



WhatsApp and Privacy: Common Myths

Authors: Krishna CV Grandhi, Chandra Lekha

This paper can be downloaded without charge at:

www.csail.org



When WhatsApp was launched in India around 2010, its premier selling point was the privacy it had to offer. The main feature backing the privacy claim was the feature of ‘End-to-End Encryption’, where the platform stated that only you and the person you are chatting with can see your messages. But over the years, many people have misunderstood what this really means.

Yes, WhatsApp is much safer than the traditional SMS. However, it isn’t as private as it makes you believe.

A few of the common myths associated with WhatsApp are as follows:

1. End-to-End Encryption Means Total Privacy.

Yes, WhatsApp uses End-to-End Encryption which protects your content of your texts, calls, videos, and photos. This means that not even WhatsApp can access your conversations. But the downside is that encryption doesn’t cover everything. WhatsApp still collects meta-data like who you message, how often, at what time, your device information, and your location. This data helps sum up your daily habits even without having access to the actual messages exchanged.

2. WhatsApp Doesn’t Share Data with Anyone.

Many users think WhatsApp keeps their information restricted from third party access. In reality, WhatsApp shares certain data with its parent company Meta (Facebook). This includes your phone number, device ID. And interaction data, which may be used for targeted advertising across Meta’s platforms. So, while your messages stay private, your behavior doesn’t.

3. Deleting Messages or Chats Erases Them Forever.

Deleting a message only removes it from your screen and possibly the recipients, if unsent within the time limit. But backups are another story. If you have chat backups enabled in Google Drive or iCloud, those backups are often not encrypted enough in the same way, meaning they could be accessed through other means. So ‘delete’ doesn’t always mean gone for good.



4. WhatsApp Status and Profile Privacy Settings are Foolproof.

You can tweak settings to control who sees your status, profile picture or last seen. But screenshots, screen recordings, or third-party apps can bypass these controls. Privacy settings help, but they don't guarantee full control over your information once its visible.

So, How Do You Stay Safer on WhatsApp?

- Limit backups or turn off cloud backups if you're concerned about message storage.
- Review privacy settings to restrict who can see your details.
- Be mindful of metadata, remember that your activity patterns are still visible.
- Stay alert for scams and phishing, as privacy features won't protect you from fraud.

WhatsApp doesn't pose a privacy concern right off the bat, but it isn't the digital privacy vault that many think it is. End-to-End Encryption protects your words, not your digital footprint. Being more aware of these myths helps you make smarter choices about how you could use the app and what you share on it.

www.csail.org