Forbes

UK Orders Apple To Open Up Encrypted Messages Worldwide

Emma Woollacott. Feb 7, 2025,

Photo by Edward Berthelot/Getty Images
Getty Images

The U.K. government has reportedly ordered Apple to create a backdoor giving access to users' encrypted iCloud backups - including all Apple users worldwide.

According to the Washington Post, the order, issued under the U.K.'s Investigatory Powers Act, would give the security services blanket access to all users' end-to-end encrypted files, rather than those for specific accounts.

While iCloud backups aren't encrypted by default, the company added an optional Advanced Data Protection feature in 2022, adding end-to-end encryption that means that not even Apple can access the files.

The company could get round any access order by simply pulling the feature in the U.K. - leaving users there without the option of end-to-end encryption.

Legally, the notice can't be made public, and the Home Office has refused to comment; Apple has yet to respond to our questions.

Ever since the introduction of the Investigatory Powers Act in 2016, there has been deep concern about the privacy of internet users, from tech firms and campaigners alike.

Apple has been particularly vocal, given its much vaunted emphasis on user privacy. Last year, for example, the company told Parliament that "There is no reason why the UK 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."

If confirmed, the move will face fierce opposition. The measure won't, said Daniel Castro, vice president of the Information Technology and Innovation Foundation, prevent bad actors from accessing strong encryption; they'll simply buy encryption tools elsewhere instead.

"While law enforcement agencies should have the authority to compel access to specific data held by third parties in the course of legitimate investigations, demanding that companies deliberately undermine their own security features crosses

a critical red line. This is not about lawful access to data; it is about fundamentally weakening the technology that keeps internet users safe," he said.

What this order will do, however, is make commercial products less secure for ordinary consumers, businesses, and civil society. It exposes sensitive personal and corporate information to greater risk of cybercrime, data breaches, and unauthorized surveillance."

The ITIF is calling on the U.K. government to reveal the full details of its order, while urging other nations to object.

"Because the UK's order applies globally, its harmful effects will extend far beyond its borders, undermining the security of users worldwide," said Castro.

"This precedent is particularly troubling because it provides cover for authoritarian regimes seeking to justify their own efforts to circumvent encryption, often under the guise of national security but with the real aim of suppressing dissent and violating human rights."

I've been writing about technology for most of my adult life, focusing mainly on legal and regulatory issues. I write for a wide range of publications: credits include the Times, Daily Telegraph and Financial Times newspapers, as well as BBC radio and numerous technology titles. Here, I'll be covering the ways content is controlled on the internet, from censorship to online piracy and copyright. You can follow my posts by clicking the ' Follow' button under my name, or follow me on X and Bluesky.