Should end-to-end encrypted messages be surveilled?

Encryption is a method of scrambling data in such a way that the intended recipient and only the intended recipient can decipher it. End-to-end encryption is encrypted communication between the sender and receiver. In some messaging apps there is a server which is responsible for the storage of messages and the relaying of messages between users. In end-to-end encryption the server is unable to read users' messages.

End-to-end encryption use for messaging poses a problem for law enforcement as it prevents law enforcement agencies from accessing messages to use as evidence for prosecuting crimes or preventing them. One piece of proposed legislation, the EARN IT Act, incentivized the removal of end-to-end encryption by making companies liable for everything on their platforms whether they can see it or not. This would encourage companies to stop providing end-to-end encryption. The potential loss of end-to-end encryption caused the public to speak up against the legislation. Thus far the EARN IT Act has been introduced but not passed.

Even though end-to-end encryption does make it harder in some cases to prosecute criminals, we should still support the protection of end-to-end encryption because any form of surveillance or backdoor would violate the human right to privacy and fundamentally weaken security, allowing criminals to read sensitive messages and exploit people's information. The only thing that keeps end-to-end encrypted messages private is the fact that they are end-to-end encrypted. If there was a key that could decrypt end-to-end encrypted messages and it was found by someone, that would make it possible for that person to access encrypted messages, allowing people's data to be leaked. This would not only violate the human right to privacy but also could cause more criminal activity.There are around 3 billion users of end-to-end encrypted messaging apps, such as WhatsApp and iMessage. All of these users' personal communications could be in danger of being leaked if there was a master key to decrypt communications.

In response to the concern about incentivizing the removal of end-to-end encryption, Congress added to the proposed legislation that encryption on its own would not be illegal. However, the legislation still allowed for client-side scanning. Client-side scanning is a process where the data of a message gets scanned for content of a certain type before it gets encrypted. Client-side scanning consists of scanning content before it gets encrypted for anything in a known database of objectionable content. If the message data matches a pattern in the data from this database then the algorithm notifies law enforcement and other relevant parties of this and blocks it from being sent. Some implementations have the scanning of user messages occur locally on the user's device and others have it happen on a server.

While client-side scanning sounds like a good idea because it would report and remove objectionable content without need for human intervention, client-side scanning introduces many possible points of attack from bad actors. Someone with the power to modify the database would have the ability to know when certain types of content are being shared, allowing them to get information that could be used for criminal purposes. These bad actors could also block communication between people, organizations, and agencies.

A study was done on the effectiveness of client-side scanning. It found that if an assumed 7.5 billion messages were sent a day, there were low rates of false positives. However, there were still millions of regular messages that could be identified as objectionable. This could interfere with users' communication and distract law enforcement from real criminals. Even though client-side scanning does not decrypt user messages, it still interferes with the protections offered by end-to-end encryption. It is important not to interfere with these protections.

In conclusion, while end-to-end encryption could make it harder to prosecute and prevent crimes in some cases, it still should be used as it protects the fundamental human right to privacy and keeps user messages secure from bad actors.

Gideon

Citations

Cross, Allison. “Save End-to-End Encryption in the U.S. - Internet Society.” *Internet Society*, 18 July 2023, www.internetsociety.org/blog/2023/06/speak-out-against-bills-that-threaten-end-to-end-encryption.

“A Deep Dive on End-to-End Encryption: How Do Public Key Encryption Systems Work?” *Surveillance Self-Defense*, ssd.eff.org/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work.

EARN IT Act of 2023. www.congress.gov/bill/118th-congress/senate-bill/1207/all-actions.

“Four Ways the EARN IT Act Protects Kids Online.” *IJM USA*, www.ijm.org/news/four-ways-earn-it-act-protects-kids-online.

Imessage Statistics Statistics: Market Data Report 2024. worldmetrics.org/imessage-statistics.

Internet Society. “Fact Sheet: Client-Side Scanning - Internet Society.” *Internet Society*, 26 Apr. 2024, www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning.

Kaspersky. “Digital fingerprint.” *Kaspersky*, 8 Dec. 2023, encyclopedia.kaspersky.com/glossary/fingerprint.

McKinney, India. “Dangerous EARN IT Bill Advances Out of Committee, but Several.” *Electronic Frontier Foundation*, 10 May 2023, www.eff.org/deeplinks/2023/05/dangerous-earn-it-bill-advances-out-committee-several-senators-offer-objections.

Scheffler, Sarah, and Jonathan Mayer. *SoK: Content Moderation for End-to-End Encryption*. 7 Mar. 2023, arxiv.org/pdf/2303.03979.

Team, Backlinko. “WhatsApp User Statistics 2024: How Many People Use WhatsApp?” *Backlinko*, 3 Sept. 2024, backlinko.com/whatsapp-users.

United Nations. *Universal Declaration of Human Rights*. www.un.org/en/about-us/universal-declaration-of-human-rights.