CHANAKYA LAW REVIEW (CLR)

VOL. V (ISSUE 01) JAN-JUNE, 2024, pp.36-55

CYBERNETIC CONUNDRUM: DECRYPTING PRIVACY CONCERNS AMID GOVERNMENTAL DATA REGULATION EFFORTS

Ananya Gupta[1]

INTRODUCTION

In the contemporary Internet age, netizens are assiduously engaged in online social media platforms. The advancement of technology has given rise to platforms that provide instantaneous updates on global occurrences to almost everyone. Nonetheless, it has progressed and transformed from a cutting-edge innovation to a potential tool for exploitation.

Most applications utilized for daily communication deploy various security checks for the safety of user data, with encryption being a commonly used measure. Encryption encodes users' messages to prevent any third party from interfering in communication. However, cybercriminals are also exploiting this technological anonymity for various illicit activities. To address such instances, the government requires access to the Encryption keys which can decrypt cybercriminals' data to trace the originator of messages.

This presents a conundrum due to the potential for misuse of these backdoor encryption keys by the government. While the primary aim is to curb unlawful activities, there is a risk that these measures could lead to violations of the right to privacy and freedom of speech and expression, if not regulated. This potential misuse threat has given rise to the conundrum for the intermediaries to share the keys with the government due to the legal considerations surrounding the same, both globally and specifically within India. The present Article addresses the plight of users in the backdrop of the enactment of the Digital Data Protection Act, 2023 in India.2

The research paper is structured into five sections. Section II shall provide an overview of the Encryption method used by Intermediaries. Section III shall explain the measures adopted by the Government Agencies to get access to backdoor encryption keys. Section IV shall delve into the intricacies of conundrum; which intermediaries are facing due to such measures. Section V shall provide alternative methods that can be considered by the Government. Section VI will highlight the key features of the Digital Personal Data Protection Act, 2023, focusing on how the Act, in the backdrop of such conundrum, introduces certain provisions that are burdensome for users, as they infringe upon their rights and freedoms. Section VII will

[1] BA LL.B., NLIU, Bhopal

[2] The Digital Personal Data Protection Act, 2023.

present the conclusions and offer recommendations.

THE DEVELOPMENT OF CRYPTOGRAPHY: A HISTORICAL OVERVIEW AND CONTEMPORARY ENCRYPTION METHODS

In the contemporary digital landscape, social media platforms employ encryption to safeguard users' data from unauthorized access. Nevertheless, this technology, albeit by a different name, has been in practice for a significant duration and was historically referred to as cryptography.

Cryptography

Cryptography[3] originates from two Greek words: "Krypto," meaning hidden, and "grafo," meaning to write, thus encapsulating the concept of concealed or hidden writing. Historically, cryptography is rooted in ancient practices where it served to obscure the content of messages during transmission.[4] In essence, cryptography refers to the process of converting a message into a code or alphanumeric value to secure its contents.

In ancient times, cryptography was employed primarily for the protection of basic communication messages. These early methods were essential for ensuring the authentication of the message's sender and the confidentiality of its content during transmission. Historical cryptographic techniques, such as the Caesar cipher and the substitution cipher, were fundamental in securing messages from unauthorized access and verifying the integrity of communications. For example, the Caesar cipher, used by Julius Caesar, shifted letters in the alphabet to encode messages, a simple yet effective means of maintaining secrecy and authenticity.

However, as we transition from these historical practices to the present era, our focus shifts to contemporary technological advancements in the field of cryptography. Modern cryptographic techniques have evolved far beyond these rudimentary methods, incorporating sophisticated algorithms and protocols to address complex security challenges in the digital age. In the contemporary age, such technology is termed Encryption.

Encryption

"Encryption is a reversible or irreversible transformation of data from the original to a difficult-to-interpret format to protect confidentiality, integrity and sometimes its authenticity".[5] In the field of Encryption, a *key* is a sequence of characters used within an encryption algorithm to transform data, rendering it seemingly random and unintelligible to unauthorized individuals. Analogous to a physical key that locks or unlocks a door, the cryptographic key serves to *encrypt* data, making it accessible for *decryption* only to those who

[3] Oxford English Dictionary (10th edn, 2020).

[4] M.S. Baptista, 'Cryptography with Chaos' (1998) 240(1) Physics Letters A 54.

[5] Apar Gupta, Commentary on Information Technology Act (3ed edn, Lexis Nexis 2015) 55.

possess the correct key. In this process, the original data is known as *plaintext*, while the data that results from encryption is referred to as *cipher text*.

Historically, before the advent of computers, creating ciphertext often involved a simple technique called a substitution cipher. In this method, each letter of the plaintext is substituted with another letter in the alphabet based on a fixed system or pattern. Consider a scenario where someone transmits a message "Hello" to another person, and each letter is substituted with the succeeding one in the alphabet: "Hello" transforms into "Ifmmp." Although "Ifmmp" appears as a seemingly random sequence of letters, possessing the key allows one to substitute the corresponding letters and decipher the message back to "Hello." In this instance, the key is determined by shifting each letter down one position in the alphabet, unveiling the original letter.

These ciphers are relatively susceptible to decryption through straightforward statistical analysis, as certain letters tend to appear more frequently in any given text (for instance, E is the most common letter in the English language). To counter this vulnerability, cryptographers introduced a system known as the one-time pad. A one-time pad is a key designed for single-use only, comprising at least as many values as there are characters in the plaintext. Essentially, each letter is substituted with another letter that represents a distinct number of positions removed from it in the alphabet. For instance, if someone needs to encrypt the message "Hello" using a one-time pad with the values 7, 17, 24, 9, and 11.[6]

Different platforms employ various encryption methods, which can be categorized based on different parameters. In this paper, we will focus specifically on differentiating encryption methods based on the “recoverability” of the encrypted data.

