Source : www.thehindu.com Date : 2021-05-30

EXPLAINED

Relevant for: Science & Technology | Topic: IT, Internet and Communications

The story so far: On May 25, Facebook's messaging platform WhatsApp moved the Delhi High Court against India's new Information Technology rules. May 25 was the deadline for IT intermediaries to comply with the new rules, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, notified in February.

Under the new rules, a "significant social media intermediary providing services primarily in the nature of messaging shall enable the identification of the first originator of the information on its computer resource as may be required by a judicial order…" This is the rule WhatsApp finds problematic.

Centre accuses WhatsApp of attempt to stall norms

To simplify, a significant social media intermediary, as per the new norms, is a social media intermediary which has more than 50 lakh registered users. WhatsApp, which reportedly has close to half a billion users in India, is a significant social media intermediary. It is also a service "primarily in the nature of messaging". The rules, therefore, require WhatsApp and those offering messaging services and having a user base of over 50 lakh to be able to trace 'problematic' messages to their originators. The requirement is one of traceability, and WhatsApp is opposed to it.

WhatsApp's messaging system is end-to-end encrypted, which means, in its own words, "only you and the person you're communicating with can read what's sent, and nobody in between, not even WhatsApp". This has been the case since 2016. The encryption protocol that it uses is one that was developed by Open Whisper Systems, which is well known for its Signal app.

Traceability, according to WhatsApp, is a threat to user privacy.

In a blog entry, titled *What is traceability and why does WhatsApp oppose it?*, it argues that traceability would end up "breaking the very guarantees that end-to-end encryption provide". It says, "In order to trace even one message, services would have to trace every message." The reason it says this is because there is no way to know what a government would want to investigate in the future.

A WhatsApp spokesperson has been quoted in *The Hindu* as saying that: "Requiring messaging apps to 'trace' chats is the equivalent of asking us to keep a fingerprint of every single message sent on WhatsApp, which would break end-to-end encryption and fundamentally undermines people's right to privacy."

Further, in its blog, WhatsApp has said that traceability violates human rights. It says, "Innocent people could get caught up in investigations, or even go to jail, for sharing content that later becomes problematic in the eyes of a government, even if they did not mean any harm by sharing it in the first place." This, it says, could pertain to cases where people shared something just out of concern or for checking its accuracy.

WhatsApp users have nothing to fear: Ravi Shankar Prasad

WhatsApp also says traceability doesn't work. It gives an example: "If you simply downloaded an image and shared it, took a screenshot and resent it, or sent an article on WhatsApp that

someone emailed you, you would be determined to be the originator of that content." And that is why it reckons that "tracing messages would be ineffective and highly susceptible to abuse".

Even without traceability, WhatsApp says, "We respond to valid requests by providing the limited categories of information available to us, consistent with applicable law and policy. We also have a team devoted to assisting law enforcement 24/7 with emergencies involving imminent harm or risk of death or serious physical injury. We consistently receive feedback from law enforcement that our responses to requests help solve crimes and bring people to justice."

WhatsApp has also cited the pro-privacy arguments of organisations such as Mozilla, Access Now, Internet Society, Center for Democracy and Technology, Stanford Internet Observatory, Electronic Frontier Foundation, and Internet Freedom Foundation to bolster its point.

In the U.S., for instance, WhatsApp, under different requirements of law, may be compelled to share the name, start date of the service, last seen date, IP address, email address, numbers blocked by the user, 'about' information, profile photos, group information, and address book.

Editorial | Fitful approach: On WhatsApp privacy policy and need for data protection laws

Electronics & Information Technology Minister Ravi Shankar Prasad has said the government "is committed to ensure the Right of Privacy to all its citizens but at the same time it is also the responsibility of the government to maintain law and order and ensure national security."

A release by the Ministry of Electronics and IT elaborates on two legal points related to the traceability requirement. The first is regarding reasonable restrictions, or the conditions that could trigger a traceability order by a court. The release says, "No Fundamental Right, including the Right to Privacy, is absolute and it is subject to reasonable restrictions." A traceability order shall only come about, as Rule 4(2) states, "for the purposes of prevention, detection, investigation, prosecution or punishment of an offence related to the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order, or of incitement to an offence relating to the above or in relation with rape, sexually explicit material or child sexual abuse material, punishable with imprisonment for a term of not less than five years".

The second legal argument is about the test of proportionality, the cornerstone of which, as the release says, "is whether a lesser effective alternative remedy exists". The traceability measure will be a measure of "last resort", according to the release, which cites the rule in this regard. The rules further state that "in complying with an order for identification of the first originator, no significant social media intermediary shall be required to disclose the contents of any electronic message, any other information related to the first originator, or any information related to its other users".

Centre asks WhatsApp to withdraw privacy policy update

The Ministry has also criticised WhatsApp for making "no specific objection" to this requirement till date. The release says, "Any operations being run in India are subject to the law of the land. WhatsApp's refusal to comply with the guidelines is a clear act of defiance of a measure whose intent can certainly not be doubted."

It also makes a reference to another issue where WhatsApp and the government have a difference of opinion. It says, "At one end, WhatsApp seeks to mandate a privacy policy wherein it will share the data of all its users with its parent company, Facebook, for marketing and advertising purposes. On the other hand, WhatsApp makes every effort to refuse the enactment of the Intermediary Guidelines which are necessary to uphold law and order and curb the

menace of fake news."

This pertains to the Indian Government's opposition to WhatsApp's privacy update. The privacy update was announced for February but was postponed following a severe backlash from users in India, some of whom moved to alternatives such as Signal. The government, which filed a case against the privacy update in the Delhi High Court, has argued that privacy, data security and individual choice are at stake. The privacy update will ensure that users will no longer be able to stop WhatsApp from sharing data with its parent Facebook, and the only way they can prevent this is by deleting their accounts.

WhatsApp scraps May 15 deadline for accepting privacy policy terms

While welcoming strong encryption as a means of safeguarding user privacy, the communiqué, however, said, "We are concerned where companies deliberately design their systems in a way that precludes any form of access to content, even in case of the most serious crime. This approach puts citizens and society at risk by severely eroding a company's ability to identify and respond to the most harmful illegal content... Tech companies should include mechanism[s] in the design of their encrypted products and services whereby governments, acting with appropriate legal authority, can obtain access to data in a readable and usable format."

Antony Clement Rubin vs Union of India was one of the recent prominent cases where the question of traceability was discussed (there were other similar cases as well). This came up initially in the Madras High Court as a petition to link users' Aadhaar number with their social media accounts. The Supreme Court of India eventually took over the case but not before technical solutions on tracing the originator were heard. WhatsApp has maintained all along the impossibility of traceability coexisting with end-to-end encryption. The last hearing in this case was in early 2020.

Our code of editorial values

Please enter a valid email address.

To empathise with netizens on the mental health front and to give them more control of their social media, Instagram and Facebook are officially rolling out the option to remove 'likes'

The software giant made several announcements on day one that included bringing one of the most powerful language models, GPT-3, to its Power Platform; new features and tools for Teams developers; and introducing PyTorch Enterprise on Azure.

END

Downloaded from **crackIAS.com**

© **Zuccess App** by crackIAS.com