Congress of the United States

Washington, DC 20515

February 26, 2025

The Honorable Pam Bondi
Attorney General of the United States
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Attorney General Bondi:

We write to seek the Department of Justice's views on whether the United Kingdom (U.K.) may have breached or otherwise acted inconsistently with the terms or spirit of the U.S.-U.K.'s Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime ("Agreement") authorized by the *Clarifying Lawful Overseas Use of Data Act* ("*CLOUD Act*").

According to press reports, the U.K.'s Home Secretary served Apple, a major U.S. technology firm, with a secret technical capabilities notice ("Notice") last month. This notice reportedly requires the U.S. company to weaken the encryption of its entire global iCloud backup service and give the U.K. government the "blanket capability" to access customers' data in plaintext. Reports further suggest the U.K. believes its notice applies not just domestically to U.K. companies, but across borders with global effect. As reported, the U.K. law is no mere domestic law and could conflict with the laws and public policy of other jurisdictions, intrude on the rights of far more people than just U.K. citizens, and significantly affect U.S. interests in ensuring U.S. companies follow responsible cybersecurity practices. Last week, Apple announced the company can no longer offer encrypted cloud backup in the U.K. to new users, and that current U.K. users would eventually need to disable this security feature, giving rise to the inference that the U.K. did indeed issue a notice to Apple, as reported. Apple is reportedly prohibited from acknowledging that it received such a notice, which limits Congressional oversight into the matter, including the extent to which the U.K. is asserting its authority over U.S. persons and entities outside of the U.K.

If these press reports are true, they necessitate the Department of Justice's review of its approval of the U.K. as a qualifying nation under the *CLOUD Act*, and whether the notice may violate or otherwise be inconsistent with U.S. law and public policy, as well as with the Agreement.

The case made for the *CLOUD Act* rested on the argument, asserted by U.K. officials in hearings before Congress and elsewhere, that without it, the U.K. would not be able to reach providers under U.S. jurisdiction to assist in investigating serious crime without those providers violating U.S. law. As you know, relying on these representations, Congress authorized the DOJ via the *CLOUD Act* to form an executive agreement with qualifying jurisdictions, which would partially lift the U.S. legal prohibitions on providers voluntarily honoring foreign legal process. The Attorney General, with the concurrence of the Secretary of State, must determine and submit a written certification to Congress that the criteria set out in the *CLOUD Act* have been met. The certification must also include an explanation of each of the statutory considerations.

Section 2523(b)(3) of Title 18 emphasizes that agreements must not create an obligation that providers be capable of decrypting data. While the statute does not say that a qualifying jurisdiction is barred from adopting laws that undermine encryption, the U.K.'s notice to Apple has the effect of extending to U.K. disclosure demands made under the Agreement the obligation to decrypt. This obligation would not exist but for the fact that the Agreement effectively removes the bar to disclosure on which Apple would otherwise rely in refusing

to make the disclosure. It splits the finest of hairs to say that because the Agreement itself does not contain an obligation to decrypt that a *CLOUD Act* country can impose such an obligation on a U.S. provider, issue disclosure orders under the Agreement that rely on such obligation, and impose penalties for non-disclosure when compliance with such orders is refused.

Notably, there is no obligation under U.S. law to require a provider subject to U.S. jurisdiction to take the actions reportedly required by the U.K. notice. Encryption is also acknowledged by all to be a critical means to secure information systems essential to the national security and economy of our country. In the wake of recent significant cybersecurity compromises, such as the Salt Typhoon hack, U.S. officials have encouraged the adoption of encrypted communications. It is difficult to see the U.K.'s notice to Apple, if the reports are accurate, as anything less than an action that undermines U.S. law, public policy, and information security by requiring U.S. companies to take such reckless action as undermining encryption for all users globally.

In addition, to qualify for an agreement with the U.S. and gain the benefits of streamlined enforcement, section 2523(b)(1)(B)(v) of Title 18 requires the foreign government's domestic surveillance law to have sufficient accountability and transparency. The complete secrecy surrounding this matter suggests serious cause for concern that this requirement is being violated by the U.K. Gagging the recipient of such a notice to disclose its effect to its users – or even to the U.S. government – seems inconsistent with the commitment to transparency on which the certification of the Agreement in part rests.

These agreements are a product of legislation passed by the Congress. The statute contemplates Congress continuing to play a significant role in the agreements signed between the United States and foreign governments. As you know, the *CLOUD Act* gives Congress the power to prevent a proposed executive agreement from entering into force through expedited congressional review provisions after the certifications are provided by the Department.

Therefore, given the U.K.'s reported conduct, and Congress's important oversight role in these matters, we respectfully request that the DOJ conduct a review of the U.K.'s compliance with the statutory requirements of the *CLOUD Act* and the terms of the Agreement, taking into account the factual predicates behind the *CLOUD Act*, the sovereign interests of the U.S. in regulating the conduct of U.S. companies, and cybersecurity public policy imperatives. This review is essential to ensure that agreements under the *CLOUD Act* uphold the privacy, security, and human rights standards that Congress set in enacting the *CLOUD Act* and will inform Congress as to whether statutory reforms are necessary to protect these strong U.S. interests.

In addition to your broader review, we ask that you respond in writing to the following questions:

1. Was the Department of Justice or anyone in the Trump Administration notified of, or consulted about, the U.K. Home Secretary's Notice? And if so, by what means and when?

2. Is the Department of Justice aware of the issuance of such a Notice to any other U.S. tech company respecting an encrypted service offered by such company, or of any plans by the U.K. government to issue such a Notice to any other U.S. tech company with respect to an encrypted service?

3. What is the Department's view on whether the U.K.'s Notice is evidence that the domestic authorities under the U.K.'s Investigatory Powers Act may be inconsistent with the statutory criteria required of the *CLOUD Act*?

4. What is the Department's view as to whether because of the U.K.'s Notice or the nontransparent nature of its issuance, the DOJ should reassess the U.K. as a qualifying foreign government for purposes of the *CLOUD Act*?

5. What is the Department's view on the imposition of extraterritorial regulations by a foreign government on U.S. providers that are contrary to U.S. law or public policy?

6. In its report to Congress accompanying the renewal of the U.S.-U.K. *CLOUD Act* Agreement in November 2024, the DOJ stated that it had "taken the opportunity of this determination to remind the U.K. of the statute's requirements that the terms of the Agreement shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data." Please share with whom the DOJ met, what specifically was communicated, and whether the DOJ considered whether the U.K.'s use of its Investigatory Powers Act might undermine U.S. interests.

7. Has the DOJ taken any steps to protect U.S. interests as contemplated by the *CLOUD Act* and the Agreement before or since the reports became public?

8. If Apple were to comply with the Notice as initially reported: (a) could the U.K. obtain U.S. person data, which would have been encrypted absent compliance with the Notice, through means other than the *CLOUD Act*, and (b) could other jurisdictions obtain data, which would have been encrypted, absent compliance with the Notice?

We appreciate your timely attention to this serious matter and welcome hearing your response by March 5, 2025.

Sincerely,

Alex Padilla
United States Senator

Zoe Lofgren
Member of Congress
Ranking Member, Committee on
Science, Space, and Technology

cc: The Honorable Marco Rubio

Secretary, U.S. Department of State