Testimony of Gregory T. Nojeim

Director, Security and Surveillance Project

Center for Democracy & Technology

before the

House Judiciary Committee
Subcommittee on Crime and Federal Government Surveillance

On

"Foreign Influence on Americans' Data Through the CLOUD Act"

June 5, 2025

CENTER FOR DEMOCRACY & TECHNOLOGY

Chairman Biggs, Ranking Member McBath, and Members of the Subcommittee:

My name is Greg Nojeim, and I direct the Security and Surveillance Project at the Center for Democracy & Technology (CDT). CDT is a nonprofit, nonpartisan organization that defends civil rights, civil liberties, and democratic values in the digital age. For nearly three decades, CDT has worked to ensure that rapid technological advances promote democracy and human rights.

We are calling on Congress and the Department of Justice (DOJ) to protect the privacy and security of Americans' data against threats to it by countries that benefit from agreements entered into under the U.S. CLOUD Act. The first country to receive the benefits of a CLOUD Act agreement — the United Kingdom — has ordered Apple, a U.S. communication service provider, to build in a backdoor to its encrypted cloud back up service to facilitate surveillance demands the UK will make of Apple under the auspices of the CLOUD Act. Such a requirement compromises the privacy and security of the communications of everyone who uses that service even if they are not located in the United Kingdom, including Americans.

Today, I will:

- Explain why Congress enacted the CLOUD Act and describe the broad scope of the surveillance demands it authorizes, what the CLOUD Act omits, and how it fails to protect encryption;
- Indicate that CLOUD Act agreements entered into so far are silent on encryption, and explain how that silence has opened the door to problematic conduct by counties that benefit from CLOUD Act agreements;
- Show how the U.S. can and should use its leverage to protect encryption in the context of existing CLOUD Act agreements, and those into which it will enter in the future; and
- Outline changes Congress could make to the CLOUD Act to protect encryption if the Department of Justice (DOJ) does not act to do so.

How the CLOUD Act Facilitates Foreign Government Surveillance

Congress enacted the CLOUD Act in 2018 by tacking it on to the end of a 2,322-page omnibus spending bill. Reduced to its essence, the CLOUD Act did two things: (1) it granted U.S. law enforcement entities new powers to compel U.S. companies to disclose communications and data on U.S. and foreign users that is stored overseas when the U.S. companies can exercise control over that data, and (2) it empowered the DOJ to — without congressional approval — enter into executive agreements with foreign countries through which U.S. providers can disclose user data, from storage and in real time, directly to foreign states under the laws of those foreign states, subject to certain requirements.

We are focused on the latter change. It was accomplished by removing the block in the Electronic Communications Privacy Act that otherwise prohibited the direct disclosure of user content to a foreign governmental entity. Before the CLOUD Act, and today in the absence of a CLOUD Act agreement, the foreign government would have to make a request under the relevant Mutual Legal Assistance Treaty (MLAT) between the foreign government and the U.S., and enlist the DOJ to apply to a federal magistrate for a warrant, based on a showing of probable cause. The MLAT system is slow, and foreign law enforcement officials need speedy responses in order to investigate crimes in their own countries, and to prevent them. Moreover, MLAT agreements do not authorize foreign governments to engage in wiretapping by obtaining access to communications in real time. This real time access was particularly important to the UK, which lobbied Congress and elements of the U.S. government to include it in the CLOUD Act.

To preserve the privacy of Americans and of everyone in the U.S., the CLOUD Act requires that surveillance orders that a foreign government issues under a CLOUD Act agreement cannot intentionally target a U.S. person or a person located in the U.S. (18 U.S.C. § 2523(b)(4)(A-B)). In theory, they would remain protected under U.S. law and the U.S. Constitution, but, as explained later, their rights can still be compromised by the conduct of countries that enjoy the benefits of a CLOUD Act agreement. The CLOUD Act imposes other requirements, including limiting disclosures to cases involving serious crimes, and barring the DOJ from entering into a CLOUD Act agreement unless the DOJ can certify that the country's laws and practices meet certain human rights standards.

The CLOUD Act requires that "the terms of [CLOUD Act agreements] shall not create any obligation that providers be capable of decrypting data [...]," (18 U.S.C. § 2523(b)(3)). But the plain text of this provision does not prevent the U.S. from entering CLOUD Act agreements with countries that impose such obligations under domestic legal authorities, as long as the relevant CLOUD Act agreement does not directly impose those obligations. CDT opposed the CLOUD Act in part because it did not sufficiently safeguard encrypted services.

