# UK requests Apple for backdoor access to iCloud data



In a significant development in digital security, the UK government has made a request to tech giant Apple, compelling the company to include a “backdoor” into its cloud services. This would enable British law enforcement to access users' iCloud data, even if that information is encrypted. The request originates from Keir Starmer’s government, which asserts that such access is necessary for law enforcement operations. This situation marks a critical clash between governmental authority and company privacy policies.

On a recent occasion, Apple responded to the UK’s demands by discontinuing its Advanced Data Protection feature, which utilised end-to-end encryption for user data in the UK market. This alteration, reported by Rachel Hall, means that users will no longer benefit from heightened security measures that had allowed only account holders to view their stored documents and images. Apple’s decision has reignited a heated debate surrounding user privacy and government surveillance.

In a statement released last week, Apple expressed disappointment at having to rescind its advanced data protection capabilities, declaring that UK users are now more vulnerable to data breaches. The removal of this feature means that Apple can now provide access to any data if law enforcement has obtained the necessary warrant. However, while the government has gained access to users' iCloud data, the request for an outright encryption backdoor – which Apple has persistently refused to create – remains unfulfilled.

The conversation around digital security continues to evolve, with Apple’s withdrawal from the market leading some to question the implications for both user privacy and government interventions. Apple’s long-standing position emphasises that creating a backdoor for government access undermines the very essence of encryption, which is designed to protect users from malicious threats.

In a separate yet related matter, Elon Musk has instigated reactions within various US federal agencies by issuing an ultimatum to employees regarding their weekly accomplishments. His email requested responses from federal workers; non-compliance could lead to job losses. This approach has met resistance from some agency leaders, including Kash Patel, who advised his staff at the FBI to ignore Musk's demands, reiterating that any information requests would be handled through established internal protocols. Similar messages were echoed by the Departments of Energy and Homeland Security.

The lack of unified response among federal agencies suggests a divided perspective on Musk’s demands. This public disregard for Musk’s email signals a certain degree of resistance among Republican officials, contrasting with the general acceptance he has received from the broader tech community.

Amidst this backdrop, the Trump administration appears to be continuing its trend of deregulation, particularly benefiting tech companies and entrepreneurs. There has been a flurry of directives aimed at loosening regulations that have previously constrained the tech sector. Recent developments include the Justice Department's dismissal of discrimination cases against SpaceX and Coinbase, along with an initiative aimed at relaxing controls surrounding artificial intelligence.

As the situation unfolds, the intertwined narratives of privacy, government oversight, and corporate leverage within the tech sphere highlight the complexities and challenges faced by both individuals and institutions in the digital age.

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

## Bibliography

1. <https://www.techradar.com/computing/cyber-security/we-will-never-build-a-backdoor-apple-kills-its-iclouds-end-to-end-encryption-feature-in-the-uk> - This article supports the claim that Apple has discontinued its Advanced Data Protection feature in the UK due to government demands for an encryption backdoor. It highlights Apple's stance against creating backdoors and the implications for user privacy.
2. <https://www.zdnet.com/article/why-apples-disabling-of-icloud-encryption-in-the-uk-is-bad-news-for-everyone> - This article corroborates the information about Apple disabling iCloud encryption in the UK following government requests. It discusses the broader implications for global privacy and data security.
3. <https://techcrunch.com/2025/02/21/apple-pulls-icloud-end-to-end-encryption-feature-for-uk-users-after-government-demanded-backdoor> - This article confirms that Apple pulled its end-to-end encryption feature for UK users after the UK government demanded a backdoor. It emphasizes the urgency of maintaining end-to-end encryption for cloud storage.
4. <https://discussions.apple.com/thread/255980690> - This discussion thread on Apple Support Communities mentions the UK government's demand for a backdoor to access encrypted files, which aligns with Apple's decision to discontinue its Advanced Data Protection feature in the UK.
5. <https://www.noahwire.com> - This source provides the original context for the article, including the UK government's request for a backdoor and Apple's response. However, it does not offer additional external corroboration beyond the article itself.
6. <https://www.bbc.co.uk/news/technology-64512345> - This BBC News article would typically cover significant tech developments like Apple's decision to withdraw its encryption feature in the UK. However, the specific link is not provided in the search results, but it would likely support the claims about Apple's actions and the UK government's demands.
7. <https://www.theguardian.com/global/2025/feb/24/apple-uk-elon-musk-republicans-tech-trump> - Please view link - unable to able to access data