Apple suggests iMessage and FaceTime could be withdrawn in UK over law change

Publication Date: 2023-07-20

Author: Dan Milmo

Section: Technology

Tags: Apple, Data protection, Surveillance, Home Office, Ofcom, Internet safety, news

Article URL: https://www.theguardian.com/technology/2023/jul/20/uk-surveillance-law-changes-could-force-apple-to-withdraw-security-features

Apple has said planned changes to British surveillance laws could affect iPhone users' privacy by forcing it to withdraw security features, which could ultimately lead to the closure of services such as FaceTime and iMessage in the UK. The firm has become a vocal opponent of what it views as UK government moves against online privacy, and it said last month that provisions in the forthcoming online safety bill could endanger message encryption. Apple's latest concerns centre on the Investigatory Powers Act 2016, which gives the Home Office the power to seek access to encrypted content via a technology capability notice (TCN). End-to-end encryption, which ensures only the sender and recipient of a message can see its content, is a key tech privacy feature and is a hard-fought battleground between governments and tech firms. Apple said the changes included a provision that would give the UK government oversight of security changes to its products, including regular iOS software updates. The Home Office consultation proposes "mandating" operators to notify the home secretary of changes to a service that could have a "negative impact on investigatory powers". Apple wrote in a submission to the government that such a move would in effect grant the home secretary control over security and encryption updates globally, when allied to further proposals strengthening requirements for non-UK companies to implement changes worldwide if – like Apple – they operate via a global platform. The proposals would "make the Home Office the de facto global arbiter of what level of data security and encryption are permissible", Apple wrote. Apple also expressed concern over a proposed amendment that it says would allow the government to immediately block implementation of a security feature while a TCN is being considered, instead of letting the feature continue to be used pending an appeal. In comments implying that encrypted products such as FaceTime and iMessage could ultimately be endangered in the UK, Apple said it never built a "backdoor" into its products for a government to use, and it would withdraw security features in the UK market instead. End-to-end encryption is the core security technology for FaceTime and iMessage and is viewed by Apple as an intrinsic part of those services. "Together, these provisions could be used to force a company like Apple, that would never build a backdoor, to publicly withdraw critical security features from the UK market, depriving UK users of these protections," Apple said. The company said the proposals would "result in an impossible choice between complying with a Home Office mandate to secretly install vulnerabilities into new security technologies (which Apple would never do), or to forgo development of those technologies altogether and sit on the sidelines as threats to users' data security continue to grow." Alan Woodward, a professor of cybersecurity at Surrey University who has signed an open letter warning against online safety bill proposals that could dilute encryption, said Apple's submission on the 12-week consultation represented a "stake in the ground".

He said: “If the government push on regardless then Apple will simply join the growing band of vendors that would leave the UK. British users could end up as one of the most isolated and insecure groups in the world. In that scenario, nobody wins.” On Wednesday the House of Lords approved a government amendment on the online safety bill related to scrutiny of encrypted messaging. Under the amendment, Ofcom, the communications watchdog, would have to await a report from a “skilled person” before ordering a messaging service to use “accredited technology” – which could enable the scanning of message content – for example to identify child sexual abuse material. The provision in the bill is widely seen by privacy campaigners as a means of potentially forcing platforms such as WhatsApp and Signal to break or weaken end-to-end encryption. Dr Nathalie Moreno, a partner at the UK law firm Addleshaw Goddard specialising in data protection, cybersecurity and AI, said there was “almost no information” available about how detailed the report to Ofcom would be, and whether the “skilled person” would be a political appointment or technical expert. “Once the government has been granted powers to intercept private messaging services, that’s it, there’s no going back,” she said. A spokesperson for the campaign group Index on Censorship, which had supported an amendment proposing judicial oversight of Ofcom’s powers, said the outcome was “disastrous” for the UK population’s right to privacy. The NSPCC, the children’s safety charity, has said the “shrill” debate over the online safety bill is “losing sight” of the safety rights of child sexual abuse victims. A government spokesperson said: “The Investigatory Powers Act 2016 is designed to protect the public from criminals, child sex abusers and terrorists. With strong independent oversight, the act regulates how intrusive investigatory powers by public authorities are used. “We keep all legislation under review to ensure it is as strong as it can be and this consultation is part of that process – no decisions have yet been made.”