So far, the U.S. has entered into two CLOUD Act agreements: one with Australia, and one with the United Kingdom (UK).[1] The UK-U.S. CLOUD Act Agreement ("Agreement") entered into force on October 3, 2022. Under its terms, the Agreement expires after five years unless renewed by an exchange of diplomatic notes, which means it is set to expire on October 3, 2027. Notably, the Agreement is silent on encryption. But that silence speaks volumes: the CLOUD Act Agreement clears the way for the UK to make surveillance demands on U.S. providers under UK law, but does nothing to ensure that the UK cannot require U.S. providers to decrypt otherwise encrypted communications and thereby compromise users' privacy and security.

[1] Negotiations have been initiated with at least two other foreign governments: Canada and the European Union. It is not apparent whether these negotiations are ongoing.

CENTER FOR DEMOCRACY & TECHNOLOGY

The UK Has Ordered Apple To Compromise Cybersecurity Worldwide

The UK's Investigatory Powers Act (IPA) of 2016, commonly known as the "Snoopers' Charter," grants sweeping surveillance authorities, including the ability to issue Technical Capability Notices (TCNs) to communication service providers. Under this provision, the UK Home Office can compel providers to make changes to their systems and services to ensure they have the ability to give effect to surveillance demands. This includes requirements to remove electronic protections like end-to-end encryption. Crucially, TCNs can be issued secretly, and can gag the provider who receives the order from disclosing its existence even to authorities in its home country. TCNs have what can best be described as "super extraterritoriality." They can be enforced extraterritorially, against companies headquartered outside the UK, requiring them to engage in conduct at their facilities outside the UK, that comprises the security of their users outside the UK, even if those users are not UK citizens or residents.

Encryption is an essential tool for combatting today's increasingly sophisticated cybersecurity threats, including those from state-sponsored hacking campaigns like the Salt Typhoon attack that targeted critical infrastructure and government agencies. Introducing a back door into end-to-end encryption means introducing systemic security flaws, as the UK knows, and back doors into encryption jeopardize all users' privacy and cybersecurity because criminals specifically look to exploit these vulnerabilities. Across the world, cybersecurity experts agree that there is no way to provide government access to end-to-end encrypted data without breaking end-to-end encryption and introducing vulnerabilities that could be exploited by anyone, not just law enforcement.

In February 2025, the Washington Post reported that the UK Home Office issued such a TCN to Apple, seeking to compel the company to introduce a back door into its end-to-end encrypted cloud storage service, "Advanced Data Protection" (ADP). This back door access would allow UK officials to require Apple to provide in decrypted form content that any user worldwide had uploaded to the cloud using ADP. Apple is the world's second largest provider of mobile devices. Compelling back door access into its encrypted cloud storage service would mean putting millions of users at risk across the globe. The most harmful impact would fall on those who rely on encryption because they have the most need for secure communications. They include journalists, lawyers, domestic violence survivors, LGBTQ+ persons, and others. More than 100 civil society organizations, cybersecurity researchers, and industry leaders signed a joint letter organized by the Global Encryption Coalition condemning the UK Home Office's use of its IPA authorities to undermine end-to-end encryption. The letter emphasized that such actions set a dangerous precedent and lead to a less secure and less free Internet for everyone.

Rather than capitulate to the demand, Apple made the principled decision to cease offering ADP in the UK, and appealed the notice to the UK Investigatory Powers Tribunal (IPT), which has the authority to review complaints related to UK surveillance. Because of amendments adopted last year, the IPA requires Apple to comply with the TCN even while an appeal is pending. As a result of this obligation and the authority the UK claims to enforce its laws on a global basis, British authorities may insist that Apple build a back door to ADP even though it no longer offers ADP in the UK.

Under the IPA, the UK Home Office has likely prohibited Apple from disclosing the existence of its demand, and Apple has not publicly acknowledged its existence despite widespread media reporting. To make matters worse, the appeal process is also shrouded in secrecy. This means the UK Home Office can place Apple, or any other service provider, under a strict gag order when it issues a TCN. The chilling result is that the public does not know which providers of other encrypted services have received such notices, and if so, which of them complied with those notices, putting user data at risk.

Apple won a significant procedural victory in April when the IPT rejected the government's attempt to keep the litigation entirely secret. According to the judgment, the Home Office argued that revealing the existence of the claim, as well as the names of the parties involved, would be damaging to national security. But the IPT disagreed, citing widespread media reporting, written interventions from civil society organizations, and a letter from members of the U.S. Congress. The judgment officially confirmed for the first time that the IPT was hearing a case brought against the Home Office by Apple over the power to issue a TCN under the IPA. However, nothing more than the bare details of the case were confirmed. The case remains ongoing.

