

Congress of the United States

Washington, DC 20515

March 13, 2025

The President
Investigatory Powers Tribunal
PO Box 3322
London SW1H 9ZQ
United Kingdom

Dear Judge:

We write to request the Investigatory Powers Tribunal (IPT) remove the cloak of secrecy related to notices given to American technology companies by the United Kingdom, which infringes on free speech and privacy, undermines important United States Congress and U.K. parliamentary oversight, harms national security, and ultimately, undermines the special relationship between the United States and the United Kingdom.

According to recent press reports, the U.K. Home Secretary served Apple with a technical capability notice last month, directing the company to weaken the security of its iCloud backup service to facilitate spying by the U.K. government. The United Kingdom's demand reportedly used controversial powers that were enacted as part of the Investigatory Powers Act 2016. The Financial Times subsequently reported that Apple is challenging the order at the IPT. The IPT's public schedule states that it will hear an application in private (IPT/25/68/CH) on March 14, 2025, which press reports have indicated is the challenge brought by Apple.

We invite the IPT to apply the principles of open justice to the hearing on March 14, 2025, and to all subsequent proceedings in Apple's application. The existence of the technical capabilities notice has been widely reported and commented on, making any argument for a closed hearing on this very existence unsustainable. Further, the reality that Apple has received such a notice is confirmed by its public decision to withdraw its encryption service for all U.K. users. Apple presumably would not do this unless it felt compelled to do so by a request to insert a backdoor. Holding public hearings in these proceedings would also allow the IPT to hear expert evidence from cybersecurity specialists, civil society representatives and experts on U.S.-U.K. data flows, enabling the IPT to reach a well-informed decision as to the lawfulness of the notice. Further, it is in the public interest for there to be open hearings about the extent to which important communications services have been deliberately compromised to make them less secure.

The U.K.'s demand of Apple raises a number of serious concerns which directly impact national security and therefore warrant robust public debate. Tulsi Gabbard, the Director of National Intelligence, stated in a recent letter to Congress that the U.K.'s reported demand would be "a clear and egregious violation of Americans' privacy and civil liberties, and open up a serious vulnerability for cyber exploitation by adversarial actors." President Trump also publicly confirmed that he raised this issue during Prime Minister Starmer's recent visit to Washington, comparing the U.K.'s actions to the conduct of China.

Further, by attempting to gag U.S. companies and prohibit them from answering questions from Congress, the U.K. is both violating the free speech rights of U.S. companies and impairing Congress's power and duty to conduct oversight on matters of national security. The First Amendment to the U.S. Constitution guarantees Americans, including U.S. companies, "the right to petition the government for redress of grievances." This rule extends to communications with Congress and responses to Congressional oversight requests for information.

The U.K.'s attempted gag has already restricted U.S. companies from engaging in speech that is constitutionally protected under U.S. law and necessary for ongoing Congressional oversight. Apple has informed Congress that had it received a technical capabilities notice, it would be barred by U.K. law from telling Congress whether or not it received such a notice from the U.K., as the press has reported. Google also recently told Senator Wyden's office that, if it had received a technical capabilities notice, it would be prohibited from disclosing that fact. The U.K. embassy has also not responded to a recent request from Senator Wyden's office regarding potential demands from the U.K. to other U.S. companies.

The security of U.S. technology companies' products against surveillance by foreign governments is an important topic for ongoing Congressional oversight because of several recent hacks of the communications of senior U.S. government officials. This includes:

- The "Salt Typhoon" espionage incident in 2024, in which China hacked several major US telecommunications carriers, using lawful interception systems as the conduit to gain access. Through these hacks, China was reportedly able to tap the phone calls of senior officials including President Trump and Vice President Vance, as well as steal millions of phone records.
- The April 2024 "Snowflake" incident, in which hackers stole the phone records of "nearly all" AT&T customers. The hackers were reportedly able to identify the records of members of President Trump's family, then-Vice President Kamala Harris, and the wife of now-Secretary of State Marco Rubio, which they reportedly sent to AT&T as part of an extortion demand.
- The summer 2023 hack by China of Microsoft-hosted U.S. government email accounts, resulting in the theft of over 60,000 emails from the Department of State, as well as the compromise of the email accounts of then-Commerce Secretary Gina Raimondo, then-U.S. Ambassador to China R. Nicholas Burns, and Congressman Don Bacon.

The common link between these incidents is that sensitive government data held by third party companies was not properly secured and subsequently accessed by hackers. Further, and most importantly, the Salt Typhoon incident reportedly involved compromising "lawful intercept" systems of the kind that it appears Apple has been ordered to build. Such systems create grave vulnerabilities which can be exploited by hostile foreign government hackers. In the wake of the most recent hack, the Cybersecurity and Infrastructure Security Agency issued public guidance in December 2024 recommending that senior government officials only use end-to-end encryption for their communications, to reduce the potential harm caused by future hacks of companies used by the government. Congress continues to conduct bipartisan oversight into the important national security issues highlighted by these cybersecurity incidents, including pushing U.S. government agencies to secure government data with end-to-end encryption.

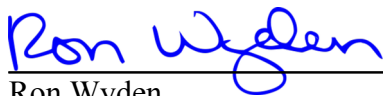
Given the significant technical complexity of this issue, as well as the important national security harms that will result from weakening cybersecurity defenses, it is imperative that the U.K.'s technical demands of Apple — and of any other U.S. companies — be subjected to robust, public analysis and debate by cybersecurity experts. Secret court hearings featuring intelligence agencies and a handful of individuals approved by them do not enable robust challenges on highly technical matters. Moreover, given the potential impact on U.S. national security, it is vital that American cybersecurity experts be permitted to analyze and comment on the security of what is proposed.

Accordingly, we urge you to permit U.S. companies to discuss the technical demands they have received from the U.K. under the Investigatory Powers Act with Congress, as well as to permit and invite robust public debate by independent cybersecurity experts before deciding the merits of the reported challenge that Apple has brought.

We invite the IPT to take account of the submissions set out in this letter in its consideration of the principles of open justice in application number IPT/25/68/CH and of any related substantive matters. We invite you to share the contents of this letter with relevant parties. We would welcome indications should any other procedure be followed for us to bring the contents of this letter within the consideration of the IPT as we seek to highlight the significant implications of the matter before you.

Thank you for your attention to this important matter.

Sincerely,



Ron Wyden
United States Senator



Andy Biggs
Member of Congress



Alex Padilla
United States Senator



Warren Davidson
Member of Congress



Zoe Lofgren
Member of Congress