Amnesty International has ranked Facebook’s messaging apps – Whatsapp and Messenger – the most secure in terms of protected communication. Both apps have not been ranked individually, however, and rather the ranking has been done on a collective basis combining 2 billion users of both messaging apps – hence declaring Facebook at the top as a whole.

This is where the mobile app security ranking may not be considered very accurate by some analysts because of the fact that both apps have a different approach when it comes to security. Whatsapp uses end-to-end encryption as default and in case where a chat is not secured by end-to-end encryption it clearly warns the user. Messenger, on the other hand, does not apply end-to-end encryption as default and never warns its users that normal Messenger conversations are less secure unless end-to-end encryption is enabled.

Whatsapp works on Signal Protocol developed by an open-source private messaging system – Open Whisper System, endorsed by Edward Snowden. Amnesty International encourages the existence of secure communications system because they believe it can allow journalists and activists to securely communicate while working in countries where the nature of their work can put them in danger.

Moreover, in early 2016 Whatsapp had announced that it would share its data with Facebook. This statement has been brought under investigation by an EU Competition Commissioner, since at the time Facebook was acquiring Whatsapp in 2014, it assured that no data would be shared.

In addition to that, Electronic Frontier Foundation has also stipulated users from using Whatsapp for three reasons. Firstly, messages that are backed up on cloud cannot be encrypted; hence users that require encryption must select the option of never backing up the messages. Secondly, if a message recipient alters their encryption key, Whatsapp does not notify you and hides this fact by default. Lastly, the desktop version of Whatsapp is less secure than a web extension of Whatsapp.

Messenger, on the other hand, has been introducing new features like location sharing, peer-to-peer payments and voice calls ever since it was introduced as an app. Not only did it leave no other option with facebook users but to download the app in order to read the messages, it has also not kept itself at pace with Whatsapp in terms of security features. The end-to-end encryption, known as “secret conversations” was introduced this October with a Facebook update, but users did not get any alerts.

Facebook, with a score of 73, managed to achieve the highest position for the mobile app security for its messaging apps amongst competitors. But Telegram, and Apple’s iMessage and Facetime that came to a close second position with a score of 67 also deserve praise for their encryption and transparent rules for government data requests. Apple not only provides default end-to-end encryption, it also refused working with FBI in San Bernardino shooting case. Their argument was that a backdoor creation to encrypted information will globally put the devices of Apple users at risk. However, the only feature that Apple lacks is that it does not notify its users when messages are not protected by end-to-end encryption.

Telegram with its considerably low number of users in comparison with Whatsapp, was developed specifically for promotion and protection of privacy. However, Amnesty argues that end-to-end encryption is not set as default and there is no warning to users when they are communicating under weaker encryption.

Amnesty International has called for all messaging apps to improve mobile app security and set up default end-to-end encryption in order to be transparent to their users about the security level of their communications.