Types of Encryptions:

Encryption can be classified into multiple categories based on varied parameters. Amongst others, one such criterion is the “Recoverability” of encoded information. Lewis, Carter, and Zheng differentiated encryption based on recoverability in 2017, by classifying the encryption method as Recoverable and Non-Recoverable encryption.[7]

Recoverable Encryption

In Recoverable Encryption, the service provider has the access to the decryption key. This helps the service provider to decrypt the data in the message. The service provider or whosoever has access to the private key can access the information by decrypting it.

[6] ‘What is a Cryptography Key’ <https://www.cloudflare.com/en-gb/learning/ssl/what-is-a-cryptographic-key/> accessed 22 December 2023.

[7] James A. Lewis, Denise E. Zheng and William A. Carter, ‘The Effect of Encryption on Lawful Access to communications and Data’ (2017) Centre For Strategic International Studies.

Recoverable encryption is advantageous for recovering lost data in many situations by using effective decryption algorithms such as File Vault 2 and BitLocker[8]. However, it poses a risk, potentially violating the Right to Privacy,[9] by unauthorised data access or interference. Therefore, in Recoverable Encryption even if the data is encrypted, the service provider has access to the information.[10]

Non-Recoverable Encryption

Non-recoverable encryption entails situations where the technology used by the service provider does not have access to the content of the information. In this form of encryption, the content of the message cannot be recovered because the service provider or any third party does not have access to the decryption key. Non-recoverable encryption is prevalent in End-to-End Encryption being used by Social Media Applications. In End-to-End Encryption the content of the message is encrypted for both the sender and receiver, unless they have access to decryption keys.

Social Media Applications, which are intrinsically used by individuals for day-to-day communications, employ this technology to offer privacy and autonomy to their customers for a safe and better experience while communicating. Applications such as WhatsApp,[11] Telegram[12] and Signal[13] set off an example of the usage of technology for a wide user base. The beneficiaries of End-to-End encryption are inclusive of government agencies. Notably, the Ukrainian government has demonstrated a growing reliance on Telegram as an official platform for communication during both the Russia-Ukraine War and the COVID-19 pandemic.[14] This highlights the benefits associated with the utilization of end-to-end encryption technologies in facilitating reliable communication channels.

Therefore, the Non-Recoverable technology employed by the Social media application ensures anonymity since the decryption key is unavailable to the service provider and any third party.

PARADOX OF NON-RECOVERABLE ENCRYPTION: GOVERNMENTAL EFFORTS

The significant benefits of employing end-to-end encryption technologies in creating reliable communication channels, as highlighted, are noteworthy. Yet, the flip side of the coin encompasses the drawbacks linked to

[8] 'Comparing BitLocker, FileVault And Encryption On External Disks – What's The Difference' <https://www.micronicsindia.com/comparing-bitlocker-filevault-and-encryption-on-external-disks-whats-the-difference/#:~:text=Both%20BitLocker%20and%20FileVault%20use,encrypt%20certain%20types%20of%20data.> accessed 29 December 2023.

[9] *Justice K.S. Puttaswamy (Retd.), and Anr v Union of India* AIR 2018 SC (SUPP) 1841.

[10] Rishab Bailey, Vrinda Bhandari and Faiza Rahman, 'Backdoors to Encryption: Analysing an intermediary's duty to provide "Technical Assistance"' (2021).

[11] 'About end-to-end encryption' (WhatsApp) < https://faq.whatsapp.com/820124435853543> accessed 25 December 2023.

[12]'Telegram Privacy Policy' (Telegram)<https://telegram.org/privacy?setln=fa#:~:text=Telegram%20has%20two%20fundamental%20principles, and%20feature%2Drich%20messaging%20service.> accessed 25 December 2023.

[13]'Signal Terms & Privacy Policy' (Signal) < https://signal.org/legal/#:~:text=Signal%20utilizes%20state%2Dof%2Dthe, yourself%20and%20the%20intended%20recipients.> accessed 25 December 2023.

[14] Matt Burges, 'When War Struck, Ukraine Turned to Telegram' (2022).

the secrecy and privacy afforded by end-to-end encryption on these platforms. With the widespread accessibility of the internet, such applications have reached the wrong hands, enabling them to disseminate disinformation and rumours, thereby escalating chaos within society. Numerous instances attest to the paradoxical nature of technology, where what was intended as a boon is sometimes manipulated for detrimental purposes.

For instance, according to French Investigators, a group of ISIS had utilised Telegram for coordinating and planning the terrorist attack. Multiple Reports suggest that even WhatsApp has purportedly been employed by such organizations to coordinate attacks, including the bombings in Sri Lanka[15] and Paris.[16] Additionally, instances of Rumours and misinformation have also rampantly increased on such applications.[17]

Government Efforts vis-à-vis Access to Decryption Keys

To combat illicit activities, misinformation, and rumours, governments worldwide, including India, have decided to implement stricter regulations on social media platforms to more effectively monitor and control the third-party content disseminated on these platforms. Despite various global efforts to resolve these issues, no solution has proven fully effective. One proposed solution by government agencies is to gain access to backdoor encryption keys from Social Media Applications for encrypted messages, enabling them to decrypt and decipher which messages contain illicit information.

A backdoor is a covert method of bypassing data authentication or encryption, enabling surreptitious access to information.[18] An example of a legitimate backdoor is when a manufacturer incorporates a mechanism in its software or device for restoring the data.[19] Henceforth, a back-door encryption key is a way, whereby the government has access to the Decryption Key to decrypt the chats or the required data.

