IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Encryption Vs. Decryption: A Brewing Crisis For User Privacy?

D Dhanusha Shree[1], N Akash Pranal[2]

[1]Postgraduate Student (LL.M), [2]Advocate

[1]School of Law, VIT Chennai, Chennai, India

Abstract: The growing use of WhatsApp encryption has given users with unprecedented power over the privacy of their message information. However, a potential conflict has arisen between national security concerns and user privacy rights after the Indian government's recent amendment to the IT Rules in 2022. This paper assesses how WhatsApp's end-to-end encryption and the Indian government's motive for deeper access to encrypted conversations due to national security concerns are balanced. The paper examines the vital aspects of WhatsApp encryption and its advantages in protecting user privacy. Later, it compares the primary provisions of the IT ACT 2000 and IT Rules 2022 that are traceable and decrypted upon lawful interception. The paper highlights the drawbacks of these amendments to WhatsApp's encryption protocol and the potential outcomes for user privacy. In addition, the paper delves into cyber crimes that cause significant threats to national security. People who introduced the amendment emphasize the importance of access to encrypted messages for investigating cybercrimes and national security threats. On the other side, concerns have been raised about the possibility of misuse of powers and the violation of freedom of expression. The purpose of this research paper is to evaluate India's growing user privacy dilemma critically. A balanced strategy is advocated in the paper's conclusion, which offers several potential solutions to maintain a balance between both national security and user privacy rights in digital India.

Keywords: WhatsApp encryption, IT Rules Amendment 2022, National security, right to expression, privacy rights, cybercrimes, deep fake

I. INTRODUCTION

II.

One of the strongest quotes about social media and privacy by the CEO of Mashable, Pete Cashmore, is: "Privacy is dead, social media holds the smoking gun", where he says that anything stupid done today will always remain eternal because of the internet. WhatsApp is one of the most prominent social interaction and communication applications. The application gained popularity during its initial stage offering users freedom of privacy over the messages they share and access. On the other hand, the Indian Government's amendment to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules) has created a stir between user privacy rights and national security concerns. The ambition of this amendment is to brace cybersecurity and tackle cybercrimes, which in turn also raised repercussions for user privacy rights. WhatsApp's end-to-end encryption is considered one of the net-worthy features of the application when compared to traditional SMS. The users trust this application more than others because they believe the shared messages are accessible only by the sender and the recipient. However, during unavoidable circumstances, i.e.; emergencies, national emergencies, it is important for a third party's intervention into privacy which is considered lawful. The latest amendment made in the IT Act enables a third party, i.e.; an intermediary to trace and decrypt harmful messages for national security purposes. This conflict has raised questions about governmental surveillance powers and individual liberty in digital India.

The major intention of this paper is to promote the new amendment made in the IT Act without compromising the personal liberty of users in demands of national security and propose possible solutions that uphold both.

CYBERCRIMES: A NATIONAL SECURITY THREAT?

The World Economic Forum's Global Risks 2013 Report has reported the increasing spread of false information and rumours via social media as a national security threat. It is impossible to believe today that any information put up by a person on the internet or in his system is completely confidential. The growth of cybercrimes has increased gradually creating a great threat to national security. Some of the major cybercrimes that are causing threats to national security are phishing, cyber defamation, child pornography, Denial of Service attacks (DoS), etc.[1] Deepfakes are also one of the emerging cybercrime threats to the government. The increasing use of social media and mobile phones has led to the phenomenon of "Flash Crowds", which means information spreads rapidly among the public owing to their immediate responses. Especially Facebook and YouTube are the prime sources for the same. WhatsApp was also used to spread fake news about "child lifting" that went wrong leading to mob lynching of innocent people. To cause a national security threat, the antinational elements use social media platforms to create panic among North Eastern citizens during violence in Myanmar. [2]Therefore, it is evident that there is no control over social media, even if the government took a step forward, they were rejected on the grounds of freedom of expression and right to privacy. [3]The fundamental rights guaranteed in the Indian Constitution are misused. An increase in hate speech and troll disinformation of the government has become very common and they are used to suppress the government by the opponents. From cyber-attacks to protecting data the Government of India has initiated steps towards national security. Four Sectoral Computer Emergency Teams in Power Systems, Transmission, Thermal, Hydro, and Distribution were set up by the government of India. The first half of 2017 alone witnessed around 27,000 cybersecurity threat incidents and the majority of the threats were, phishing, ransomware attacks, website intrusions, and defacements. The National Security Policy of the Indian Government is also a great initiative to combat cybercrimes. The motive behind the policy is to draft a secured cyber ecosystem framework. The formulation of policies like the National Cyber Security Policy 2020 are also notable initiatives by the Government.

