is obligated to seek to determine the non-U.S. person status and location of its targets. Nonetheless, the federal government has taken the position that communications whose source remains unknown are treated as foreign, and thus subject to few privacy protections. This legal theory is spelled out in the NSA's declassified targeting procedures for surveillance under Section 702 of FISA, which state that "A person known to be located outside the United States or whose location is not known will be presumed to be a non-United States person unless such person is identified as a United States person, or the circumstances otherwise give rise to a reasonable belief that such person is a United States person."

These presumptions also apply to surveillance conducted under EO 12333. For example, procedures governing Department of Defense signals intelligence activities state that "A person or organization outside the United States, or whose location is not known to be in the United States, is presumed to be a non-U.S. person, unless specific information to the contrary is obtained."

Americans reportedly spend billions of dollars each year on commercial VPN services, many of which are offered by foreign-headquartered companies using servers located overseas. According to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, VPNs have the potential to be vulnerable to surveillance by foreign adversaries. While Americans should be warned of these risks, they should also be told if these VPN services, which are advertised as a privacy protection, including by elements of the federal government, could, in fact, negatively impact their rights against U.S. government surveillance. To that end, we urge you to be more transparent with the American public about whether the use of VPNs can impact their privacy with regard to U.S. government surveillance, and clarify what, if anything, American consumers can do to ensure they receive the privacy protections they are entitled to under the law and Constitution.

Thank you for your attention to this important matter.

Sincerely,

Ron Wyden
United States Senator

Sara Jacobs
Member of Congress

Alex Padilla
United States Senator

Edward J. Markey
United States Senator

Pramila Jayapal
Member of Congress

Elizabeth Warren
United States Senator