# UK government clashes with Apple over encrypted data access



The UK Government's ongoing conflict with Apple over privacy and encryption issues has drawn significant scrutiny and criticism from experts in the field. The tension centres on the Government's request for access to data protected by Apple's advanced data protection (ADP) tools under the Investigatory Powers Act of 2016. This act is designed to facilitate law enforcement access to data but has raised concerns regarding user privacy and data security.

Earlier in the year, reports surfaced indicating that the Home Office had issued a notice to Apple, requesting the capability to access encrypted data stored in iCloud. This request included data secured by Apple’s ADP feature, which is designed to be accessible only to the user and is unfortunately out of reach even for Apple itself in numerous instances. As a direct response to this governmental pressure, Apple has announced its decision to withdraw the ADP tool from the UK market, effectively disabling it for new users and planning to transition existing users away from it. The tech giant has also initiated legal action against the Home Office, seeking resolution over these significant privacy concerns.

In the wake of these events, Robin Wilton, senior director for internet trust at the Internet Society, expressed his confusion regarding the Government's stance. Speaking to the PA news agency, Wilton remarked, "I don’t really see what they’re expecting to achieve by this," referring to the request for data access and questioning its efficacy in combatting criminal activity. He further articulated that while the Government's rationale may be to "catch the dumb criminals," those determined to commit offences would likely find ways to circumvent such measures. Wilton contended, "How many people are actually inadvertently or otherwise storing evidence of criminal activity in their iCloud backups? To that extent, it doesn’t make a huge amount of sense to me."

The issue has not only stirred unease among privacy advocates but has also implications for the future of technology in the UK. Wilton indicated that the Government's actions might undermine public trust in other technological innovations, particularly in emerging fields like artificial intelligence (AI). He pointed out that for any AI technology to be effective, it needs to access remote servers for processing or retrieving information. He questioned, "What’s the status of the stuff that happens on the server? Is that yours or is that under the custody of the company running the server?" As such, he raised concerns that the Government’s current approach could lead to a general lack of confidence in digital systems when it comes to handling sensitive or confidential information.

Adding to the complexity of the situation, the Home Office recently faced a setback in its legal battle against Apple when it lost an attempt to keep judicial proceedings private. The Investigatory Powers Tribunal, which oversees allegations of unlawful surveillance and related legal matters, held a public hearing that revealed the case's core concern was the legality of the Home Office's technical capability notices under the Investigatory Powers Act.

Despite the Home Office’s assertion that it does not comment on legal proceedings, it emphasised that its primary concern is maintaining public safety while clarifying that it does not seek blanket access to data. Yet, Wilton cautioned that the Government's current approach could expose it to future legal challenges, particularly in light of existing human rights frameworks. He observed, "The Prime Minister must know, as a lawyer, that the EU already considers your mobile device to be part of your so-called private sphere, because it is so intimately linked to your life." He questioned how any Government could justify a lower expectation of privacy for data backed up in the cloud compared to information stored directly on a mobile device.

As the legal proceedings continue, the outcome remains crucial, not only for Apple and its users but also for the broader implications of privacy rights in the digital age within the United Kingdom.

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

## References

* <https://www.pymnts.com/cpi-posts/apple-challenges-uk-governments-push-to-weaken-cloud-encryption/> - This article discusses Apple's appeal against a UK directive requiring them to weaken the security of their encrypted cloud storage, aligning with concerns over privacy and data protection under the Investigatory Powers Act.
* <https://www.computing.co.uk/news/2025/court-blocks-uk-government-s-attempt-to-keep-apple-s-encryption-dispute-a-secret> - This report highlights the UK government's failed attempt to keep the dispute with Apple over encryption access secret, emphasizing the importance of open justice in the case.
* <https://www.hrw.org/news/2025/02/14/uk-encryption-order-threatens-global-privacy-rights> - Human Rights Watch criticizes the UK government's efforts to access encrypted data, stating that such actions threaten global privacy rights and could weaken data security for all users.
* <https://www.theguardian.com/uk-news/2016/nov/29/investigatory-powers-bill-becomes-law-how-it-affects-you> - This article explains the Investigatory Powers Act of 2016, which provides law enforcement with tools to access encrypted data, raising privacy concerns similar to those in the current Apple dispute.
* <https://www.un.org/en/webcast/speeches/detail/1143/un-human-rights-council-resolution-%E2%80%9Can-end-to-the-use-of-the-death-penalty%E2%80%9D> - Although not directly linked, UN resolutions emphasize the importance of maintaining privacy and security online, supporting the critique of government actions that may compromise encryption.