DEEPFAKE: REAL OR REEL?

Deepfake technologies emerged in 2017 and have taken the seriousness of cybercrimes to the next level creating confusion among the public to identify whether it is *real* or *fake*. Initially, it targeted celebrities, but later caused threats to the common man, institutions, and the Government. For an opponent or an individual to defame the government and to disrupt the political landscape, the Deepfake technology was of great advantage. The spreading of misleading political information especially during the election period, fake videos, and pornography are all the major threats caused by deepfake technology. The technology uses Artificial Intelligence's help by extracting the original content and complying with them by matching expressions with AI and delivering a fake video. One of the most famous examples of deepfake videos is the one created by actor and comedian Jordan Peele showing former president of the US, Barack Obama delivering a public speech on raising awareness about deepfake technology and its ability to spread fake news. [4]However, this was humorous, but it is important to know the seriousness behind the problem. Deepfakes can change the public's perception and pose a threat to elections, democracy, and the entire political landscape by spreading fake videos of statements not told by the politicians and actions not done by them. In India, in November 2023, the Indian Government issued a warning about the "dangerous and damaging" implications of AI technology when a deepfake video of Bollywood actress Rashmika Mandanna went viral. [5]Last month, Bollywood actors, Ranveer Singh and Aamir Khan became prey to the deepfake technology showing them campaigning for the opposition Congress party.[6] IT Rules 2021 plays a significant role in undertaking expeditious actions during such cases and scenarios. Users are told not to host malicious content or deep fake

and to remove such content when reported within 36 hours. Rule 7 of the IT Rules, 2021 would attract if the said actions are not undertaken.[7] Collaborative efforts and private-public partnerships between governments with Global cooperation can combat the global spread of misinformation through deepfake technology.

GLOBAL ASPECT

After WhatsApp's E2E encryption policy, even Facebook launched to incorporate the same in 2019. However, this feature of WhatsApp is a high hindrance for investigative work for law enforcement. During that time, the United States, the United Kingdom, Australia, Canada, and New Zealand, the "Five Eyes" intelligence alliance issued a joint statement in 2019 stating to allow legal access to the information through, an "encryption backdoor", which allows only legal authorities and government agencies to decrypt information for national security concerns.

- **Australia**
  The Surveillance Legislation Amendment (Identify and Disrupt) 2021 was introduced providing three new powers to the Australian crime branch:
  1. Data disruption warrants. Harmful content like child pornography materials is deleted and disrupted by the agency.
  2. Network activity warrants. Where an agency issues investigatory warrants on access to computer networks to trace when criminal networks carry out any criminal activity.
  3. Account takeover warrants. The agency takes control of social media accounts and bank accounts to investigate criminal activities.[8]

- **United States**
  The EARN IT Act in the US plays a vital role in addressing online child sexual exploitation by modifying Section 230 of the Act. The legislation enhanced the reporting requirements while it aimed to protect minors and create more accountability for online service providers. Therefore, there are ongoing debates about balancing privacy which is not yet attained completely.

- **United Kingdom**
  "Ghost Protocol" by GCHQ was proposed to allow law enforcement access by compromising user privacy. This mechanism will create a law enforcement account as a hidden participant and the messages are encrypted to all the recipients. Here the law enforcement account is into play without the user's knowledge.