The IPT has also confirmed that it will hear challenges from two UK-based civil society organizations, Liberty and Privacy International, related to the Home Office's alleged decision to force Apple to give the UK government access to users' private data stored on the cloud. Liberty and Privacy International are also challenging the authority of the UK government to issue TCNs at all. Though the case is ongoing and could ultimately result in a decision that protects Apple's encrypted cloud back up service, the DOJ and Congress can act to promote or to ensure that result.

What the DOJ Should Do To Protect Americans' Data Security Against Attack By Countries That Benefit From CLOUD Act Agreements

Although the UK's TCN to Apple was issued under its domestic legal authorities, and not the CLOUD Act or the UK-U.S. CLOUD Act Agreement, the Agreement effectively enables the UK to issue such orders to Apple. The Agreement allows the UK to compel U.S. providers like Apple to disclose user content directly, bypassing the traditional and bulky MLAT process and its requirement for U.S. judicial oversight. This deprives U.S.

companies like Apple the opportunity to challenge the order in U.S. courts under substantive U.S. laws that do not authorize orders like the UK's TCNs, and offers a streamlined path for foreign officials to access Americans' private data. Furthermore, the Agreement permits real-time interception, which MLATs do not allow, further incentivizing UK surveillance orders on U.S.providers.

If Apple is forced to build a back door to ADP to facilitate UK surveillance, UK officials would exploit that opportunity without meaningful transparency. The combined effect of a secret TCN, the access to data held by U.S.communications service providers that is enabled by the Agreement, and the asserted global reach of UK surveillance law would create a powerful tool for surveillance worldwide, with virtually no accountability to users, and limited accountability to the U.S. government.

If the UK insists on using secret orders to force U.S. companies to undermine encryption and thereby put at risk the data of Americans and other people around the world, the DOJ can and should terminate the Agreement or require that it be modified to prohibit orders that force providers to build a decryption capability for encrypted services. Under the terms of the Agreement, the U.S. can unilaterally terminate it without cause and with only 30 days notice. Hopefully, the threat of termination would lead the UK to accept the prohibition on decryption orders.

Terminating the Agreement would have far more severe consequences for the UK than the U.S. In November 2024, around the Thanksgiving congressional recess, the U.S. Department of Justice (DOJ) quietly recertified the Agreement, as required by the CLOUD Act.[2] It did so without fully disclosing to Congress information about the UK TCN authority and how it was likely to be exercised. The DOJ's recertification report provided several key insights about the UK's conduct under the Agreement, not least that the UK issued more than 20,000 requests to U.S. service providers over the two years in which the Agreement was in effect. The bulk of those requests included wiretapping surveillance. In comparison, the U.S. issued a mere 63 to British providers, mostly for stored data. Twenty thousand is an astounding number of wiretaps for criminal cases. In contrast, federal and state law enforcement authorities in the U.S. (which has five times the population of the UK) obtained wiretap orders in criminal cases in only 4,507 instances in the two-year period covering calendar years 2022 and 2023, the most recent years for which data is available.[3] On top of this imbalance, the

[2] The DOJ's "recertification" that a CLOUD Act agreement continues to satisfy the CLOUD Act's § 2523(e) requirements does not serve to extend the "termination" date of that agreement. Rather, the termination date is established in each individual CLOUD Act agreement. Recertification every five years after the Attorney General's original certification is required by Congress to compel the DOJ to regularly re-assess foreign countries' compliance with CLOUD Act obligations. The UK-U.S. CLOUD Act Agreement provides that it will terminate five years after October 3, 2022, the date on which it entered into force, unless terminated earlier by one of the parties with 30 days notice.

[3] Administrative Office of the U.S. Courts, Annual Wiretap Reports issued in 2023 and 2024, covering wiretaps reported in the prior year in each case. This figure combines the number of wiretap orders

DOJ admitted in its Thanksgiving-time recertification to Congress that the U.S. is not getting what it bargained for in the Agreement: a substantial reduction in the number of MLAT requests the UK has sent to the U.S. Processing those requests requires a substantial expenditure of DOJ and judicial resources to secure court orders for crimes that usually occur outside the U.S. and involve non-US person perpetrators and victims.

The dramatic imbalance in the value of the Agreement to the U.S. as compared to the UK owes to the concentration of major communications service providers in the U.S. It demonstrates the overwhelming importance of the Agreement to the UK and its relative lack of importance to the U.S. The U.S. draws some benefits from the Agreement that go beyond the numbers. To the extent the UK engages in surveillance, the product of which is used to disrupt global trade in drugs, the proliferation of nuclear weapons and other transnational crimes, the Agreement makes Americans safer. Moreover, the Agreement relieves pressure that the UK would otherwise apply to U.S. tech companies to compel them to make disclosures that are required under UK law or to store data in the UK ("data localization") to bring it within UK jurisdiction. In other countries, those pressure tactics include fining tech companies for non-compliance with surveillance orders, and arresting and imprisoning their officials until disclosures are made. Terminating the Agreement could invite such pressure tactics.

