

The WhatsApp conundrum

The recent violence in Uttar Pradesh's Kasganj displayed, once again, the threat WhatsApp can pose in such fragile times. After the death of a youth, Chandan Gupta, in the violence, rumours were spread claiming the death of another person — Rahul Upadhyay. These rumours were circulated on Twitter, [Facebook](#) and WhatsApp groups, among other social media platforms. Some publications even carried the "news" of Upadhyay's death, which added to the communal tension. Upadhyay later clarified to the media that the rumours of his death were greatly exaggerated, and were being used by people spreading hate and paranoia on social media.

The situation is distressing because there is no apparent solution or even a proper diagnosis of the problem WhatsApp poses for law enforcement agencies, and society at large. The issue of checking "fake news" and misinformation on WhatsApp has never become part of popular discourse. Unlike Facebook or [Google](#), the messaging service did not play a role in allegedly "influencing" the US elections and is not as popular in the West. The challenge it poses, however, is far more complex.

WhatsApp works in a way that is fundamentally different from Facebook and Twitter. In the latter, it is comparatively easier to check fake news and prevent the spread of misinformation.

Posts on Facebook can be viewed by the friends of a user, whereas WhatsApp (the app is owned by Facebook) messages are encrypted end-to-end — a feature that is great from the perspective of privacy of users. Facebook newsfeeds are regulated by algorithms, which can be tweaked by the social media platform. WhatsApp's rationale for its security is a viable one: The encryption helps messages, photos, videos, voice messages, documents, status updates etc from falling into the wrong hands and can be controlled by users. There is no way to turn off the end-to-end encryption.

I don't think anyone would disagree with WhatsApp's claims. And privacy, of course, is an increasingly salient concern for many of us. But for those who care about what's happening beyond their private lives, the encryption presents a conundrum.

WhatsApp's end-to-end encryption ensures only you and the person or group you're communicating with can read and see what is sent, and nobody in between — interestingly even WhatsApp does not have access to the media and messages. When a message leaves a person's phone, it is assigned a cryptographic lock, and only the person receiving the message has the key to this lock. These keys change with every single message that is sent.

In India, however, WhatsApp's reach is what makes it dangerous at times. According to Satista, a leading statistics company, the number of monthly active WhatsApp users in India in February 2017 was 200 million — exponentially greater from August 2013, when it was just 20 million. The messaging application is being used more and more by rural and older populations, who are often new to the internet and less tech-savvy. With the prices of smartphones and mobile data falling rapidly, the number of WhatsApp users in the country will only grow.

The problem of fake news and misinformation being spread via WhatsApp is not exclusive to India. It has become a trend across the globe. Media organisations and fact-checkers face a problem every time they get a message on WhatsApp with something that is potential news. As passionate journalists, we always get excited by information that can make a news story. The problem with what we receive on WhatsApp is that often we cannot confirm the source of the message. Many messages are shared on groups, where you might not have the contact of the

person who has shared the the message saved on your phone.

A colleague recently received a message which said that the recent stoning on a school bus ferrying children was carried out by five Muslim men at a time when the anti-[Padmaavat](#) protests were in full swing. The message on WhatsApp had named all the five “accused” and was spread widely on WhatsApp and later on Facebook and Twitter. It was used to spread anti-Muslim hysteria and several people shared that message to make political gains.

What can be done? The spread of fake news through WhasApp is something we might not be able to control directly, and its encryption does protect the privacy of its users. This puts the responsibility of stopping this spread of misinformation on citizens and the media. People need to be told that messages on WhatsApp can be dangerous and false information can be spread by people looking to create trouble.

Most users do not understand the intricacies of technology. For them, the message needs to be repeated to drive the point home. Public figures and authorities need to stop sharing messages they receive on WhatsApp and the messaging app should issue disclaimers stating that messages can be false.

END

Downloaded from [crackIAS.com](#)

© **Zuccess App** by crackIAS.com