END-TO-END ENCRYPTION

"Messages are end-to-end encrypted", often pops up when we use the WhatsApp application while chatting. As the application stated, WhatsApp intended to communicate end-to-end encrypted without any third party's intervention. It means, no one can read or access the information sent by the sender to the receiver unless any of their devices is stolen and the information is accessed by opening their device using the password. End- to End Encryption, is a type of messaging that keeps messages private from others including the messaging services that provide a server for transmission. In the process of End-to-End Encryption when an message is being sent by a person through a medium, the data are encrypted from the sender's end and travel through the server reaching the intended receiving end. The messages or the data cannot be read, viewed, or tampered with by the server only the recipient can decrypt it thus restricting the internet service provider (ISP), applications, hacker or any other entity or service.
The keys used i.e., the cryptographic keys used to encrypt and decrypt messages are stored in two endpoints one on the sender's end and the other on the receiver's end. Once a message shared, others can use the public key to encrypt a message and send it to owner of the public key. The message can only be decrypted by a private key correspondingly, also called the decryption. The method of E2EE is practiced when data security and privacy are necessitated which could comprise the sectors of finance, healthcare, and communications industries. It is used often by the companies to comply with data privacy and security regulations of the laws of respective nations.

LIMITATIONS AND OBLIGATIONS BY IT RULES 2021

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[9] is a subordinate or substitute legislation that has suppressed India's Intermediary Guidelines Rules 2011. The IT Rules 2021 are based on the motion to "resolve the Government for strengthening the legal framework and making social media platforms accountable under the law", these rules stem from section 87 of the Information Technology Act, 2000[10] and are a combination of the OTT Regulation and Code of Ethics for Digital Media and the draft Intermediaries Rules, 2018. Under Rule 4(2)5 of the IT Rules, 2021[11] a social media intermediary should additionally observe that such intermediary can be asked to trace the first originator of a message or a post or a tweet for prevention, investigation, detection, punishment, or protection of an offence related to sovereignty or integrity of India, friendly relations with other states, security of the state, or public order or incitement of any of the offences mentioned above or other offences related to sexual abuse/ assault or rape, child abuse or any offence that is not punishable with less than 5 years. This rule is breaking the principle of interoperability and common standards on which the open internet is operating. This rule is asking intermediaries like WhatsApp to archive what people are sharing through the platform, by breaking end-to-end encryption of a conversation and violate the absolute right of privacy.

Alternatively, social media intermediaries are required under Rule 4(4)6 of the IT Rules 2021[12] to actively detect content that depicts or encourages rape or child abuse actions, whether directly or indirectly. To do this, they must employ automated tools and technology-based procedures. Requiring social media intermediaries to adhere to rules 4(2) and 4(4) may compromise Indian residents' privacy, even though the goal is to keep security protocols up to date with quickly evolving technological developments. Rule 4(4) states that in order to identify shared information, platforms like WhatsApp will have to break end-to-end encryption, which would be a gross invasion of privacy. According to Rule 4 (1) (b)8, it is required to appoint a Nodal Contact Person to coordinate with law enforcement agencies around the clock. Rule 4 requires the appointment of a Resident Grievance Officer under subclause (c) and the monthly publication of a compliance report under subclause (d). The clauses are not just adding to the intermediaries' workload, but also adding complications that impact their effectiveness.[13]

WHATSAPP CRITICISM OVER THE IMPUGNED PROVISON IN THE IT RULES 2021

The legitimacy of IT Rules 2021 has been contested in a number of instances filed in various high courts by parties aggrieved by certain mandatory parts of the rule, including rule 4(2) for tracing the author of a message. WhatsApp has brought one of these lawsuits before the Delhi High Court. According to WhatsApp's high court appeal, rule 4(2) is unlawful since it forces citizens' privacy to be violated by decrypting end-to-end encrypted conversations, in violation of Articles 14, 19, (1) (a), 19 (1) (g), and 21 of the Indian constitution[14]. According to the norm, an intermediary must determine who sent a message in the first place; this identifying process is referred to as "traceability." Experts in technology and privacy have concluded that traceability violates end-to-end encryption and jeopardises the privacy of billions of users who communicate online.[15] Since the government cannot foresee which messages it will choose to look into, it has made traceability of all messages sent and received through the platform mandatory, opening the door to a new kind of widespread surveillance. In order to comply with this regulation, the intermediaries will need to keep an enormous and continuously expanding data record of each message sent over the platform, or they will need to permanently append an identity stamp to each message that will serve as a message's fingerprint and be used to track it down.

