

Twitter launches encrypted private messages despite new law banning it

/ [News](#) / By [Claudia Cookson](#) / May 16, 2023

The Online Safety Bill will outlaw end-to-end encryption



Twitter has launched an encrypted messaging service, enabling select users to communicate more securely.

Many users of the platform have long called for its direct messages to be made more secure.

However, the timing has drawn attention, given that in the UK, the Online Safety Bill, which will effectively outlaw end-to-end encryption, is currently working its way through Parliament.

End-to-end encryption means that private messages can only be read by the sender and the recipient, not even the third party like Twitter can access them.

Twitter's chief executive Elon Musk said it meant he could not see users' messages "even if there was a gun to my head".

The landmark legislation promises "to make the UK the safest place in the world to be online while defending free expression".

But WhatsApp, Signal and other messaging services have urged the government to rethink the bill. In March, WhatsApp's chief, Will Cathcart, said the app would leave the UK rather than abide by a requirement to weaken encryption.

Because encryption means apps cannot read messages sent over its service, they can't comply with law enforcement requests to hand over messages, or requests to actively monitor communications for child protection or anti-terror purposes.

Child safety campaigners argue that without this requirement child abuse will never really be policed.

However, critics say the law creates a 'back door' for rogue nation states, terrorists, and criminals to take advantage.

The encrypted messages is only accessible for people who pay for Twitter Blue or are affiliated to a verified Twitter account.

Warning that the new service is an early version, Musk said people should "try it, but don't trust it yet".

At the moment, users can only send text and links but not media in the messages.

Twitter said it was "not quite there yet" with encryption. A post on its support site stated: "While messages themselves are encrypted, metadata (recipient, creation time, etc) are not, and neither is any linked content.

"If someone – for example, a malicious insider, or Twitter itself as a result of a compulsory legal process – were to compromise an encrypted conversation, neither the sender or receiver would know."