A notable instance illustrating this demand occurred in the legal dispute between the Federal Bureau of Investigation (FBI) and Apple Inc., known as FBI v. Apple.[20] In this case, the FBI requested Apple to supply anti-encryption software to access data on an iPhone. Initially, Apple refused, citing concerns about customer privacy. Despite a court directive, Apple contested the order. Notably, the FBI later revealed it had acquired a third-party solution, obviating the need for Apple's involvement.

The never-ending resolute of governments across the world to gain backdoor entry to Encrypted messages has again become relevant. United Kingdom’s government drafted the Online Safety Bill which attempts to

[15] *ibid.*
[16] *ibid.*
[17] Nic Newman, Richard Fletcher, Anne Schulz, Simge Andı, and Rasmus Kleis Nielsen, ‘Reuters Institute Digital News Report 2020’ Reuters Institute for the Study of Journalism, p.19.
[18] Kim Zetter, ‘Hacker Lexicon: What Is a Backdoor?’ (2014).
[19] Donald L. Buresh, ‘The Battle for Backdoors and Encryption Keys’ (2021) p.22.
[20] *Apple v FBI* 2015 C.D. Cal.

assault the End-to-Encryption prevalent in the social applications.[21] The Bill has noble aims however, the method to approach the same may lead to privacy intrusions for the customers. The Bill's objective to enforce age verification through government documents, biometric data, or facial scans poses a grave threat to individual privacy.

The privacy intrusion due to the bill could be such that Wikipedia has claimed that it will withdraw from the United Kingdom, if necessary.[22] Leading social media applications like WhatsApp[23] and Signal[24] have asserted their intention to exit the United Kingdom instead of compromising encryption as stipulated in the Bill.

Similarly, the United States drafted the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2022,[25] which attempts to penalise companies for not breaking end-to-end encryption. Similar to the United Kingdom's Bill, this act also penalises companies for not scanning CSAM content, making it necessary for them to break end-to-end encryption. Security experts have unequivocally and unambiguously opposed the Government's access to Encrypted Communication as it can wreak havoc on citizens' innate privacy.[26]

Indian Government's Mandate: Compliance at the stake of losing the Intermediary Status

To counteract the rumours, illicit activities and misinformation the government of India has since long established a web of rules and regulations to impose stricter regulations on Intermediaries. Intermediaries are Social Media applications which act as a platform for users to communicate.

Information Technology Act, 2000[27] is the grundnorm of the other regulations that have been drafted by the Government of India for regulating the third-party content on Social Media Platforms (herein referred to as intermediary). According to Information Technology Act, 2000[28] (herein referred to as the Act), an intermediary is any person who on behalf of another person receives, stores or transmits that message or provides any service concerning that message, under section 2(1)(w) of the Act.[29] Further, under section 79(1) of the Act,[30] an intermediary is granted an exemption from any third-party information, data, or

[21] Joe Mullin, 'The U.K. Government Is Very Close to Eroding Encryption Worldwide' (2023).

[22] Dan Milmo, 'UK readers may lose access to Wikipedia amid online safety bill requirements' (2023) *The Guardian.*

[23] James Vincent, 'WhatsApp says it will leave the UK rather than weaken encryption under Online Safety Bill' (2023).

[24] Chris Vallance, 'Signal would 'walk' from UK if Online Safety Bill undermined encryption' (2023) *BBC News.*

[25] Eliminating Abusive and Rampant Neglect of Interactive Technologies Act, 2022.

[26] Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, and Daniel J. Weitzner, 'Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications' (2015) Computer Science and Artificial Intelligence Laboratory Technical Report.

[27] The Information Technology Act, 2000 (21 of 2000).

[28] *ibid.*

[29] The Information Technology Act, 2000 (21 of 2000) s 2(1)(w).

[30] The Information Technology Act, 2000 (21 of 2000) s 79 (1).

communication link made available or hosted by him. The exemption provided is subject to section 79(2) of the Act.[31]

The provision requires an intermediary to act as a host,[32] and not initiate transmission or select or receiver of transmission.[33] Furthermore, under section 79(2)(c) of the Act,[34] An intermediary is required to observe due diligence and to observe guidelines as may be prescribed. Thereby, if an intermediary need to take protection from third-party content on the website by using the *'safe harbour provision'* under section 79(1) of the Act,[35] it is required to follow due diligence and guidelines as may be prescribed.

The guidelines, in the form of Rules, to be followed by Social Media Intermediaries are enacted by the Central Government of India, through the power conferred by sections 87(1)(z) [36]and 87(2) (zg)[37] of the Act. The Rules are Information Technology Rules (Intermediary Guidelines and Digital Media Ethics Code) 2021[38] *(IT Rule 2021),* Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 and Information Technology (Procedure and safeguards for blocking for access of information by Public) Rules 2009[39] (*'IT Rules, 2009'*).

The Primary bone of contention between the Government and the Intermediaries in India is the IT Rules 2021. Section 7 of the IT Rules 2021,[40] clearly notifies that a failure to follow these rules by the intermediary would lead to the forfeiture of its protection under Section 79(1) of the Act[41] which, conclusively, rips the intermediary off its status of an intermediary in the country. Hence, an Intermediary is mandatorily required to follow the stipulated regulations to gain the status of an Intermediary.