Technology and privacy experts have determined that traceability breaches end-to-end encryption and puts the privacy of billions of online communicators at risk. Because the government cannot predict the messages it will investigate, it now requires traceability of all messages on the platform, leading to increased surveillance. To meet this rule, intermediaries must maintain a vast and ever-growing data log of all messages on the platform, or they must add a unique identifier to each message to track it indefinitely. The government's

attempt to facilitate traceability is not only violating citizens' privacy by compromising end-to-end encryption but also proves to be ineffective and easily open to misuse. If someone unknowingly shares a screenshot, a copied message, or an article on WhatsApp sent by someone else, they could be mistakenly perceived as the original source of that content and be implicated in a criminal investigation despite not being involved. If we view the big picture as a tree, it's clear that examining just one branch won't uncover the roots without traversing various connections between branches during the investigation. Next, traceability is used to reverse the typical investigation process where technology companies give individuals' information to authorities during legal proceedings. However, when it comes to traceability, the authorities conducting the investigation will share specific details and request the intermediary to identify the initial source.

Protecting citizens' privacy is the utmost duty of the state as the right to privacy is one of the fundamental pillars holding the democracy of the country. Hence for protecting the same Hon'ble justice D.Y. Chandrachud has put forth a three-part test for making a law to invade the privacy of a person, by stating that, "A law which encroaches upon privacy will have to withstand the touchstone of permissible restrictions on fundamental rights. In the context of Article 21, an invasion of privacy must be justified on the basis of a law which stipulates a procedure which is fair, just and reasonable. The law must also be valid with reference to the encroachment on life and personal liberty under Article 21. An invasion of life or personal liberty must meet the threefold requirement of (i) legality, which postulates the existence of law; (ii) need, defined in terms of a legitimate State aim; and (iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them".[16]
Therefore any law which intends to invade the privacy of a citizen shall meet these three touchstones to be constitutionally valid. Rule 4(2) [17]is prima facie not meeting the same as the rule is obligating an intermediary break the end-to-end encryption and breach privacy of a person for investigating a crime that is not committed by such person. Forcing an intermediary for breaching the privacy of a person does not create a rational nexus between the object and means used to achieve such information cannot be a proportional law.

However, if India is required to reveal the initial source of the information, it will have negative consequences such as journalists facing danger, clients and attorneys being hesitant to share information, and civil activists facing risks for speaking out about rights and policies. It all comes down to the individual's choice in deciding when and with whom they want to share information, including divulging their own identity. According to a Supreme Court case involving Central Public Information Officer, Supreme Court vs. Subhash Chandra Agrawal[18], individuals have the right to choose who they reveal their identity to and to remain anonymous to others, as it is part of the right to privacy. The challenged sections of IT Rules, 2021 seem to be random and are suspected of being a government attempt to quickly solve a problem that could be addressed in other ways without violating citizens' privacy, making it unconstitutional[19]. In the case of Ram Jeth Malani vs. Union of India[20], it was stated that fundamental rights should not be compromised in order to quickly address a systemic issue.[21]

CONCLUSION

This paper discusses the conflict between user privacy rights and national security concerns in the context of WhatsApp and the Indian Government's recent amendment to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules). The paper highlights the increasing cybercrimes as a national security threat, including the emergence of Deepfake technology, which poses a serious challenge in identifying real and fake information. It explores the global aspect of cybersecurity measures taken by countries like Australia, the United States, and the United Kingdom to combat cybercrimes. The paper delves into the concept of End-to-End Encryption used by WhatsApp to ensure message privacy, as well as the limitations and obligations imposed by the IT Rules 2021. It discusses the concerns raised by WhatsApp regarding the violation of user privacy rights in the context of traceability of messages as mandated by the IT Rules 2021, and the potential implications on citizens' privacy and fundamental rights. The paper

also highlights the importance of upholding the right to privacy and the three-part test prescribed by Hon'ble Justice D.Y. Chandrachud to evaluate the constitutionality of laws that invade privacy.

