Meta encryption plan will let child abusers ‘hide in the dark’, says UK campaign

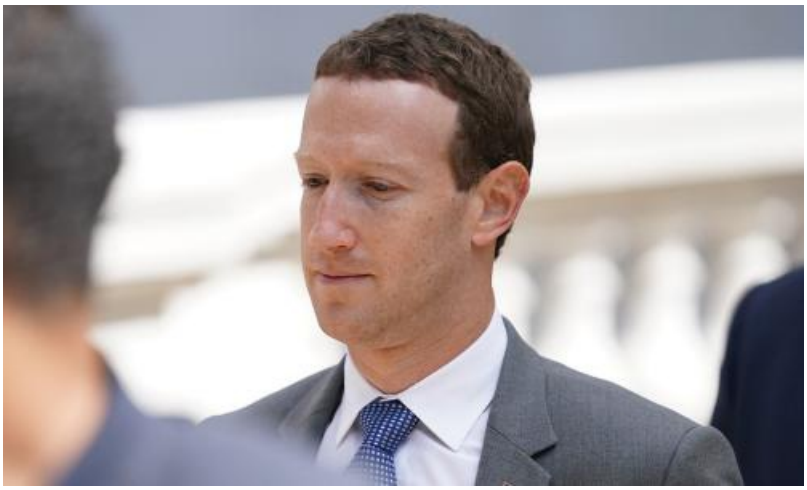
Publication Date: 2023-09-20

Author: Dan Milmo

Section: Technology

Tags: Meta, Facebook, Child protection, Encryption, Mark Zuckerberg, Home Office, Children, news

Article URL: https://www.theguardian.com/technology/2023/sep/20/meta-encryption-plan-will-let-child-abusers-hide-in-the-dark-says-uk-campaign



Mark Zuckerberg’s plan to roll out encrypted messaging on his platforms will let child abusers “hide in the dark”, according to a government campaign urging the tech billionaire to halt the move. The Facebook founder has been under pressure from ministers over plans to automatically encrypt communications on his Messenger service later this year, with Instagram expected to follow soon after. On Wednesday the Home Office launched a new campaign, including a statement from an abuse survivor, urging Zuckerberg’s Meta to halt its plans until it has safety plans in place to detect child abuse activity within encrypted messages. A video to be distributed on social media features a message from one survivor, Rhiannon-Faye McDonald, who addresses her concerns to Mark Zuckerberg. “Your plans will let abusers hide in the dark,” she says as she urges the Meta CEO to “take responsibility”. McDonald, 33, was groomed online and sexually abused at the age of 13, although she did not encounter her abuser on Meta platforms. The campaign was launched a day after the online safety bill, which privacy campaigners fear could undermine encryption, completed its passage through parliament. The National Crime Agency, which fights serious and organised crime, estimates that encrypting Messenger and Instagram messages will lead to sharp reductions in abuse referrals to the National Center for Missing and Exploited Children (NCMEC), a US-based organisation that processes reports of online sexual child exploitation from US tech platforms, with 90% of those occurring outside the US. Suella Braverman, the home secretary, said Meta had not provided sufficient assurances on child safety in meetings about its plans for end-to-end encryption, a privacy-friendly technology that means only the sender and recipient of a message can see it. Meta also owns WhatsApp, an encrypted messaging service. “Meta has failed to provide assurances that they will keep their platforms safe from sickening abusers,” she said. “They must develop appropriate safeguards to sit alongside their plans for end-to-end encryption. I have been clear time and time again, I am not willing to compromise on child safety.” The government and child safety campaigners are concerned that end-to-end encryption will enable abusers to evade detection when grooming children and receiving and sending images of sexual abuse. A Meta spokesperson said encryption keeps the UK population “safe from hackers, fraudsters and criminals”. “We don’t think people want us reading their private messages so we have spent the last five years developing robust safety measures to prevent, detect and combat abuse while maintaining online security.” Meta also published an updated report on safety measures for Messenger and Instagram direct messages, pointing to safeguards such as restricting over-19s from messaging teens who do not follow them and using artificial intelligence systems to spot suspicious activity. “As we roll out end-to-end encryption, we expect to continue providing more reports to law enforcement than our peers due to our industry

leading work on keeping people safe," the spokesperson added. Meta said last month that it was "on track" to make end-to-end encryption a default setting for one-to-one friends and family chats on Messenger by the end of 2023. The Verge, a tech news site, also reported in August that Instagram would soon follow Messenger with encryption of its direct messages. Meanwhile, the online safety bill completed its passage through parliament on Tuesday after it was approved by the House of Lords. It will officially become law when it receives royal assent. The bill contains a controversial provision on combating child sexual abuse material [CSAM], which empowers the communications watchdog, Ofcom, to order a messaging service to use "accredited technology" to look for and take down such content. Privacy campaigners and tech firms have warned that the clause poses a fundamental threat to encryption because it could require the scanning of private messages. The government has attempted to clarify use of the new powers, stating that Ofcom would only be able to intervene if scanning content was "technically feasible" and if the process met minimum standards of privacy and accuracy.