# Do we need end-to-end encryption in messaging applications?

WhatsApp is the most common messaging application all over the world; we use it for chats, group chats, voice calls, video calls, images, videos, stories, and even money transfer. Two years ago, I saw a pop up on my WhatsApp notifying me that my interactions would be end-to-end encrypted. It made no sense back then but now I will use this essay to explore how this encryption is done, its social benefits, and why the government was against it.

In WhatsApp, users have private keys that the servers do not have access to. When a sender sends a message, the message is encrypted using the sender's private encryption key and a public key that both parties and all users have access to, only the receiver is able to decrypt the message using their private key. This ensures that no outsiders, including WhatsApp servers have access to information shared.

One of the main social benefits of the security offered in end-to-end encryption is independence from oppressive regimes. Oppressive regimes could be anything from your government to your guardians to your school. According to Privacillia (2000), privacy helps maintain individuality. When an individual knows they are being watched, they tend to act differently to appeal to the viewer. Exercising control over how much personal information is available to the public is a concern many have and is one of the main reasons why the internet is popular; one can be anonymous and express themselves freely. This benefit, however, comes at a cost.

The government was wary of end-to-end encryption in social applications because it would no longer have access to information that could be important. In the 2017 Westminister terror attack, it emerged that the attacker had mentioned the attack on WhatsApp. Since WhatsApp switched to end-to-end encryption in 2016, no one would have been able to intercept the communication between the attackers. Similarly, the anonymity afforded without end-to-end encryption could be detrimental if citizens used it for activities such as bullying.

In conclusion, we can see that there is a tradeoff between individual privacy and group security, but most applications are prioritizing individual privacy.

References:

Understanding Amy Boyer's Law: Social Security Numbers, Crime Control, and Privacy. (2000, November). Retrieved from http://www.privacilla.org/releases/AmyBoyer.pdf

Essay on Individual Privacy vs National Security. (n.d.). Retrieved from https://www.bartleby.com/essay/Individual-Privacy-vs-National-Security-P3CW8SZNBJ

Encrypted Messaging – What Is It, Why Should You Use It and What Are the Best Apps? (n.d.). Retrieved from https://pixelprivacy.com/resources/encrypted-messaging/

Kim Sengupta Defence Editor. (2017, April 28). The final WhatsApp message sent by Westminster attacker Khalid Masood has been released by security agencies. Retrieved from https://www.independent.co.uk/news/uk/crime/last-message-left-by-westminster-attacker-khalid-masood-uncovered-by-security-agencies-a7706561.html