Preventing Misuse of WhatsApp

What is the issue?

\n\n

\n
- There has been a spate of mob violence and lynching across the country due to fear generated by rumours shared on social media platforms.
\n
- Of all the platforms, WhatsApp is proving the most challenging for investigators due to its strong privacy policy.
\n

\n\n

What makes WhatsApp different?

\n\n

\n
- All social media platforms struggle with rumours and misinformation, which are spread through posts as well as direct messages.
\n
- **Messaging -** While posts can be tracked, messaging services do not leave a trail, making it difficult to track the origin and spread of data.
\n
- Nonetheless, in most messaging services, information is stored in the parent server and police can request companies to share IP details if needed.
\n
- But contrarily, WhatsApp communications are "end-to-end encrypted" and information is stored in the devices of users and not on a common server.
\n
- **Instant -** This means, WhatsApp's servers handle only "encoded messages in transit", which can be decoded only in the receiver's device.
\n
- Also, even the encrypted messages are deleted once they are delivered at the receiver's end, thereby leaving no trace within WhatsApp's apparatus.
\n
- This implies, even whatsApp doesn't know what is being disseminated through its platform and hence can't provide investigating agencies with

information.
\n

- **Delayed -** If a message cannot be delivered immediately (e.g. if the receiver is offline), then whatsApp's servers are said to retain messages for 30 days.
\n
- But if a message is still undelivered after 30 days, it is nonetheless deleted without a trace.
\n

\n\n

How have WhatsApp based cases been handled thus far?

\n\n

\n

- Maharashtra Cops claim to have tracked down the source in a few cases were the posts had been shared just a few times.
\n
- Their "modus operandi" was largely conventional (non technological), and they followed the sender-receiver trail manually by interrogating the entire chain.
\n
- Such an approach has already proved futile when forwarded messages had gone viral with millions of shares.
\n
- Hence, if metadata is deleted like in WhatsApp, it is almost impossible to track the trail of forwards beyond a few users.
\n
- Notably, metadata means – information like "user name, device info, log-in time" and other specifics, which are used for enabling the service function.
\n

\n\n

How is WhatsApp trying to prevent the misuse of its platform?

\n\n

Research:

\n\n

\n

- WhatsApp has stated that the company is trying to learn more about the

way misinformation spreads on its platform.
\n

- **Data Analysis -** Its current spree of research is through the amount of metadata that the company gets access to while transmitting messages.
\n
- The drive is largely focused on understanding when spam is being spread intentionally and when it is happening unintentionally.
\n
- **Collaboration -** WhatsApp is also seeking to collaborate with various other organisations and governments to arrive at a solution to the current malice.
\n
- Nonetheless, WhatsApp has asserted its unfettered commitment to user privacy and encrypted instant message delivery without data retention.
\n

\n\n

Framing Fixes:

\n\n

\n

- At the moment, WhatsApp is working on a mix of in-platform fixes and off-platform intervention.
\n
- **Internal Fixes -** Within the platform it planning to give more authority to group administrators for restricting publishing in the group.
\n
- A forward label (which marks forwarded messages) is in beta testing, and an option for flagging doubtful forwarded content is also being considered.
\n
- Resources like fact-checking websites for verifying content are also being developed in parallel.
\n
- **External Fixes -** Off-platform, it is expected to initiate measures to educate people about the perils of misinformation and ways to identify them.
\n

\n\n

What are some actions governments worldwide have taken?

\n\n

\n

- **Liability -** In India, authorities can book group administrators if they are found endorsing false malicious content.
\n
- But as the admin has no control over what other people in the group will post, he/she is not liable for action if he is a mere spectator.
\n
- **Awareness -** Group admins are expected to inform any member posting misinformation about the consequences and restrain them from doing so.
\n
- Government officials too have taken out awareness campaigns to educate the masses on the perils of fake information.
\n
- In Mexico, private groups collaborated to set up Verificado 2018, a fact-checking initiative, to disrupt the spread of fake news.
\n
- **Curtailments -** Many nations (including India) have restricted internet during times of unrest, primarily to block ill intentioned WhatsApp campaigns.
\n
- Uganda has introduced a social media tax as check on online gossip.
\n

\n\n

\n\n

Source: Indian Express

\n