OpenVoiceNews U.K.

Transparent. Unbiased. Yours.

UK Government Rethinks Encryption Order Amid US Tensions

July 21, 2025

— Categories: Politics & Government

The UK government is seeking a resolution to a high-stakes dispute with the United States over its demand that Apple build a backdoor into encrypted iCloud data, raising questions about privacy, national security, and transatlantic tech cooperation.

In January 2025, the Home Office issued Apple a technical capability notices under the Investigatory Powers Act 2016, often referred to by critics as the “Snoopers’ Charter”, requiring the company to provide a method for government access to users’ encrypted backups. Apple responded by removing its Advanced Data Protection feature from the UK market and launching a legal challenge at the Investigatory Powers Tribunal. Messaging platform WhatsApp, owned by Meta Platforms, has joined the appeal, citing concerns over user privacy and encryption standards.

The move prompted concern in Washington. US lawmakers, including Senator JD Vance, and senior intelligence officials warned that the UK’s demand could undermine privacy protections for American citizens and complicate the functioning of the US–UK Cloud Act data-sharing framework, which relies on mutual legal processes rather than unilateral access. Quiet diplomatic discussions are now reportedly under way between British and American officials, aiming to defuse the situation and restore confidence in joint cooperation on artificial intelligence, cyber security, and data governance.

British officials are said to be reconsidering the enforcement of the notice, exploring potential alternatives that would satisfy law enforcement needs without jeopardising relations with the United States or hindering the UK’s broader ambitions for digital trade. One senior official within the Department for Science, Innovation and Technology admitted that the Home Office “has its back against the wall” under growing international pressure.

Privacy campaigners, including representatives from encrypted messaging service Signal, argue that undermining end-to-end encryption

sets a dangerous precedent. Once a backdoor is introduced, they warn, it becomes a permanent vulnerability that can be exploited not only by governments, but also by cyber criminals and hostile foreign actors.

From a centre-right perspective, this standoff highlights the need for a careful balance between enabling law enforcement to tackle serious threats and protecting individual privacy rights. Regulatory powers must be proportionate and must not compromise national cyber resilience or international partnerships.

As legal and diplomatic manoeuvres continue, the outcome could set a global precedent. If the UK intends to remain at the forefront of digital innovation and security, any compromise must preserve trust in its technological standards while upholding the rule of law and national interest.