This legislation triggered a dispute between the government and social media applications. Notably, the Indian government opted to withdraw Twitter's Intermediary status due to non-compliance with the IT Rules, 2021,[42] specifically regarding the appointment of statutory officers.[43]

Significantly, Rule 4 of IT Rules 2021,[44] stipulates 'Additional due diligence' that must be adhered to by Significant Social Media Intermediaries[45] (*SSMIs)*. SSMIs are intermediaries with over 50 lakh registered

[31] The Information Technology Act, 2000 (21 of 2000) s 79(2).
[32] The Information Technology Act, 2000 (21 of 2000) s 79(2)(a).
[33] The Information Technology Act, 2000 (21 of 2000) s 79(2)(b).
[34] The Information Technology Act, 2000 (21 of 2000) s 79(2)(c).
[35] The Information Technology Act, 2000 (21 of 2000) s 79(1).
[36] The Information Technology Act, 2000 (21 of 2000) s 81 (1)(z).
[37] The Information Technology Act, 2000 (21 of 2000) s 87 (2) (zg).
[38] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
[39] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.
[40] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) r 7.
[41] The Information Technology Act, 2000 (21 of 2000) s 79(1).
[42] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E).
[43] Sowmya Ramasubramanian, 'Reports of witter losing intermediary status is based on incorrect reading of the law: Internet Freedom Foundation' *The Hindu* (New Delhi 16 June 2021) <https://www.thehindu.com/sci-tech/technology/internet/reports-of-twitter-losing-intermediary-status-is-based-on-incorrect-reading-of-the-law-internet-freedom-foundation/article61811195.ece> accessed 222 December 2023.

users.[46] Under Rule 4(2) of the IT Rules, 2021,[47] SSMIs are mandated to facilitate the identification of the *first originator* of information on their computer resources as deemed necessary by a judicial order from a Court of Competent Jurisdiction or an order issued under Section 69 of the Act[48] by the Competent Authority as outlined in the IT Rules, 2009.[49]

The introduction of Rule 4 in the IT Rules 2021 highlights the government's intention to trace the original perpetrators of misinformation or illicit activities. However, this requirement has led to legal and technical challenges for intermediaries, who are caught between upholding their intermediary status and protecting the privacy of millions of users. The following section will address these challenges focusing on the aspects of privacy and technical feasibility.

EXPLAINING THE PRIVACY CONUNDRUM VIS-À-VIS LEGAL AND TECHNICAL IMPLICATION

The IT Rules, 2021,[50] stipulates that the SSMIs should facilitate the identification of the first originator. However, the Intermediaries have challenged the IT Rules 2021 and the government's order due to Legal and Technical irregularities. Intermediaries such as WhatsApp have vociferously denied traceability[51] and have challenged the legality of Rule 4(2) of IT Rules 2021,[52] before the Delhi High Court. In the present section, the same shall be enlisted while explaining the dilemma of the Intermediaries.

Technical non-feasibility of the Government Order under Rule 4(2) of the IT Rules, 2021

The primary contention raised by intermediaries is that to identify the originator of a message, in accordance with Rule 4(2) of IT Rules of 2021 by the governmental order, they are required to trace the message through every individual chat to which it has been forwarded. In the process of tracing a message, intermediaries are required to scan and intercept messages, a task rendered impractical due to the implementation of end-to-end encryption.

End-to-end encryption utilises unrecoverable encryption technology, as elucidated earlier, wherein even service providers lack access to decryption keys. The absence of decryption keys on the part of the service

[44] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) r 4.

[45] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) r 2(v).

[46] Ministry of Electronics and Information Technology, 'Notification CG-DL-E-26022021-225497' <https://www.meity.gov.in/writereaddata/files/Gazette%20Significant%20social%20media%20threshold.pdf> accessed 24 December 2023.

[47] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) r 4.

[48] The Information Technology Act, 2000 (21 of 2000) s 69.

[49] The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rule, 2009, G.S.R. 781(E).

[50] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) r 4(2).

[51] WhatsApp, 'What is traceability and why does WhatsApp oppose it?' <https://faq.whatsapp.com/1206094619954598> accessed 20th December 2023.

[52] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) r 4(2).

provider implies the impossibility of message recovery. The keys are essential for message decryption to reside on the user's device rather than with the intermediary. Thus, the interception and reading of messages by service providers is not possible in the first instance.

Legal Challenges concerning Rule 4(2) of IT Rules, 2021

The primary criticism with Rule 4(2) of the IT Rules, 2021,[53] is that it is claimed to violate Articles 21 and 19 of the Constitution of India,[54] which protect the Right to Privacy and the Right to Freedom of Expression, respectively.

Violation of Article 21: Right to Life and Privacy

Article 21 of the Constitution of India[55] guarantees the Right to Life, which has been interpreted to include the right to privacy. The right to Privacy can be construed positively and negatively.[56] The former deals with the aspect when the State has to intervene and provide the facilities so that a person's right to privacy is ensured, while the latter deals with the concept when the State is not allowed to interfere with the personal sphere of an individual.

This right was affirmed in the landmark judgment of *Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors*[57]. Rule 4(2) of the IT Rules, 2021[58] which mandates that SSMIs enable the identification of the first originator of information on their platforms. This requirement raises significant privacy concerns because it would necessitate the interception and scanning of all messages to trace the originator, thus infringing on users' privacy.

A four-pronged test was laid down by K.S. Puttaswamy which has to be fulfilled to determine whether the action by the State is proportional or is in violation of the Right to Privacy, which has been articulated from the work of David Bilchitz's, who is a distinguished Fundamental rights and constitutional law scholar. It is categorised into the following prongs:

There has to be the existence of a legislation and for the formulated legislation, there has to be a legitimate State Aim. Furthermore, there has to be a Rational Nexus between the impugned method and the Aim. Additionally, the impugned measure should be the Least Restrictive Method and equally efficient. Lastly, there should be a balance between the benefits to be attained and the rights which are infringed.

[53] *ibid*.
[54] The Constitution of India, 1950 Arts 21 and 19.
[55] The Constitution of India, 1950 Art 21.
[56]Lok Sabha Secretariat, 'Right to Privacy' (*Lok Sabha Secretariat Internet,* 2017) <https://loksabhadocs.nic.in/Refinput/New_Reference_Notes/English/Right%20to%20Privacy%20as%20a%20fundamental%20Right.pdf> accessed 1 Feb 2024.
[57] *Justice K.S. Puttaswamy (Retd.) and Anr. v Union of India and Ors* (2017) 10 SCC 1.
[58] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), r 4(2).