REFERENCES

[1] Mirdul Sharma & Satvinder Kaur, Cyber Crimes Becoming Threat to Cyber Security, 02 ACADEMIC JOURNAL OF FORENSIC SCIENCES. 36- 40 (2019)
[2] Mohammed Khalid, Emerging Challenges to India's National Security: a Domestic Dimension, 09. SCH J ARTS HUMANIT SOC SCI. 3, 4 (2021)
[3] 04 LIOR TABANSKY, MILITARY AND STRATEGIC AFFAIRS 131- 132 (2012)
[4] Valencia A. Jones, Artificial Intelligence Enabled – Deepfake Technology: The Emergence of a New Threat, UTICA COLLEGE PROQUEST DISSERTATION & THESES (May 2020), https://www.proquest.com/openview/60d6b06b94904dccf257c4ea7c297226/1?pq-origsite=gscholar&cbl=18750&diss=y

[5] Darya Bazarkina, Evgeny Pashentsev, The Malicious Use of AI: Challenges to Psychological Security in the Republic of India (Apr 2024), https://d1wqtxts1xzle7.cloudfront.net/113321263/Malicious_Use_of_AI_and_Challenges_to_Psychological_Security_of_BRICS_Countries-libre.pdf?1713099850=&response-content-disposition=inline%3B+filename%3DMalicious_Use_of_AI_and_Challenges_to_Ps.pdf&Expires=1716660891&Signature=W~LxRjZKTdhBlFcnufuBjKLIqhDQpd3bpFF-6~ZBsNFynVIAZvttNs~5PeJBdW8mvMVJJFHdi52GjFa-m6Whrk66eMGDJcTIxJa~n0ka9U~y2Cnvz2Y5r98UwxW7zRazXhaIXaWT-w4ey5tCPek0qRhbQc2nKEf8EWc7~psyg0-5w5ukgm6BKVaKGjMfJyUKZItb6rq9c1Fu6IA8BVwt2jsEE2mxjjYFzpIWjMNWZrBuDLACyEEAK4-TIM~U~ktJJwNG8EUNjC3sgIrLsx264qJvUTV6DSwT5IMyv~fXIcMhG5dSbWUPH5LRyzlYPw~kAAdQPCOB6idIFyEeoxuzow__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA#page=71
[6] Meryl Sebastian, AI and deepfakes blur reality in India elections, BBC (May 16, 2024), https://www.bbc.com/news/world-asia-india-68918330
[7] Dr. Pawan Singh , Dr. Bharat Dhiman . Exploding AI-Generated Deepfakes and Misinformation: A Threat to Global Concern in the 21st Century. TechRxiv. December 05, 2023.
[8] CROSS-BORDER LITIGATION IN A DIGITAL CONTEXT: FROM CLASSROOMS TO JUDICIARY 200- 210 (Dykinson, S.L. Meléndez Valdés)
[9] Vide G.S.R. 139(E), dated 25.2.2021, published in the Gazette of India, Extra., Pt. II, Sec. 3(i), dated 25.2.2021.
[10] THE INFORMATION TECHNOLOGY ACT, 2000 (No. 21 OF 2000), MGIP(PLU)MRND—1359G1—14-6-2000.
[11] Rule 4(2)of the IT RULES, Supra 9
[12] under Rule 4(4)6 of the IT Rules 2021,supra 9
[13] Supra 9
[14] Articles 14,19 and 21, THE CONSTITUTION OF INDIA [As on May, 2022] 2022
[15] What is Traceability and Why WhatsApp Oppose it?, WhatsApp, https://faq.whatsapp.com/general/security-and-privacy/what-is-traceability-and-why-does-whatsapp-oppose-it, last seen on 10/09/2021. What is Traceability and Why WhatsApp Oppose it?, WhatsApp, https://faq.whatsapp.com/general/security-and-privacy/what-is-traceability-and-why-does-whatsapp-oppose-it, last seen on 10/09/2021.
[16] K.S. Puttaswamy vs. Union of India, AIR 2017SC 4161.
[17] Supra 9
[18] Central Public Information Officer, Supreme Court v. Subhash Chandra Agrawal, (2020) 5 SCC 481.
[19] Del HC| Whatsapp challenges Intermediary Rules, says traceability will break end-to-end encryption, breach privacy; Union of India says no Fundamental Right is absolute, SCC Online, https://www.scconline.com/blog/post/2021/05/27/del-hc-whatsapp-challenges-intermediary-rules-says-traceability-will-break-end-to-end-encryption-breach-privacy-union-of-india-says-no-fundamental-right-is-absolute/, last seen on 09/09/2021
[20] Ram Jethmalani v. Union of India, (2011) 8 SCC 1
[21] Ibid