

Congress of the United States

Washington, DC 20515

February 13, 2025

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

Dear Director Gabbard:

We write to urge you to act decisively to protect the security of Americans' communications from dangerous, shortsighted efforts by the United Kingdom (U.K.) that will undermine Americans' privacy rights and expose them to espionage by China, Russia and other adversaries.

According to recent press reports, the U.K.'s Home Secretary served Apple with a secret order last month, directing the company to weaken the security of its iCloud backup service to facilitate government spying. This directive reportedly requires the company to weaken the encryption of its iCloud backup service, giving the U.K. government the "blanket capability" to access customers' encrypted files. This order was reportedly issued under the U.K.'s Investigatory Powers Act 2016, commonly known as the "Snoopers' Charter," which does not require a judge's approval. Apple is reportedly gagged from acknowledging that it received such an order, and the company faces criminal penalties that prevent it from even confirming to the U.S. Congress the accuracy of these press reports.

These reported actions seriously threaten the privacy and security of both the American people and the U.S. government. Apple does not make different versions of its encryption software for each market; Apple customers in the U.K. use the same software as Americans. If Apple is forced to build a backdoor in its products, that backdoor will end up in Americans' phones, tablets, and computers, undermining the security of Americans' data, as well as of the countless federal, state and local government agencies that entrust sensitive data to Apple products.

The Salt Typhoon hack of U.S. telephone carriers' wiretapping systems last year — in which President Trump and Vice President Vance's calls were tapped by China — provides a perfect example of the dangers of surveillance backdoors. They will inevitably be compromised by sophisticated foreign adversaries and exploited in ways harmful to U.S. national security. As the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI confirmed last November, People's Republic of China (PRC)-affiliated actors were involved in "copying of certain information that was subject to U.S. law enforcement requests pursuant to court orders."

The risk does not just come from wiretapping systems — when sensitive data is stored by third parties, without end-to-end encryption, it is vulnerable to theft when those service providers are hacked. That is exactly what has happened in 2023, when PRC-affiliated hackers broke into Microsoft's systems storing federal agencies' emails. As the Department of Homeland Security's Cyber Safety Review Board documented, the foreign spies "struck the espionage equivalent of gold," enabling them to access "the official email accounts of many of the most senior U.S. government officials managing our country's relationship with the People's Republic of China" and "downloaded approximately 60,000 emails from State Department alone."

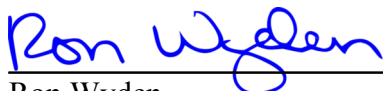
After years of senior U.S. government officials — from both Republican and Democratic Administrations — pushing for weaker encryption and surveillance backdoors, it seems that the U.S. government has finally come around to a position we have long argued: strong end-to-end encryption protects national security. Indeed, in the wake of the Salt Typhoon hack, CISA released public guidance which recommended that high-value targets, including Members of Congress, solely use end-to-end encrypted communications tools, like Signal.

While the U.K has been a trusted ally, the U.S. government must not permit what is effectively a foreign cyberattack waged through political means. If the U.K. does not immediately reverse this dangerous effort, we urge you to reevaluate U.S.-U.K. cybersecurity arrangements and programs as well as U.S. intelligence sharing with the U.K. As the U.K. Parliament’s intelligence oversight committee described in a December, 2023 public report, the U.K. benefits greatly from a “mutual presumption towards unrestricted sharing of [Signals Intelligence]” between the U.S. and U.K. and that “[t]he weight of advantage in the partnership with the [National Security Agency] is overwhelmingly in [the U.K.’s] favour.” The bilateral U.S.-U.K. relationship must be built on trust. If the U.K. is secretly undermining one of the foundations of U.S. cybersecurity, that trust has been profoundly breached.

You stated at your confirmation hearing that “backdoors lead down a dangerous path that can undermine Americans' Fourth Amendment rights and civil liberties.” And you wrote in response to a written question that “[m]andating mechanisms to bypass encryption or privacy technologies undermines user security, privacy, and trust and poses significant risks of exploitation by malicious actors.” We urge you to put those words into action by giving the U.K. an ultimatum: back down from this dangerous attack on U.S. cybersecurity, or face serious consequences. To inform ongoing Congressional oversight, please also provide us with unclassified answers to the following questions by March 3, 2025:

1. Was the Trump Administration made aware of this reported order, either by the U.K. or Apple, prior to the press reports and, if so, when and by whom?
2. What is the Trump Administration’s understanding of U.K. law and the bilateral CLOUD Act agreement with regard to an exception to gag orders for notice to the U.S. government?
3. What is the Trump Administration’s understanding of its obligation to inform Congress and the American public about foreign government demands for U.S. companies to weaken the security of their products, pursuant to the CLOUD Act?

Sincerely,



Ron Wyden
United States Senator



Andy Biggs
Member of Congress

CC: Mr. Peter Mandelson, British Ambassador.