Rule 4(2) of IT Rules, 2021[59] satisfies the first prong of the test, i.e., there is a Legislation. The second prong, i.e., Legitimate State Aim is also justified by the State because the originator is required in scenarios where there has been a disturbance in public tranquillity and order. However, the rational nexus between the Aim and the Method is absent. This can be construed as for rational nexus the action of the State needs to be least restrictive, should not be disproportionate and the balance between the benefits and rights which are infringed should be maintained.

However, in the present case, if SSMIs are required to break end-to-end encryption to trace the originator, it would entail that decryption keys are held by service providers for millions of users' chats. This creates a significant risk of misuse and interception by malicious actors, such as scammers.

Despite any justified aim behind the request, such as maintaining public order, breaking end-to-end encryption is not the least restrictive measure available. This approach could have a chilling effect, not only compromising individuals' privacy but also impinging on their freedom of speech and expression. Additionally, breaking encryption is technologically infeasible as SSMIs do not possess the decryption keys necessary for this task.

Moreover, Rule 4(2) of IT Rules, 2021[60] stipulates that *"No SSMI 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."* [61]The government's order to trace the originator would require SSMIs to scan and intercept messages, directly contravening this stipulation and leading to a breach of the right to privacy protected under Article 21 of the Constitution.[62]

Violation of Article 19: Right to Freedom of Expression

Article 19 of the Constitution of India[63] guarantees the Right to Freedom of Expression. Rule 4(2) of the IT Rules, 2021,[64] by imposing the obligation on SSMIs to trace the originator of messages, indirectly curtails this freedom. The fear of being traced can lead to self-censorship among users, thereby hampering free expression of the users.

In the case of *K.A. Abbas v Union of India* the Supreme Court recognized that the "*freedom of expression can be curtailed if regulations are reasonable and serve a legitimate purpose, but it also stressed that excessive control could infringe upon the freedom guaranteed under Article 19(1)(a)*"[65] This was further solidified in the case of *S. Rangarajan Etc vs P. Jagjivan Ram* where the Supreme Court held that

[59] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), r 4(2).
[60] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) r 4(2).
[61] *ibid.*
[62] The Constitution of India,1950 Art 21.
[63] The Constitution of India,1950 Art 19.
[64] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) r 4(2).
[65] *K.A. Abbas v Union of India* (1970) 2 SCC 780.

"*Restrictions on freedom of expression must be reasonable and proportionate. Excessive controls which unduly restrict free expression violate the fundamental right under Article 19(1)(a).*"[66]

The present act of Government to trace the originator of the message, controls and restricts the freedom of expression by creating a chilling effect on users' willingness to communicate freely and openly on intermediary platforms. Thus, in line with the principle established in K.A. Abbas v Union of India, although the IT Rules, 2021 serve a legitimate purpose, excessive control could infringe upon the freedom guaranteed under Article 19(1)(a) of the Constitution of India.

Procedural Safeguards under IT Rules, 2009

The IT Rules, 2009 [67]lay down procedural safeguards that must be followed when an order under Section 69 of the Act[68] is issued by the Competent Authority for interception, monitoring, or decryption. Rule 4(2) of the IT Rules, 2021 states, *"by a judicial order passed by a court of competent jurisdiction or an order passed under section 69 by the Competent Authority as per the Information Technology (Procedure and Safeguards for interception, monitoring and decryption of information) Rules, 2009."*[69]

Technological Infeasibility, Legislative Intent, and Privacy Concerns

The legislative intent behind Rule 4(2) of the IT Rules, 2021,[70] is that any order passed by the Competent Authority must align with the IT Rules, 2009. Intermediaries have made it clear that they do not have control over the decryption keys for the messages sent on their platforms.

Rule 13(3) of the IT Rules, 2009[71] stipulates that *"Any direction of decryption of information issued under Rule (3) to an intermediary shall be limited to the extent the information is encrypted by the intermediary or the intermediary has control over the decryption key."* This provision clearly states that an order requiring an intermediary to decrypt information is limited to cases where the intermediary possesses the decryption key.

In this instance, Social Media Intermediaries, such as WhatsApp, do not have access to or control over the decryption keys, preventing them from decrypting the information. An order demanding that an intermediary decrypt messages, which they are unable to do due to the lack of a decryption key, contravenes the procedural safeguard outlined in Rule 13(3) of the IT Rules, 2009.[72]

[66] *S. Rangarajan Etc v P. Jagjivan Ram* 1989 SCR (2) 204.

[67] The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, G.S.R. 780(E).

[68] The Information Technology Act, 2000 (21 of 2000) s 69.

[69] *ibid.*

[70] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) r 4(2).

[71] The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, G.S.R. 780(E) r 13 (3).

[72] *ibid.*

Therefore, the order to trace the originator of the message under Rule 4(2) of IT Rules, 2021 is not technologically feasible due to unrecoverable encryption. In arguendo, if technologically feasible it will lead to a violation of the Right to Privacy because millions of chats will be at the helm of access by the government and Intermediaries. Further, the order of Rule 4(2) of IT Rules, 2021 procedural safeguards of IT Rules, 2009[73] apply to such orders or not.

EMPLOYMENT OF ALTERNATIVES TO RESOLVE THE CONUNDRUM

Indian Technical and Legal minds have raised substantive alternatives for the Intermediaries to fulfil the demand of the Government Orders, however, the same proposition is still sub judice before the Courts. Furthermore, there are certain existing legal principles which may help in fulfilling the demands of the Government. In this section, we shall analyse the same.