In deciding whether and how to terminate the Agreement or require that it prohibit decryption orders for encrypted services, the DOJ should weigh the effect such a step might have on the conduct of other countries that have or are seeking CLOUD Act agreements. The UK is not alone in having legal authority to compel companies to assist with surveillance. Authorities in Australia, the only other country that currently benefits from a CLOUD Act agreement, are also statutorily authorized to issue similar technical assistance and capability notices under Australia's Telecommunications and Other Legislation Amendment (TOLA) Act. Like the UK's TCN authority, TOLA allows Australian authorities to require providers to make changes to their systems to ensure access to encrypted communications. While both laws authorize secret demands to weaken encryption, there are some differences. Australia's law explicitly prohibits requiring a provider to build in a "systemic weakness" or "systemic vulnerability," though the statute fails to define these terms clearly, and critics argue the exception is too vague to be effective. The UK IPA, by contrast, imposes no such limitation. If the DOJ moves to terminate or modify the Agreement with the UK, it should consult with

issued by federal and state courts in criminal cases. Some wiretaps issued under intelligence surveillance authorities are issued primarily for criminal purposes. But, even when all of the 606 FISA wiretapping orders reported by the DOJ National Security Division for the two most recent years for which data is available are added to the criminal wiretapping orders, the UK's 20,142 orders dwarf 5113 wiretapping orders sought by federal and state authorities in the U.S. The comparison between the two countries' laws is further complicated by the fact that a small portion of the surveillance orders issued under FISA Section 702 may have been issued in circumstances in which a criminal wiretap order could have been obtained, and are not included in this comparison.

Australian authorities about their use of technical assistance and capability notices to assess whether they are being secretly used to compromise encryption.

What Congress Should Do To Protect Americans' Data Security Against Attack By Countries that Benefit from CLOUD Act Agreements

Congress should amend the CLOUD Act to prohibit agreements with countries whose laws authorize them to mandate backdoors to encryption, and it should require that CLOUD Act agreements prohibit the imposition of such backdoors on any U.S. provider.

To effectively safeguard encrypted services, Congress should amend the CLOUD Act to prohibit CLOUD Act agreements with countries whose laws or practices permit orders that compel providers to build back doors to encryption. This would cut the problem off at the source by preventing the U.S. from forming partnerships with governments that undermine encryption. While a country could later change its laws and violate this requirement, the permissive termination provisions that now appear in CLOUD Act agreements, as well as the requirement of periodic DOJ recertification, should deter such conduct.

Requiring foreign governments to change their domestic laws, particularly as applied to non-U.S. providers, is ambitious. But it is entirely consistent with the DOJ's original pitch to Congress when it proposed the bill that became the CLOUD Act. The DOJ claimed that the law would incentivize adoption of pro-privacy and civil liberties reforms in other countries by conditioning access to data held by U.S. providers on meaningful human rights protections. In fact, the UK enacted legislation specifically to enable its compliance with the CLOUD Act. Conditioning agreements on non-interference with encryption would be a natural and principled extension of that logic and would help ensure that the CLOUD Act promotes, rather than undermines, global cybersecurity norms.

At a minimum, Congress should amend the CLOUD Act to require that CLOUD Act agreements include a provision indicating that while the agreement is in force, the foreign government will not issue orders to U.S. service providers that require undermining encryption. This approach would create clear contractual guardrails, enforceable through the agreement's termination provisions. Its effectiveness would depend on political will and enforcement by the DOJ. As it stands, the UK-U.S. CLOUD Act Agreement contains no provisions addressing encryption, which is a dangerous oversight. Requiring future agreements to explicitly prohibit foreign governments from compelling communications service providers to undermine the security of the communications they carry would be a meaningful reform.

Congress Should Consider Other Amendments to the CLOUD Act

Beyond addressing back doors to encryption, Congress should consider adopting additional amendments to the CLOUD Act to better protect privacy, due process, and human rights. First, the law should be revised to require that all foreign surveillance orders issued pursuant to a CLOUD Act agreement be *authorized* by a court or by another independent tribunal. Instead, the CLOUD Act currently provides that such orders be subject to subsequent independent review or oversight after the surveillance has occurred and when damage to privacy is already done. Judicial authorization requirements are not unique to the U.S.: the Grand Chamber of the European Court for Human Rights in *Zakharov v. Russia* indicated that "the authority competent to authorise the surveillance" must be "sufficiently independent from the executive" (para. 258) to survive review under Article 8 of the European Convention on Human Rights, which protects the right to privacy.

