Apple ordered to open encrypted user accounts globally to UK spying

Apple has reportedly been ordered by the UK government to create a backdoor that would give security officials access to users' encrypted iCloud backups. If implemented, British security services would have access to the backups of any user worldwide, not just Brits, and Apple would not be permitted to alert users that their encryption was compromised.

The Washington Post reports that the secret order, issued last month, is based on rights given under the UK's Investigatory Powers Act of 2016, also known as the Snoopers' Charter. Officials have apparently demanded blanket access to end-to-end encrypted files uploaded by any user worldwide, rather than access to a specific account.

Apple's iCloud backups aren't encrypted by default, but the Advanced Data Protection option was added in 2022, and must be enabled manually. It uses end-to-end encryption so that not even Apple can access encrypted files. In response to the order, Apple is expected to simply stop offering Advanced Data Protection in the UK. This wouldn't meet the UK's demand for access to files shared by global users, however.

Apple has the right to appeal the notice on the basis of the cost of implementing it and whether the demand is proportionate to security requirements, but any appeal cannot delay implementation of the original order.

The UK has reportedly served Apple a document called a technical capability notice. It's a criminal offense to even

reveal that the government has made a demand. Similarly, if Apple did accede to the UK's demands then it apparently would not be allowed to warn users that its encrypted service is no longer fully secure.

"There is no reason why the UK [government] should have the authority to decide for citizens of the world whether they can avail themselves of the proven security benefits that flow from end-to-end encryption," Apple told the British parliament in March 2024 amidst a discussion of an amendment to the Investigatory Powers Act. It has previously pushed back against other UK attempts to legislate backdoors to encrypted communications.

Security services and lawmakers in the UK have consistently pushed back against end-to-end encryption services, arguing that the technology makes it easier for terrorists and child abusers to hide from law enforcement. "End-to-end encryption cannot be allowed to hamper efforts to catch perpetrators of the most serious crimes," a UK government spokesperson told *The Guardian* in 2022 after Apple first introduced end-to-end encryption.

US agencies including the FBI have expressed similar fears in the past, but have more recently begun recommending encryption as a way to counter hackers linked to China. In December 2024 the NSA and FBI joined Canada, Australia, and New Zealand's cyber security centers in recommending web traffic be "end-to-end encrypted to the maximum extent possible," in new security best practices. UK security services didn't join them.

If Apple grants the UK government access to encrypted data, it's likely that other countries, including the US and China, will see the opportunity to demand the same right. Apple will have to decide whether to comply, or remove its encryption service entirely. Other tech companies would almost certainly face similar requests next.

Google has offered encrypted Android backups by default since 2018, and Meta also offers encrypted backups for WhatsApp users. Spokespeople for both declined to comment to *The Washington Post* on whether they had received governmental requests for backdoors. Google's Ed Fernandez reiterated that the company "can't access Android end-to-end encrypted backup data, even with a legal order," while Meta pointed to a previous statement that no backdoors would be implemented.

https://www.theverge.com/news/608145/apple-uk-icloud-encrypted-backups-spying-snoopers-charter