# TechScape: Will Meta’s encryption plans be a ‘devastating blow’ to child safety online?

Publication Date: 2023-12-12

Author: Josh Taylor

Section: Technology

Tags: Meta, TechScape newsletter, Facebook, Instagram, Online abuse, Social networking, Internet, Internet safety, features

Article URL: https://www.theguardian.com/technology/2023/dec/12/techscape-how-will-meta-end-to-end-encryption-impact-online-safety-for-children

There was a rare utterance from an internet regulator last month: praise for Facebook and Instagram’s parent company, Meta. Australia’s e-safety commissioner, Julie Inman Grant, described Meta as “one of the better detection performers” for reporting child sexual abuse material on its services, making around 27m reports to the National Center for Missing and Exploited Children (NCMEC) last year. Apple, for comparison, reported just 234. To date, Meta has been able to report this material by analysing the images being shared over Messenger against databases of known child abuse material. The company had access to what was being shared, because Messenger chats are not end-to-end encrypted (e2ee). But this is about to change, though, and child safety groups are warning that encryption will impact online safety for children. Last week, Meta announced that it will enable end-to-end encryption by default on Messenger. The NCMEC said this would make communications on the platform go dark, and will be a “devastating blow” to child protection. The child safety groups and regulators have pleaded with the tech company to put the encryption project on hold until it can detect material being shared. For Meta, though, the change is inevitable. Messenger is an outlier when it comes to one-to-one communications as more and more are encrypted. Then there’s a cybersecurity risk for existing Messenger communications, which have not been stored via end-to-end encryption. Those too will be encrypted over the coming months as part of the change. Last week, when announcing the changes, the company pointed to its September paper outlining how it will detect and take down material showing child abuse on its services even without being able to see the content of the messages. Treating everything like spam Once e2ee is rolled out, the company said it will “continue to disrupt harm related to Messenger and Instagram DMs using similar technology to that used to detect spam and scams”. Once users have reported a conversation to Meta, the company will then be able to read the messages in question. Meta said: “Our systems are designed to identify suspicious behaviour, then restrict account features to make it harder for those users to find and contact people they don’t know, including children, thereby disrupting potential harm before it happens.” Meta also said it uses machine learning to detect patterns of behaviour and stop predator accounts before they can contact children or share content. The company said bad actors often reveal their intentions with obvious public signals, including child-sexualised content, coded language in bios or joining questionable groups. “Much like email spam filters, analysing behavioural signals in a private space with privacy-preserving techniques provides opportunities to detect bad actors connecting with one another, and most importantly, to detect when they may be targeting victims,” the company said. It also has limits on who can message children, profiles are private by default, and

there are limits to the search teen profiles outside Facebook. It's difficult to imagine regulators will take much comfort in these features, however, when the immediate result of e2ee is likely to be a substantial drop in reports. And it's not yet clear if such preventative steps can be measured. Are regulators ready for a fight? Whether online safety regulators are willing or able to put up a fight is another thing. The UK already backed down in a fight over end-to-end encryption with Apple this year after the company threatened to withdraw iMessage. This week, the company was also encouraging users to go further and harden the encryption on their iCloud data. In Australia, in an apparent acknowledgment of the UK fight, the e-safety commissioner's draft standard released in November would only require companies such as Apple and Meta to do what is "technically feasible" and would not compromise encryption. This would include clear and identifiable user reporting mechanisms as well as the capacity to detect patterns in the behaviour of users; Meta is doing both. Cash is king Australia's coins are in the process of being updated with the portrait of King Charles. In addition to how antiquated it can feel for a foreign monarch to be put on our currency, it is difficult to recall the last time many of us paid for anything in cash. Australians are early adopters for tech like tap-to-pay and phone payments, which were turbocharged by the pandemic. Cash payments are now very low – 13% of all transactions, compared to 27% pre-pandemic. And while there's been no talk of doing away with cash, look to the comments on X and you can easily find someone worried that the government is about to outlaw cash, leading some people to stockpile notes and coins. A couple of recent incidents have made me think some of these people are right to do so. In November, one-third of Australia's communications went offline for 14 hours due to an outage of the country's second-largest telecommunications companies, Optus. Payment systems for many retailers were unavailable, and cash was suddenly king again. If people had it. Even if you do have money in the bank, accessing it depends on you being able to see the money in the bank's app or at the ATM – if the bank has connectivity – and then to withdraw cash. If we can't depend on our systems having 100% availability, there needs to be manual options. During the cost of living crisis, there has also been the dystopian news that banks are scouring customer transactions and using a "credit risk algorithm" to determine whether their spending habits are changing and putting them at risk for loan default. There's also the brewing fight between the banks, retailers, Apple and Google over ticket-clipping fees for transactions through payment apps adding to the overall cost of using digital payments. It's enough to send you packing for the ATM. If you want to read the complete version of the newsletter please subscribe to receive TechScape in your inbox every Tuesday.