Justice and Law Bulletin (JLB)
January-April, 2024 [Vol.3, Issue 1], pg.34- 46, www.apricusjournals.com

Fortifying India's Digital Landscape: Encryption as the Pillar of Privacy, Freedom, and Cybersecurity

Anamika Singh[1,*]

Abstract

This article inquires about the critical role of encryption in safeguarding the Indian digital ecosystem. As the country rapidly digitizes, the need for robust cybersecurity measures becomes paramount. Encryption emerges as a fundamental pillar, supporting privacy, freedom of expression, and national security in the digital realm. The paper examines how encryption protects individual citizens' data from unauthorized access, preserves journalistic integrity, and secures sensitive government and corporate information. It also addresses the challenges faced by law enforcement and intelligence agencies in balancing security concerns with digital rights. The author reviews India's current encryption policies and highlights areas for improvement. Additionally, it discusses the economic implications of strong encryption for India's growing IT sector and its potential to attract foreign investment. The paper concludes by proposing a framework for a comprehensive national encryption policy that harmonizes individual rights, economic growth, and national security interests. By embracing encryption as a cornerstone of its digital infrastructure, India can position itself as a leader in the global digital economy while safeguarding the freedoms and security of its citizens.

Keywords: *encryption, privacy, cyber security, traceability*
Author for Correspondence* email id. anamika.singh@nusrlranchi.ac.in

Introduction

In an era where digital interactions form the backbone of personal, professional, and governmental activities, the importance of robust cybersecurity measures cannot be overstated. India, with its rapidly expanding digital economy and growing internet user base, faces unique challenges and opportunities in safeguarding its digital frontier. At the heart of this endeavour lies encryption—a powerful tool that ensures the confidentiality, integrity, and authenticity of data.

Encryption serves as the bedrock of privacy, enabling individuals to communicate and transact securely without fear of unauthorized access or surveillance. It is also a cornerstone of free speech, allowing citizens to express themselves freely and confidentially in the digital realm. Furthermore, encryption is vital for national security, protecting sensitive information from cyber threats and ensuring the resilience of critical infrastructure.

Former British Prime Minister William Pitt presented one of the most powerful arguments in defence of privacy against government interference in 1763: "*The poorest man may in his cottage, bid defiance to all the forces of the Crown. It may be frail, its roof may shake; the wind may blow through it; the storm may enter; the rain may enter, but the King of England may not enter; all his force dare not cross the threshold of the ruined tenement*." India is steadily making its way to embrace digital transformation, and the role of encryption in fortifying the nation's digital landscape has become increasingly critical. By prioritizing encryption, India

[1] Student, National University of Study and Research in Law, Ranchi, Jharkhand, India

can build a secure, private, and free digital environment that fosters innovation, protects individual rights, and strengthens national security.

The objective of this article is to add to the ongoing discussion about encryption in India by demonstrating why proposals that compromise communications security and encryption should be rejected because they will not accomplish the intended goals and will instead seriously jeopardise cybersecurity, free speech, privacy, and the economy.

The first section of this article gives the background information about encryption. By giving a synopsis of the significant developments in encryption over the previous thirty years, the second section clarifies the evolution of encryption policy in India. The third section analyses changes to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which impose a requirement that communications carried on certain messaging services be traceable to their source. "*It demonstrates how a traceability mandate would undermine encryption, fall short of the objective of halting the dissemination of false information, and fail to satisfy the standards of the proportionality test that the Supreme Court recently established in its ruling that the Indian Constitution's guarantee of privacy is a fundamental right.*" In conclusion and recommendations, the author presents arguments in favour of safeguarding and promoting encryption due to its significance for maintaining privacy in the face of widespread surveillance, its link to both economic growth and national security, and its requirement for respecting human rights.

