Meta

1 Hacker Way
Menlo Park, CA 94025
United States

August 3, 2023

Evan Greer
Fight for the Future
PO Box 55071 #95005
Boston, MA 02205

Dear Evan,

I'm writing to express Meta's appreciation for the focus that you and Fight for the Future have had on advocating for end-to-end encryption, including the advocacy campaign you've been leading globally. In light of your focus on this important issue, I wanted to share an update on our progress introducing end-to-end encryption for private conversations on Messenger and Instagram. I also wanted to explain why this is an important issue for Meta, as well as explain our broader commitments to protect individual privacy.

We remain committed to rolling our default end-to-end encryption for private conversations on Messenger in 2023, and shortly afterwards for Instagram. At the moment, we are in the testing phase, and some people will see that some of their Messenger and Instagram chats are being upgraded with the extra layer of protection provided by end-to-end encryption. We notify people in these individual chat threads as they are upgraded. This is a random process, so that there isn't a negative impact on our infrastructure and people's chat experience, ensuring our new end-to-end encrypted threads continue to give people the fast, reliable and rich experience on Messenger. However, the testing phase has ended up being longer than we anticipated for two reasons. First, it requires complex engineering work to transition messages onto servers which can deliver end-to-end encrypted traffic. Second, we have had to rebuild product features and safety tools to work with end-to-end encryption.

Building a secure and resilient end-to-end encrypted service for the billions of messages that are sent on Messenger every day requires careful testing. We'll provide updates as we continue to make progress towards this goal over the course of 2023.

More broadly, I wanted to reiterate that Meta is committed to providing the ability for people to communicate privately with their friends and loved ones where they have confidence that no one else can see into their conversations. People expect technology companies to provide the best security to protect their personal information, and we believe end-to-end is an important component of building trust with our users because it:

- Promotes a fundamental right to privacy, which allows loved ones to communicate without fear.
- Helps prevent both serious and common crimes like hacking and identity theft.
- Enables journalists, civil society, religious groups, scholars, and artists to exercise their rights to free and private speech without surveillance or retaliation.

End-to-end encryption is the best technology we have today to protect people's messages, and we also see it as an important reason why people might choose to use our products over competitors'. In fact, globally, the growth of chat platforms that offer end-to-end encryption - by default or as an option - outpace those that don't. And this is taking place within an equally significant broader trend: close to 90% of all web traffic is now encrypted, compared to just 53% in 2016.

We have been working for years to protect people's data on our platforms and to implement strong privacy controls over user data, and we provide what we believe to be industry-leading transparency about these efforts. This work includes providing users with options to keep their personal conversations private with end-to-end encryption on certain messaging products, removal of our Location History feature on Facebook, and providing users with numerous tools to help them review, understand, and control the information that we collect from and about them.

I appreciate your concern regarding the speed of the introduction of end-to-end encryption, but I wanted to reaffirm our commitment to doing this. We will keep you informed on our progress.

Best wishes,

Rob Sherman
VP, Deputy Chief Privacy Officer, Policy