

# HOW RIVALS STACK UP ON PRIVACY

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

Droves of disgruntled users scoured for alternatives after [WhatsApp](#) decided to force users to share their personal data with parent company Facebook Inc.

Telegram and Signal, which privacy advocates claim are more secure and mindful of user privacy, have seen a surge in downloads with users planning to switch to rival apps.

The older version of WhatsApp's privacy policy emphasized privacy. "Respect for your privacy is coded into our DNA," it said, but that line is missing in the new policy that takes effect on 8 February.

In contrast, Signal clearly states that it doesn't sell, rent or monetize users' personal data or content. Telegram has also assured that it doesn't use user data to show advertisements and that data collected by it only includes the phone number, contacts and email for two-factor authentication.

WhatsApp, on the other hand, gathers a lot of metadata, including information on user activity, device-specific information such as phone number, OS, IP address and phone model.

According to WhatsApp's privacy page on Apple App Store, the app also seeks purchase history, location, product interaction and advertising data. In comparison, Signal doesn't collect any data linked to users, and Telegram doesn't collect anything beyond what it states above.

Signal and Telegram also have additional privacy features that WhatsApp lacks.

For instance, WhatsApp doesn't store any user data after they are delivered and relies on third-party cloud platforms for backups of messages, photos and videos, which are not encrypted in the same way messages on WhatsApp are. If someone hacks the iCloud or Google Drive account in which WhatsApp messages are backed up, they can access the data.

Telegram, on the other hand, uses its own servers that are encrypted, so the messages remain secure even after they are backed up.

WhatsApp has also been flagged for not being able to fully secure its users.

In the past couple of years, security experts have spotted several vulnerabilities in WhatsApp.

One such vulnerability was exploited by unknown parties to spy on social activists, journalists, lawyers and political leaders in 2019 by using Pegasus spyware.

Click here to read the [Mint ePaper](#) Mint is now on Telegram. Join [Mint channel](#) in your Telegram and stay updated with the latest [business news](#).

Log in to our website to save your bookmarks. It'll just take a moment.

Oops! Looks like you have exceeded the limit to bookmark the image. Remove some to bookmark this image.

Your session has expired, please login again.

You are now subscribed to our newsletters. In case you can't find any email from our side, please check the spam folder.

**END**

Downloaded from **crackIAS.com**

© **Zuccess App** by crackIAS.com

crackIAS.com