Demystifying Encryption: A Background

Sensitive data is being kept electronically in more and greater quantities in the digital age. This growth is exponential. Data such as location, bank account information, private chats, and medical and biometric records are just a few of the numerous instances that are now easier to obtain than in the past. This trajectory's side effects include grave worries about online security and privacy. In addition to pushing many businesses and educational institutions into remote locations, the COVID-19 pandemic has increased demand for digital data by promoting technologies meant to combat the virus. This has exacerbated related privacy issues and increased the need for data security measures like encryption to safeguard people, governments, and the economy.

Data security and privacy are maintained by encryption. It is the process used in cryptography where data is "locked" and made incomprehensible to an unauthorised recipient; the message is then decrypted and converted back into plain text by the authorised recipient using a "key". Stated differently, encryption jumbles legible text or files so that only the sender and the intended recipient can decipher the contents. It shields information from unwanted access, maintains the privacy and validity of data on the internet, and offers a number of other user protections. Encryption rebalances user power with that of other parties, who usually have more authority, by guaranteeing users' choice over who can access their data. Encryption is widely utilised on most communication platforms and is present in the majority of banking applications and credit card payment terminals.

Data in transit and storage are both safeguarded by encryption. End-to-end (or "E2EE") encryption is among the safest types of encryptions. E2EE guarantees that the information transferred can only be viewed by the sender and the intended receiver, as well as any intermediaries like the communication service provider.

According to Indian IT law, encryption is "*the process of transforming plaintext data into an unintelligible form (cipher text) such that the original data cannot be recovered without the use of an inverse decryption process (two-way encryption) or cannot be recovered at all (one-way encryption)*."

"India does not have any laws relating to encryption, yet. It is mostly governed by the Information Technology Act, 2000 (often known as the "IT Act") and sector-specific rules. The Indian government's stance on encryption has changed over the past few decades, with some recent changes reflecting the government's belief that encryption presents a barrier for government institutions."

Literature Review

1. Basu, Subhajit and Jones, Richard, (2005) 'Indian Information and Technology Act 2000: review of the Regulatory Powers under the Act', International Review of Law, Computers & Technology, noted that The Information Technology Act of 2000 in India, influenced by the Model Law on E-Commerce from UNCITRAL, aims to legally recognize digital transactions and promote alternatives to paper-based communication and information storage. However, this legislation has drawn criticism for its heavy-handed approach to regulating Certificating Authorities. In this article, the authors delve into the Act's provisions, particularly those related to jurisdiction, crime, and privacy. "An act to provide for the legal recognition of transactions carried out by... alternatives to paper-based methods of communication and storage of information" sums up the main points of the Act in its lengthy title. The writers examined the "heavy-handed" approach the Indian government used to regulate certifying authorities in a prior essay. This study builds on that assessment by analysing the Act's provisions for a number of jurisdiction, criminality, and privacy-related issues. Unlike similar laws in other countries, the Indian Act introduces e-commerce and Internet-related criminal offenses, potentially impacting privacy and free speech rights for citizens both within India and beyond.

2. Nandita Mathur, 'What was the Draft Encryption Policy and Why it was Withdrawn?' (*LiveMint*, 22 September 2015)
This article highlighted how The Department of Electronics and Information Technology (DEITY) unveiled a draft encryption policy and it was met with criticism from the media and online community, who expressed worries about privacy and government overreach. The government removed it and requested that the DEITY redraft it in light of the concerns. "User shall reproduce the same Plain text and encrypted text pairs using the software/hardware used to produce the encrypted text from the given plain text," states the new draft encryption policy. According to the terms of the national laws, the relevant B/C (business/citizen) company must keep all information for ninety days following the date of the transaction and make it available to law enforcement agencies upon request.

3. Gurshabad Grover, Tanaya Rajwade & Divyank Katira, in the "Ministry and the Trace: Subverging end-to-end Encryption", 2021 noted that with end-to-end encrypted messaging, people can have private discussions without worrying about governments or businesses interfering. The Indian government has ordered online messaging providers to allow the identities of message originators across various platforms in order to facilitate monitoring and criminal prosecution. This article demonstrates how the various implementations of this "traceability" mandate—such as removing end-to-end encryption, hashing messages, and appending originator information to messages—come at a significant cost to privacy, security, and usability. We argue that traceability violates the fundamental right to privacy and goes

beyond the purview of delegated legislation under the Information Technology Act based on a legal and constitutional analysis.

