# UK demands create fresh tensions with Apple over encryption and cross-border data access



The UK government has taken a significant step in its ongoing effort to access encrypted iCloud backups of British users by ordering Apple to create a technical “back door” into its cloud storage service. This move, first revealed by the Financial Times, comes after a previous broader demand that sought global access, including data of American users, which met with fierce opposition from the US administration. In September, under the Investigatory Powers Act, the Home Office issued a technical capability notice (TCN) compelling Apple to provide this access, but limited the scope to UK users, aiming to address concerns raised during earlier negotiations.

The demand marks an escalation in a complex dispute over data privacy and law enforcement’s surveillance powers. Apple, steadfast in its commitment to user privacy, has consistently refused to weaken its encryption or create any master key or back door, arguing such actions expose users worldwide to increased risks from hackers and hostile actors. The tech giant withdrew its most secure cloud feature, Advanced Data Protection (ADP), from the UK market earlier this year, indicating the challenges posed by government demands. Apple expressed profound disappointment over the inability to offer these protections to UK customers, citing a rise in data breaches and threats to privacy.

While the UK Home Office has declined to confirm the exact nature of the notice, it reiterated its commitment to taking necessary actions domestically to safeguard citizens. Apple’s position remains clear: it has never built a back door or master key to any of its products or services and will not do so. However, the legal battle is set to continue, with Apple challenging the legality of these government demands in the Investigatory Powers Tribunal (IPT), supported by privacy advocacy groups such as Liberty and Privacy International.

Privacy campaigners have voiced alarm at the broader implications of the UK’s order. Caroline Wilson Palow, legal director at Privacy International, warned that undermining end-to-end encryption in the UK could have global repercussions, creating vulnerabilities exploitable by hostile states, cybercriminals, and other malicious entities. The concern is that once encryption protections are compromised—even in a single jurisdiction—the breach can be exploited internationally, weakening overall digital security.

The dispute has also had significant diplomatic implications. The initial UK push for global access, which included American data, provoked backlash from Washington, with key figures in the former Trump administration strongly opposing the demand. This opposition was so intense that it raised concerns about damaging wider UK-US trade and security relations. According to reports, Prime Minister Sir Keir Starmer brought up the issue in talks during his state visit to Washington, and though US officials initially pressured the UK to retract or scale back its demands, recent developments indicate they have eased off on this stance.

Behind the scenes, British and American officials have engaged in private discussions aimed at resolving these tensions. One sticking point has been whether the UK’s demands violate the US CLOUD Act, which limits such cross-border data requests. The issue remains under legal scrutiny, with related secret hearings scheduled in London’s High Court. Meanwhile, Apple’s removal of ADP encryption in the UK has already altered how the company handles iCloud backups, allowing Apple to technically access backups that can then be legally handed over to authorities, a change significant for privacy advocates and law enforcement alike.

This ongoing saga highlights the difficult balance governments face between enabling effective law enforcement and counterterrorism investigations and preserving robust digital privacy protections for users. Tech companies have repeatedly opposed efforts to undermine encryption because of the inherent risks to user security and privacy, while governments argue that encrypted data can shield criminals and terrorists from detection. The evolving legal and diplomatic battle between the UK and US, set against Apple’s firm stance, underscores the complexities of data governance in an increasingly connected world.

