Becoming more like WhatsApp won't solve Facebook's woes – here's why

March 13 2019, by Ariadna Matamoros-Fernández, Amelia Johns And Emma Baulch

Although WhatsApp is described as en encrypted messaging service, it’s not as secure as you might think. Credit: rachit tank / unsplash, CC BY

Facebook CEO Mark Zuckerberg declared last week that the company would shift away from open networks that embody "the town square" towards private, encrypted services that are more like "the digital equivalent of the living room".

The announcement comes in response to numerous privacy scandals, which have often involved third party apps accessing information about millions of Facebook users for financial and political gain.

Zuckerberg aims to make private messages private and ephemeral – meaning Facebook can't read our messages, and the data doesn't stick around on the company's servers for longer than necessary. His vision involves merging Facebook and the company's other digital platforms – Instagram, WhatsApp, and Messenger – into a super app, similar to China's WeChat.

But will these changes actually make Facebook better? Our research on the encrypted messaging platform WhatsApp suggests end-to end encrypted services pose important challenges.

WhatsApp: a 'digital living room'

Facebook acquired the instant messaging service WhatsApp in 2014. It began rolling out end-to-end encrypted messaging on the service in the same year. In theory, that means messages sent via the platform are completely private. No one aside from the sender and receiver is supposed to be able to read them – not even WhatsApp (the platform) itself.

While there has been some take up of WhatsApp in countries such as Australia and the US, it's much more popular in countries such as India, Brazil, Malaysia, and South-Africa, where it has become the preferred messaging app.

WhatsApp has also become popular among activists and whistleblowers confronting authoritarian state power in China, Malaysia, and Latin America, where surveillance of political organising on open platforms has put activists advocating for social change in danger. Our research (to

be published in a November 2019 special issue of the internet journal First Monday) shows WhatsApp has played a key role in resistance to state control in Spain, Malaysia and Indonesia.

Despite these positives, we believe becoming more like WhatsApp isn't a magic bullet solution to Facebook's privacy and other concerns. Why? Here are three reasons.

1. Encryption only creates the illusion of privacy

Since encryption minimises the ability of third parties to "read" the content of messages, it does go some way towards enhancing privacy. But encryption alone doesn't necessarily make WhatsApp a secure service, neither does it prevent third parties from accessing chat histories altogether.

In an article for the Electronic Frontier Foundation, technology experts Bill Budington and Gennie Gebhart stress that while encryption may well work to protect chat messages, it doesn't make communication on WhatsApp safer if we take a more holistic approach to the app. They argue WhatsApp "surrounding functionalities" are the threat to privacy: for example, chat history backups are stored unencrypted to the cloud, and WhatsApp web interface can easily be hacked.

In a similar vein, blogger and developer Gregorio Zanon says Facebook "could potentially" access WhatsApp chat history because of the way operating systems work on smartphones. Zanon argues that in order for us to do everyday tasks with our phones, from editing a picture to pushing content to Apple Watch, operating systems such as Apple iOS decrypt WhatsApp files and messages stored in our phones.

In his own words: "Messages are encrypted when you send them, yes. But the database that stores your chats on your iPhone does not benefit

from an extra layer of encryption. It is protected by standard iOS data protection, which decrypts files on the fly when needed."

2. Metadata means there's always a digital trail

Zuckerberg claims Facebook could limit the amount of time it stores messages. But media scholars argue it is not the content of messages itself that enables profiles to be built of users for the purposes of targeting advertising, it's the metadata. This is a key privacy concern.

Metadata includes users' contacts information and details about messages, such as the time they are sent and the identities and locations of senders and receivers, information that WhatsApp can share with the backing of the legal system.

For example, researchers have shown that WhatsApp caches popular media files. This allows the company to track forwarded media files reported as problematic, and potentially identify the source without breaking encryption.

Crucial questions around metadata and potential data breaches become even more concerning when considered in light of Facebook's plan to enable data to be shared across platforms (Facebook, WhatsApp, Instagram, Messenger). There are concerns this may make data less, rather than more, secure.

The proposal is likely to face stiff opposition in Europe, given that the EU's data protection regulator, the Data Protection Commission (DPC) has previously raised concerns around security at Facebook's plans to integrate services.

3. Encrypted messages can't be moderated

In his latest manifesto, Zuckerberg avoids addressing Facebook's other great problem beyond privacy: content moderation.

Zuckerberg acknowledges in his long Facebook post that a problem with encryption is that bad actors can exploit it to do bad things, such as "child exploitation, terrorism and extortion".

But what might end-to-end encryption mean for the spread of fake news and misinformation? Recent scholarship on Indonesia and Brazil has shown that WhatsApp has become a safe haven for producers of fake news, who can't be easily traced on encrypted services.

To deal with this problem, WhatsApp has limited the number of times messages can be forwarded in countries like India and Myanmar, where WhatsApp hoaxes have led to violence.

A more private, end-to-end encrypted system would partially free Facebook from the burdens involved in having to moderate this kind of content. This is a task the company has been reluctant to pursue, but it has been forced to do it due to its pivotal role as the contemporary "town square".

Although the app is used to discuss public issues through public groups of up to 256 people, there is no specific tool on WhatsApp that allows users to flag problematic content.

Questions also remain about the challenges that end-to-end encryption pose for the spread of racist, misogynist, and other discriminatory content.

Clearly there is a lot at stake with Facebook's proposed changes. We are right to hold the company's plans up to scrutiny, and ask whether users will be the beneficiary of these planned changes.

Provided by The Conversation