

FBI and others urge Meta to halt encryption plans, citing child abuse risk

Getty Images | Olemedia

reader comments

114 with

Share this story

The long-running battle over encryption between tech companies and law enforcement continues, with law enforcement agencies around the world calling on Meta to cancel plans for end-to-end encryption of Facebook and Instagram messages.

End-to-end encryption (often called “E2EE”) boosts security and privacy for all users, whether law-abiding or not. But government officials have long opposed plans to make the technology more widely available, citing the risk that terrorists, sex traffickers, child abusers, and other criminals will use encrypted messages to evade law enforcement.

The latest call to abandon encryption plans was made today by the Virtual Global Taskforce, a consortium of 15 law enforcement agencies, including two from the US: the FBI and ICE Homeland Security Investigations. The task force focuses specifically on child sexual abuse; other members include Europol and agencies from the UK, Canada, Colombia, Australia, New Zealand, Kenya, the Philippines, the United Arab Emirates, the Netherlands, and South Korea.

“The announced implementation of E2EE on Meta platforms Instagram and Facebook is an example of a purposeful design choice that degrades safety systems and weakens the ability to keep child users safe,” the global task force said in a statement on the UK National Crime Agency’s website.

“Meta is currently the leading reporter of detected child sexual abuse to NCMEC,” the task force said, referring to the US-based National Center for Missing & Exploited Children. Meta hasn’t provided any indication “that any new safety systems implemented post-E2EE will effectively match or improve their current detection methods,” according to the group.

“The abuse will not stop just because companies decide to stop looking,” the group also said, accusing Meta and other tech companies of “blindfolding themselves to child sexual abuse.”

End-to-end encryption is available in Facebook Messenger and Instagram as an option, but the law enforcement statement was likely spurred by Meta’s plan to turn the security feature on by default in Facebook Messenger sometime this year. The Meta-owned WhatsApp already has end-to-end encryption enabled by default.

Advertisement

Meta: People don’t want us reading private messages

When contacted by Ars, Meta provided a statement in response to the Virtual Global Taskforce:

Most Americans already rely on apps that use encryption to safely transfer money, talk to doctors, and communicate privately. We don’t think people want us reading their private messages, so have developed safety measures that prevent, detect and allow us to take action against this

heinous abuse, while maintaining online privacy and security. As we continue to roll out our end-to-end encryption plans, we remain committed to working with law enforcement and child safety experts to ensure that our platforms are safe for young people.

A Meta spokesperson said the company's plan to make end-to-end encryption the default in Facebook Messenger is still on track to be completed this year. "End-to-end encryption is already optional on Messenger. Our plan is to fully roll it out, and make it default for Messenger users, sometime in 2023. We provide regular updates on our progress," Meta said. The plan for default end-to-end encryption applies to Instagram messages, too, but the Instagram rollout may not happen in 2023, the spokesperson said.

Apple has had long-running disputes with the US government over encryption, and Facebook has faced a steady drumbeat of calls to remove encryption the past few years. "Since about 2018 the main narrative of law-enforcement and intelligence agencies has been that the end-to-end cryptography in messenger products such as WhatsApp makes life too easy for sexual predators, while the introduction of end-to-end encryption in Facebook Messenger is now claimed to pose an additional risk to children," said a 2022 paper by Ross Anderson, a security expert and professor at the University of Cambridge.

<https://arstechnica.com/?p=1933073>