# UK Government's clash with Apple over user privacy intensifies



The ongoing dispute between the UK Government and Apple regarding users' privacy and data encryption has generated significant attention and criticism from experts in the field. Central to this controversy is the Government's request for broader access to encrypted data stored in Apple's iCloud accounts, requiring Apple to provide a means to access such data, which is typically safeguarded by the company's advanced data protection (ADP) tool. This tool is designed to ensure that only the account holder can access their encrypted data, thereby placing it beyond even Apple's reach.

The Government’s request, submitted under the Investigatory Powers Act of 2016, has faced criticism for its perceived implications on privacy rights. Robin Wilton, senior director for internet trust at the Internet Society, articulated the concerns surrounding this stance, characterising it as “really strange” and saying it “doesn’t make sense.” Speaking to the PA news agency, he noted that he does not believe iCloud backups would serve as a significant repository for criminal activity, stating, “I don’t really see what they’re expecting to achieve by this.”

Apple, responding to the request, announced that it would cease the use of the ADP tool in the UK, effectively withdrawing the option for new users and initiating a remediation process for existing users already employing the feature. This decision was compounded by legal action taken by Apple against the Home Office.

The backlash against the Government’s intentions extends beyond privacy advocates, with concerns being raised about the broader implications for technology, including artificial intelligence (AI). Wilton commented on the trust issues that could emerge if the Government's position implies that data processed by AI could also be considered accessible. He reasoned that if the Government treats encrypted iCloud backups as subject to unrestricted access, it raises questions about the privacy of data processed on remote servers by AI systems.

Recent judicial developments have further complicated the matter. Just last week, the Home Office lost a bid to keep the legal proceedings initiated by Apple private. The Investigatory Powers Tribunal, which typically addresses issues related to unlawful intrusion and national security, held a closed hearing to discuss the case. However, a public ruling clarified that it pertains to Apple's challenge of the power to issue technical capability notices under the Investigatory Powers Act.

When contacted for a statement, the Home Office refrained from commenting on the details of the ongoing legal proceedings but maintained that its foremost priority is the safety of the public. It emphasised that the request for data access is not intended to be a blanket approach.

Wilton cautioned that the UK Government’s current position could expose it to future legal challenges, particularly under the Human Rights Act. He posited that the Government's interpretation of encrypted data in iCloud backups disregards the expectation of privacy that users have toward their personal data, a stance that he believes could undercut the trust consumers have in digital services and potentially hinder technological advancements, particularly in the field of AI.

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