Existing Alternatives for the Government

For instance, the metadata from a messaging service could be used to trace the origin of a message. This metadata refers to the data collected by intermediaries about individual users of the social media application. For instance, WhatsApp[74] collects various types of data, including account registration information, transaction data (if you use their services), and your IP address, among other details outlined in their Privacy Policy.

Intermediaries can share this metadata with government authorities, allowing them to trace both the sender and recipient of messages, as well as access relevant user information. However, the amount of data collected by different applications varies. For instance, Signal collects minimal data, only retaining information such as the registration date and the last date on which the numbers were active.[75] Consequently, this approach is not a viable solution for tracing the origin of messages because the amount of data available differs significantly between applications.

Proposed Alternatives by Experts

Although there appears to be no compromise between government security concerns and WhatsApp's privacy protections, Dr. V Kamakoti, a Professor of Computer Science and Engineering at IIT Madras, has proposed a potential solution. In his technical report, Dr. Kamakoti presents a strategy for achieving both end-to-end encryption and traceability of the original sender of a message. He outlined this approach in a

[73] The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, G.S.R. 780(E).

[74] 'About end-to-end encryption' (WhatsApp) < https://faq.whatsapp.com/820124435853543> accessed 25 December 2023.

[75] 'Signal Terms & Privacy Policy' (Signal) < https://signal.org/legal/#:~:text=Signal%20utilizes%20state%2Dof%2Dthe,yourself%20and%20the%20intended%20recipients.> accessed 25 December 2023.

filing to the Madras High Court, aiming to balance traceability with the confidentiality guaranteed by encrypted messaging services. However, WhatsApp has since challenged the feasibility of this proposed solution.

Dr. Kamakoti outlines two ways to trace the first originator of a message. The first method is to make the originator visible to everyone who sends or receives the message. The second method encodes the originator's information so only the platform can access it. Kamakoti identifies two key factors: whether a message can be forwarded and identifying the original sender. He proposes that the message creator should decide if a message is "forwardable" or "not forwardable." If it is "forwardable," the originator's information is included with the message. If it is "not forwardable," the person who forwards the message becomes the new originator.

Each receiver will know the originator information

This recommendation suggests including the originator's information with the message itself. For example, if A creates a message and sends it to B and C, both B and C will receive the message along with information about A, the original sender. If B forwards the message to D and E, and C forwards it to F and G, each new recipient will also see the originator's information from A. If the message was about something like a bombing, this method would allow us to trace it back to A, the original sender. Each person who receives the message will see who started it as it continues to be forwarded.

Attaching Encrypted Originator Information with each message

The second idea is similar but focuses on adding the originator's information to each message and encrypting it so only the service provider can read it. In this method, the service provider holds a special key to decrypt the originator's information included in the messages. If needed, the service provider can reveal the originator's details to authorities with a valid court order. The encrypted originator information travels with the message as it gets forwarded.

For example, if A creates a message and sends it to B and C, the originator information from A is encrypted using a public key and sent to B and C along with the message. When B forwards the message to D and E, and C forwards it to F and G, they receive the message with the encrypted originator information of A, which they cannot decrypt because the private key is held by the platform. If the message is found to be threatening or illegal, the Law Enforcement Agency can request it, and WhatsApp can use the private key to decrypt the originator information and provide it to the authorities.

Limitations of the Proposed Alternatives

The proposed solution of Dr. V. Kamakoti has been severely criticised for multiple shortcomings. Senior Advocate Kapil Sibal, WhatsApp's counsel stated, "If you open up the encryption, there is no platform."[76] The main purpose of encryption or encoding a message is compromised by the theory proposed by Dr. V. Kamakoti.

Dr. Manoj Prabhakaran, a computer science professor at IIT Bombay, submitted an expert analysis to the Madras High Court for the Internet Freedom Foundation, arguing that Dr. V. Kamakoti's traceability recommendations for WhatsApp would compromise user privacy and discourage free expression[77]. He argued that Dr. Kamakoti's claims are not practical, even if modified, because a phone number doesn't provide strong identification. Phone numbers can be easily obtained using fake identities or apps like Google Voice, Skype, and Viber. He also warned that adding a digital signature to every message would discourage people from freely expressing themselves.

Furthermore, the theory assumes that only public key cryptography, which was developed in 1976, can be used for both encrypting and decrypting messages. However, as discussed earlier, WhatsApp employs a more advanced Signal Protocol that uses both symmetric and public key cryptography, discarding encryption keys after each use. Furthermore, varied legal experts claimed that the concept of end-to-end encryption is violated the instant anything is sent along with every communication that WhatsApp can trace.

WhatsApp also highlighted several concerns. For instance, they pointed out that non-state actors might use modified versions of the app, potentially leading to innocent individuals being implicated during investigations targeting the app's creators. Modified versions of apps, often downloaded from the internet rather than official app stores, are becoming increasingly common and may include features selected for user convenience. Official developers, including WhatsApp, find it nearly impossible to deactivate these modified versions.

Furthermore, WhatsApp, Facebook Messenger, Skype, and Google, among others, use the Signal Protocol. This protocol is designed to simulate a private whisper, where the recipient knows the content of the message but cannot verify the identity of the sender. Therefore, adding information like a phone number or ID about the message's originator would not be sufficient evidence in a court of law, as it cannot prove that the claimed sender delivered the message.

[76] Aditi Agrawl, 'IIT Madras's Kamakoti Tells MediaNama How WhatsApp Traceability is Possible without Undermining End - to-End' *MediaNama* (8 August 2019) < https://www.medianama.com/2019/08/223-kamakoti-medianama-whatsapp-traceability-interview/> accessed 19 December 2023.

[77] Aditi Agrawal, 'Traceability and end-to-end encryption cannot co-exist on digital messaging platforms: Experts' *Forbes India* (16 March 2021) <https://www.forbesindia.com/article/take-one-big-story-of-the-day/traceability-and-endtoend-encryption-cannot-coexist-on-digital-messaging-platforms-experts/66969/1> accessed 19 December 2023.