Congress should also require a stronger factual basis for surveillance orders issued under CLOUD Act agreements. They need not meet the strong evidentiary standard that pertains in the U.S. — the probable cause requirement — which is unique. But the current evidentiary standard in the CLOUD Act is excessively weak and malleable: it provides that orders must be "... based on requirements for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation." 18 U.S.C. 2523(b)(4)(D).

To strengthen oversight and accountability, Congress should also require transparency and notice. U.S. providers who challenge orders should not be constrained by gag orders that bar them from revealing that they have received such orders, including revealing such a fact to the U.S. government. People who have been subject to surveillance under an order issued pursuant to a CLOUD Act should receive notice of such orders, which notice can be delayed if contemporaneous notice would thwart an investigation.

One might think that if these requirements were added to the CLOUD Act, that they would not protect Americans because the CLOUD Act prohibits the targeting of Americans by orders issued under a CLOUD Act agreement. But, as the members of this Subcommittee know from their work on Section 702 of the Foreign Intelligence Surveillance Act, surveillance that targets people abroad can incidentally or mistakenly pick up communications of Americans who are communicating with the foreign targets. Congress will never know how many Americans' communications were picked up in the 20,000 wiretaps the UK placed under the auspices of its CLOUD Act Agreement with the U.S., but it can be confident that stronger standards and the obligation to give notice would reduce that number.

CENTER FOR DEMOCRACY & TECHNOLOGY

The U.S. Should Get Its Own House in Order to Protect Encryption

While the UK's demand that Apple undermine end-to-end encryption is deeply concerning, it is not entirely without precedent, even in the United States. Although CDT believes that current U.S. law does not permit the government to issue an order like the one Apple received under the UK's IPA, past action by the U.S. DOJ suggests that the DOJ may have a different view.

In 2015, during the Obama administration, the DOJ sought an order under the All Writs Act to compel Apple to create a modified version of its iOS operating system that would enable the FBI to bypass built-in security protections on an iPhone used by a suspect in a shooting in San Bernardino, California. The case became a flashpoint in the national encryption debate, with Apple refusing to comply on the grounds that the order would set a dangerous precedent and weaken security for all users. Although the FBI ultimately withdrew the request after gaining access to the device through other means, the legal question was never resolved.

Whether the DOJ today, or in a future administration, would take the same position is unknown. For that reason, Congress should amend U.S. law to make clear that the All Writs Act does not authorize the government to compel a provider of a communications service or the manufacturer of a communications device to build in security vulnerabilities, or bypass privacy protections. Providers should be expected to comply with lawful data access requests only to the extent they can do so without compromising the integrity of their systems or devices, or the trust of their users.

Additionally, Congress should clarify that neither the Stored Communications Act nor the Wiretap Act can be interpreted to authorize such mandates. Both statutes include provisions that have been interpreted to require companies to help law enforcement execute surveillance orders.[4] But these provisions are vague and were written decades ago, long before the advent of end-to-end encryption, and should be updated to reflect today's cybersecurity realities. They must not be used as a back door route to impose the same kinds of obligations that Apple is currently fighting in the UK

Conclusion

The threats posed by the UK's order to Apple, and by similar powers under laws in other countries, illustrate the need to strengthen legal protections for encryption. The CLOUD

[4] *See* 18 U.S.C. § 2518(4) ("An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, [... to] furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception…. *See also* 18 U.S.C. §§ 2703, 2706 (although the Stored Communications Act does not contain an explicit technical assistance provision, its disclosure requirements and reimbursement provisions have been interpreted to require certain forms of technical assistance to help execute orders).

Act currently lacks meaningful safeguards against foreign mandates that compel U.S. companies to undermine the security of their services. Without reform, cross-border data access agreements risk becoming conduits for global surveillance demands that compromise cybersecurity and civil liberties of Americans and other users worldwide.

To address this, Congress should amend the CLOUD Act to prohibit agreements with countries whose laws or practices authorize their authorities to compel providers of communications service to weaken security measures, including encryption. At a minimum, it should ensure that CLOUD Act agreements explicitly forbid such demands. Finally, Congress should also clarify domestic law to prevent similar demands under statutes like the All Writs Act, the Stored Communications Act, or the Wiretap Act.

We appreciate the Subcommittee's attention to these critical issues and welcome the opportunity to work with you to enact legislation that protects encryption, preserves trust in U.S. technology, and upholds human rights and cybersecurity worldwide.