### 📌 Reference Map:

* Paragraph 1 – [[1]](https://www.cityam.com/uk-orders-apple-to-give-access-to-encrypted-icloud-backups/), [[2]](https://www.reuters.com/world/uk/uk-makes-new-attempt-access-apple-cloud-data-ft-reports-2025-10-01/), [[5]](https://www.macrumors.com/2025/02/07/uk-government-orders-access-icloud/)
* Paragraph 2 – [[1]](https://www.cityam.com/uk-orders-apple-to-give-access-to-encrypted-icloud-backups/), [[4]](https://www.macrumors.com/2025/02/21/apple-pulls-encrypted-icloud-security-feature-uk/), [[7]](https://techcrunch.com/2025/02/21/apple-pulls-icloud-end-to-end-encryption-feature-for-uk-users-after-government-demanded-backdoor/)
* Paragraph 3 – [[1]](https://www.cityam.com/uk-orders-apple-to-give-access-to-encrypted-icloud-backups/)
* Paragraph 4 – [[1]](https://www.cityam.com/uk-orders-apple-to-give-access-to-encrypted-icloud-backups/), [[7]](https://techcrunch.com/2025/02/21/apple-pulls-icloud-end-to-end-encryption-feature-for-uk-users-after-government-demanded-backdoor/)
* Paragraph 5 – [[1]](https://www.cityam.com/uk-orders-apple-to-give-access-to-encrypted-icloud-backups/), [[2]](https://www.reuters.com/world/uk/uk-makes-new-attempt-access-apple-cloud-data-ft-reports-2025-10-01/), [[6]](https://www.reuters.com/technology/uk-us-hold-private-talks-resolve-apple-encryption-order-bloomberg-news-reports-2025-03-13/)
* Paragraph 6 – [[1]](https://www.cityam.com/uk-orders-apple-to-give-access-to-encrypted-icloud-backups/), [[6]](https://www.reuters.com/technology/uk-us-hold-private-talks-resolve-apple-encryption-order-bloomberg-news-reports-2025-03-13/)
* Paragraph 7 – [[3]](https://www.cnbc.com/2025/02/07/uk-orders-apple-to-let-it-access-encrypted-accounts-washington-post.html), [[5]](https://www.macrumors.com/2025/02/07/uk-government-orders-access-icloud/)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.cityam.com/uk-orders-apple-to-give-access-to-encrypted-icloud-backups/> - Please view link - unable to able to access data
2. <https://www.reuters.com/world/uk/uk-makes-new-attempt-access-apple-cloud-data-ft-reports-2025-10-01/> - The UK government has renewed efforts to obtain access to Apple's encrypted iCloud data, focusing specifically on data belonging to UK users. This follows a previous broader mandate that included American data, which faced strong opposition from U.S. lawmakers and intelligence officials. Apple has consistently refused to create any 'back door' access into its devices or services, citing privacy and security concerns, and had appealed the initial order to the UK's Investigatory Powers Tribunal (IPT). While the UK government maintains discretion on operational matters, it reiterated its commitment to safeguarding national security. Apple has not yet issued a response to the renewed order.
3. <https://www.cnbc.com/2025/02/07/uk-orders-apple-to-let-it-access-encrypted-accounts-washington-post.html> - Britain's Home Office ordered Apple last month to create a technical 'backdoor' that would let officials view encrypted material uploaded to the cloud, the Washington Post reported Friday. Governments in the U.S., U.K. and EU have long expressed dissatisfaction with this setup, arguing it enables criminals, terrorists and sex offenders to conceal illicit activity. Tech firms — including Apple — have pushed back on attempts to undermine encryption, saying it would weaken user privacy.
4. <https://www.macrumors.com/2025/02/21/apple-pulls-encrypted-icloud-security-feature-uk/> - Apple has withdrawn its Advanced Data Protection iCloud feature from the United Kingdom following government demands for backdoor access to encrypted user data. The move comes after UK officials secretly ordered Apple to provide unrestricted access to encrypted iCloud content worldwide. Customers who are already using Advanced Data Protection, or ADP, will need to manually disable it during an unspecified grace period to keep their iCloud accounts. Apple said it will issue additional guidance in the future to affected users and that it 'does not have the ability to automatically disable it on their behalf.'
5. <https://www.macrumors.com/2025/02/07/uk-government-orders-access-icloud/> - The British government has secretly demanded that Apple give it blanket access to all encrypted user content uploaded to the cloud, reports The Washington Post. The undisclosed order is said to have been issued last month, and requires that Apple creates a back door that allows UK security officials unencumbered access to encrypted user data worldwide – an unprecedented demand not before seen in any other democratic country. The spying order came by way of a 'technical capability notice,' a document sent to Apple by the Home Secretary, ordering it to provide access under the sweeping UK Investigatory Powers Act (IPA) of 2016.
6. <https://www.reuters.com/technology/uk-us-hold-private-talks-resolve-apple-encryption-order-bloomberg-news-reports-2025-03-13/> - British officials have engaged in private discussions with U.S. officials to address concerns that the UK is pressuring Apple to build a backdoor into American encrypted data, following Apple's removal of its Advanced Data Protection encryption in the UK. This removal allows Apple to access iCloud backups, which could then be legally handed over to authorities. The matter has escalated as U.S. authorities investigate if the UK's demands violate the CLOUD Act, which prohibits demands for data from the opposing nation. A related secret hearing will take place at London's High Court. The situation reflects ongoing tensions between governments seeking data access for surveillance and crime-fighting, and tech companies prioritizing consumer privacy.
7. <https://techcrunch.com/2025/02/21/apple-pulls-icloud-end-to-end-encryption-feature-for-uk-users-after-government-demanded-backdoor/> - Apple confirmed Friday that it 'can no longer' offer a security feature that allows users in the United Kingdom to encrypt their iCloud data. In a statement provided to TechCrunch, Apple spokesperson Fred Sainz said the company’s Advanced Data Protection feature will no longer be available to new users and current U.K. users 'will eventually need to disable this security feature.' 'We are gravely disappointed that the protections provided by ADP will not be available to our customers in the U.K. given the continuing rise of data breaches and other threats to customer privacy,' the company said in a statement.