WhatsApp could disappear from UK over privacy concerns, ministers told

Publication Date: 2023-05-08

Author: Alex Hern

Section: Technology

Tags: WhatsApp, Social media, Privacy, Human rights, Digital media, news

Article URL: https://www.theguardian.com/technology/2023/may/08/whatsapp-could-disappear-uk-over-privacy-concerns-ministers-told

The UK government risks sleepwalking into a confrontation with WhatsApp that could lead to the messaging app disappearing from Britain, ministers have been warned, with options for an amicable resolution fast running out. At the centre of the row is the online safety bill, a vast piece of legislation that will touch on almost every aspect of online life in Britain. More than four years in the making, with eight secretaries of state and five prime ministers involved in its drafting, the bill, which is progressing through the House of Lords, is more than 250 pages long. The table of contents alone spans 10 pages. The bill gives Ofcom the power to impose requirements for social networks to use technology to tackle terrorism or child sexual abuse content, with fines of up to 10% of global turnover for those services that do not comply. Companies must use “best endeavours” to develop or source technology to obey the notice. But for messaging apps that secure their user data with “end-to-end encryption” (E2EE), it is technologically impossible to read user messages without fundamentally breaking their promises to users. That, they say, is a step they will not take. “The bill provides no explicit protection for encryption,” said a coalition of providers, including the market leaders WhatsApp and Signal, in an open letter last month, “and if implemented as written, could empower Ofcom to try to force the proactive scanning of private messages on end-to-end encrypted communication services, nullifying the purpose of end-to-end encryption as a result and compromising the privacy of all users.” If push came to shove, they say, they would choose to protect the security of their non-UK users. “Ninety-eight per cent of our users are outside the UK,” WhatsApp’s chief, Will Cathcart, told the Guardian in March. “They do not want us to lower the security of the product, and just as a straightforward matter, it would be an odd choice for us to choose to lower the security of the product in a way that would affect those 98% of users.” Legislators have called on the government to take the concerns seriously. “These services, such as WhatsApp, will potentially leave the UK,” Claire Fox told the House of Lords last week. “This is not like threatening to storm off. It is not done in any kind of pique in that way. In putting enormous pressure on these platforms to scan communications, we must remember that they are global platforms. “They have a system that works for billions of people all around the world. A relatively small market such as the UK is not something for which they would compromise their billions of users around the world.” A Home Office spokesperson said: “We support strong encryption, but this cannot come at the cost of public safety. Tech companies have a moral duty to ensure they are not blinding themselves and law enforcement to the unprecedented levels of child sexual abuse on their platforms. “The online safety bill in no way represents a ban on end-to-end encryption, nor will it require services to weaken encryption. “Where it is the only effective, proportionate and necessary action available, Ofcom will be able to direct platforms to use accredited technology, or make best endeavours to develop new technology, to accurately identify child sexual abuse content, so it can be taken down and the despicable predators brought to justice.” Richard Allan, the Liberal Democrat peer who worked as Meta’s head of policy for a decade until 2019, described the government approach as one of “intentional ambiguity”. “They are careful to say that they have no intention of banning end-to-end encryption … but at the same time refuse to confirm that they could not do so under the new powers in the bill. This creates a high-stakes game of chicken, where the government think companies will give them more if they hold the threat of drastic technical orders over them. “The government’s hope is that companies will blink first in the game of chicken and give them what they want.” Allan said another scenario could be that the government comes clean and declares its intent is to limit end-to-end encryption. “It would at least allow for an orderly transition, if services choose to withdraw products from the UK market rather than operate here on these terms. It might be that there are no significant withdrawals, and the UK government could congratulate themselves on calling the companies’ bluff and getting what they want at little cost, but I doubt that this would be the case.” Backers of the bill are unimpressed with efforts to rewrite it to suit big tech, though. Damian Collins, the Conservative MP who chaired a Westminster committee scrutinising the bill, said he did not support one amendment introduced to try to protect end-to-end encryption. “I don’t think you want to give companies subjective grounds for deciding whether or not they need to comply with the duties set out in the bill.” Collins added that the bill did not attack encryption because it would only require messaging companies sharing information that they have access to – which does not include message content. However, he said authorities should be able to access the background data behind users, including data about usage of the app, contacts, location and names of user groups. If users access WhatsApp through a web browser, the service can also collect information about websites visited before and after sending messages, Collins added. This week Politico reported that the Department for Science, Innovation and Technology wanted to find a way through the row and is having talks “with anyone that wants to discuss this with us”. Last year, the chief executive of the trade association Digital Content Next, Jason Kint, flagged a US antitrust complaint that contained 2019 communications between Mark Zuckerberg and his policy chief, Nick Clegg, in which they discussed flagging the importance of privacy and end-to-end encryption as a “smokescreen” in any debate over integrating the back end of Meta’s apps. Clegg wrote: “Are you suggesting we should lead with E2EE and not interoperability? You may be right that – as a matter of political practicality – the latter is easier to block/hinder than the former.” He added that it was “very easy to explain” why E2EE is helpful to users whereas integrating the interoperability of apps looks like “a play for our benefit, not necessarily users”.