Conclusively, the prevailing situation has led to a stalemate between the State and the Intermediaries, bringing the state of affairs back to square one. Technologically, no feasible solution has been identified thus far. In a hypothetical scenario, granting the capability to trace the originator by compromising end-to-end encryption could pose a significant risk to the privacy rights of millions, giving rise to concerns about the establishment of a "surveillance state."

To conclude, the ongoing conflict between the State and the Intermediaries has resulted in a standstill, bringing the situation back to a neutral stance. Technological solutions that balance traceability with privacy have not yet been identified. If a solution were found that compromised end-to-end encryption to enable originator tracing, it could endanger the privacy of millions and raise concerns about creating a “surveillance state.”

GROWING DATA PRIVACY CONCERNS VIS-À-VIS THE DIGITAL DATA PROTECTION ACT, OF 2023

The Government of India’s effort to demand access to the decryption key has been coupled with the enactment of the Digital Data Protection Act, of 2023[78] (herein referred to as DPDP Act, 2023). While the Data safety of millions of users is at the helm of being accessed by service providers and government agencies, the Government of India, in the backdrop, has enacted these legislations which have significantly raised public concerns.

Digital Personal Data Protection Act, of 2023

DPDP Act, 2023[79] was brought in to set a standard for data protection in times of major uprisings of cyber-attacks, and the introduction of the Act has wavered things southwards. The DPDP Act, of 2023 stipulates the Intermediaries as Data Fiduciaries. Under Section 8(1) of the DPDP Act,[80] there is an obligation on the Data Fiduciary to comply with the provisions of the Act. This unequivocally mandates the Fiduciary to comply with all the provisions of the Act. Amongst others, the Data Fiduciary must protect the Personal Data of the Data Principal.[81]

The DPDP Act, of 2023 enlists numerous provisions as procedural safeguards which are required to be followed by Data Fiduciaries before collecting the Data of users. These procedural Safeguards such as mandatory consent act as a sigh of relief for users of such platforms. However, Section 17(2) of the DPDP Act,[82] declares that the provisions of this Act do not extend to an instrumentality of the State established by the State Government in the interest of the sovereignty, security, integrity, friendly relations with foreign

[78] The Digital Personal Data Protection Act, 2023 (22 of 2023).
[79] *ibid.*
[80] The Digital Personal Data Protection Act, 2023 (22 of 2023) s 8(1).
[81] The Digital Personal Data Protection Act, 2023 (22 of 2023) s 17(2).
[82] *ibid.*

states, maintenance of public order, or prevention of incitement to any cognizable offence related to these concerns.

The exclusion of the provisions of the entire act implies that all the procedures and safeguards outlined for obtaining the consent of the Data Principal (User) or provisions for safeguarding Data Protection do not apply to the State Instrumentality when it engages in processing and analysing the data of individuals. The blanket exemption amounts to an excessive and arbitrary power given to the Instrumentality, and it shall certainly lead to a violation of the Right to Privacy of the citizens under Article 21 of the Constitution.[83]

Furthermore, Section 36 of the DPDP Act, 2023[84] enlists, *"The Central Government may, for the purposes of this Act, require the Board and any Data Fiduciary or intermediary to furnish such information as it may call for".* The State machinery, while exercising power under the section can have access to "*any such information as it may call for".* Such exemptions provided under the DPDP Act, 2023[85] have intensified citizens' fears about their data safety.

The government should reconsider multiple stakeholders concerning such blanket exemptions. It is imperative to narrow the broad exemption granted to the government instrumentalities under the DPDP Act, 2023[86] to safeguard the concerns of the citizens. Additionally, the government should reassess and employ various features from the Data Protection Jurisprudence, which has made significant strides in several countries worldwide.

The Model Law of Data Privacy, the General Data Protection Regulation (herein referred to as GDPR)[87] provides limited powers to the Government. The GDPR plays a crucial role in addressing privacy concerns and safeguarding personal information. Its objective is to enhance and harmonize data protection for all European Union citizens and to set standards for how global businesses manage the personal data of their customers.

Article 23 of the GDPR,[88] grants the government the authority to "process personal data for the prevention, investigation, detection, or prosecution of criminal offences, or the execution of criminal penalties, including measures to safeguard and prevent threats to public security, national security, and the protection of individuals' rights and freedoms. However, this power can only be exercised if it "respects the essence of fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society."

[83] The Constitution of India, 1950 art 21.
[84]The Digital Personal Data Protection Act, 2023 (22 of 2023) s 36.
[85] *ibid.*
[86] The Digital Personal Data Protection Act, 2023 (22 of 2023).
[87]The European General Data Protection Regulation, 2016 (679 of 2016).
[88]The European General Data Protection Regulation, 2016 (679 of 2016) art 23.

Furthermore, in the United Kingdom, the Data Protection Act[89] was enacted in 2018, and although there exists an exemption for the governmental authorities in scenarios concerning national defence and security, the data processed for such purposes is under strict surveillance for its fair use. The Investigatory Powers Act of 2016[90] governs activities such as government agencies collecting personal records in bulk for intelligence and law enforcement purposes.[91]

To protect the privacy and personal rights of its people it further provides the provision for the Secretary of State, or the Home Minister, to issue a warrant for such action, which needs judicial commissioner permission beforehand. It is necessary to determine the necessity and proportionality of such acts and retention of data after the warrant's expiration is limited. In addition, this statute establishes parliamentary supervision.

The Government could also consider the enlisted safeguards for the citizens' data in Justice B.N. Shri Krishna Committee's Report.[92] The report from the proposed committee emphasized user rights and the responsibilities of data fiduciaries, including the State. Central to the report's recommendations is the concept of informed consent for data sharing. Additionally, the report advocated for the principle of privacy by design for data processors and provided definitions for key terms such as consent, data breach, and sensitive data. The report underscores two critical aspects: first, the primary value of any data protection framework should be privacy; and second, such a framework must also consider other important values, including collective interests.

The Report also proposed the establishment of a Data Protection Authority (DPA) which aimed to oversee and enforce the provisions of the Act, ensuring a fair and transparent process. As government agencies will also be data fiduciaries under this Bill, the DPA will be governed by a board that includes six full-time members and a chairperson, all appointed by the Central Government based on recommendations from a selection committee. This committee will comprise the Chief Justice of India or her nominee (a Supreme Court judge), the Cabinet Secretary of India, and a distinguished expert.

Incorporating this proposal into amendments to the DPDP Act of 2023 is crucial. Currently, the Central Government alone has the authority to appoint members of the Data Protection Board. Such amendments are essential to address concerns with the DPDP Act, which, at first glance, aims to uphold the 'Right to Privacy.' However, its current provisions grant substantial and unchecked power to governmental entities.

[89] The Data Protection Act, 2018 (c. 12).

[90] The Investigatory Powers Act, 2016 (c. 25)

[91] *ibid* pts 6,7 and 8.

[92] Justice B.N. Shri Krishna Committee, *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians* (2018) 10.

Therefore, the DPDP Act, of 2023[93] introduces substantial data protection measures but also contains provisions that might undermine citizens' privacy rights, particularly through broad exemptions for state instrumentalities. Compared to international standards like the GDPR[94] and recommendations from the Justice B.N. Shri Krishna Committee,[95] The Act's approach to granting power to the state and data protection authorities could be improved by incorporating more stringent safeguards and achieving a better balance between privacy and collective interests.

CONCLUSION AND SUGGESTIONS

The current research conclusively addresses various questions regarding the interplay of law and technological advancement globally and particularly within the framework of the Indian regime. Governments across the world are grappling with challenges posed by social media applications. Intermediaries providing end-to-end encryption offer absolute anonymity to users' chat content. Consequently, this technology has been misused by non-state actors, such as terrorists, for planning illicit activities. Government agencies have experienced severe loss of life, property, and resources, due to the utilization of such technology.

In response to this, these agencies have requested information about the originator or content of messages used for communication by various organizations. However, Intermediary Platforms have collectively asserted that they employ unrecoverable encryption methods, making it impossible to identify or provide the government with the content or originator of the messages. Also, attempting to dismantle end-to-end encryption is argued to infringe upon the privacy rights of millions of users, as it puts all users' data at risk of misuse.

Furthermore, the possession of a backdoor encryption key by the government introduces several significant challenges. Primarily, the grant of access to such keys to numerous agencies will inevitably create a high demand for such keys to resolve issues pertaining to the respective agencies which would create a floodgate situation where the security of both encrypted chats and the backdoor encryption will itself be jeopardised. The extensive dissemination of these keys amongst law enforcement personnel poses a risk to confidentiality.

Secondly, there is a critical concern regarding the volume and quality of data accessible to the government through these keys. The complexity intensifies in situations involving disinformation disseminated across multiple devices, necessitating the government to decrypt every chat through which the misleading message was circulated to identify the source, raising profound privacy and security concerns.

[93] The Digital Personal Data Protection Act, 2023.

[94] The European General Data Protection Regulation, 2016 (679 of 2016).

[95] Justice B.N. Shri Krishna Committee, *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians* (2018) 10.

Lastly, data protection by government agencies throughout the globe is a great question to be resolved by the government. In 2023, data of 2,37,000 U.S. government employees was hacked from the government sites.[96] There are other reports which highlight the level of intrusion faced by the government agencies.[97]

In India, the Government and Intermediaries have faced a deadlock concerning the demand of the government to find the originator of the messages. The government's order under Rule 4(2) of IT Rules, 2021[98] mandates the facilitation of the Originator of a message by Social Media Application. However, the Intermediaries have vociferously challenged the legality of Rule 4(2) of IT Rules, 2021[99] and denied the technical possibility of fulfilling the government's order. The same shall lead to the loss of their "Intermediary" Status.

Against the backdrop of this perplexing situation, the Indian government enacted the Digital Data Protection Act of 2023.[100] This legislation incorporates various safeguards, including the requirement of unanimous consent from the Data Principal, and the responsibilities of Data Fiduciaries and Data Processors. However, the government has granted blanket exemptions under Sections 17(2) and 36 of the DPDP Act of 2023[101] to government instrumentalities from the entire procedural safeguards outlined in the legislation. This development has heightened concerns among numerous scholars.

The Government of India should reassess the concerns of multiple stakeholders involved in the process. This could be substantially achieved by amending the provisions of the act in accordance with Data Protection Jurisprudence across the world, such as EUGDPR and the United Kingdom's Data Protection Act and in accordance with the principle of data safety as has been incorporated in the B.N. Shri Krishna Report.

Therefore, the Government of India must address the conundrum to ensure that users can utilize apps with maximum safety and confidence. The existing stay between intermediaries and the government impacts not only the rights of businesses to operate in the country but also the privacy and freedom of speech and expression of citizens. The demand for backdoor encryption keys by the government should not come at the expense of compromising the right to privacy and the freedom of speech for millions of individuals.

****

[96] David Shepardson, 'Data of 237,000 US government employees breached' (2023).

[97] David Shepardson, 'Data of 237,000 US government employees breached' (2023).

[98] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) r 4(2).

[99] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) r 4(2).

[100] The Digital Personal Data Protection Act, 2023 (22 of 2023) s 17(2)(a).

[101] *ibid.*