4. Anirudh Burman and Prateek Jha in "Understanding the Encryption Debate in India" noted that The use of encryption to safeguard the privacy and security of internet communication has grown controversial. The past ten years have seen a rapid digitalisation that has resulted in the growth of both local and international online communication services that employ encryption. As a result, law enforcement agencies (LEAs) and national security entities face issues. In February 2021, the Indian government issued new regulations to address these issues.

Large social media platforms must allow traceability, or the capacity to reveal information about the source of online messages, in order to comply with these requirements. Because traceability would necessitate breaking the end-to-end encryption used by many online communication platforms, like WhatsApp, the security of online communications on such platforms would be compromised. For this reason, technology companies and privacy activists have opposed such a move.

However, this traceability mandate is merely the most recent development in a protracted, heated discussion about the use of encryption. The struggle to uphold stricter standards of internet security versus enacting new regulations to allow security agencies and law enforcement agencies (LEAs) technological exemptions is not unique to India. In the United States, public resistance prevented the government's initial attempt to circumvent encryption protections with a court order, leading to one of the first meaningful conversations on the subject in the 1990s. Analysts should take into account pertinent factors like (but not limited to) whether such changes will offer law enforcement officials the access they desire, how the security of encrypted communications will be affected, and how citizens' civil liberties will be affected, among others, in order to weigh the relative benefits and drawbacks of the Indian government's proposal.

5. Dr. Marco Gercke, in his report titled "Understanding Cybercrime: A Guide for developing countries" explains that the first of the seven strategic goals of the ITU Global Cybersecurity Agenda (GCA), which calls for the development of strategies for the creation of cybercrime legislation that is globally applicable and interoperable with current national and regional legislative measures, is addressed in the publication Understanding Cybercrime: A Guide for Developing Countries. It also discusses the ITU-D Study Group Q22/1 approach to organising national cybersecurity efforts. A national cybersecurity strategy must include the establishment of the necessary legislative framework. Achieving global cybersecurity primarily requires all nations to enact relevant laws prohibiting the misapplication of ICTs for illegal or other purposes, including actions meant to compromise the security of their vital information infrastructures. Threats can come from anywhere in the world, thus international cooperation, investigative support, and standard substantive and procedural rules are all necessary to address these issues, which have an international dimension. For this reason, it's critical that nations co-ordinate their legal systems in order to combat cybercrime and promote global collaboration.

The Policy Terrain and Emerging Trends of Encryption in India

In India, technology policies regarding encryption started to take shape in the 1990s. The Indian government passed the IT Act as a result of the expansion of online intermediaries, e-commerce, electronic banking, and electronic communication. A framework of regulations governing the virtual marketplace was established by the IT Act, which also brought in a number of criminal crimes relating to e-commerce and the internet.[2] The Act supported the safe flow of data and funds via Public Key Infrastructure (PKI), an encryption mechanism used for cybersecurity.[3] But as the Reserve Bank of India (RBI) acknowledged in its guidelines for online banking, PKI and other advanced encryption technologies were not widely accessible in India at the time.[4]

"In order to guarantee security in online banking, the RBI suggested 128-bit Secure Socket Layer (SSL) encryption as a substitute for PKI. Additionally, the Securities Exchange Board of India suggested using this standard by default for e-commerce.[5] But later on, government worries that encryption might prevent access to data by the government were mirrored in the direction that encryption policy took. The Indian Telegraph Act, 1885 (often known as the "Telegraph Act"), the IT Act, and sector-specific laws currently outline the regulatory environment with regard to encryption simultaneously. These regulations aim to define the acceptable level of encryption, allow government agencies to decrypt data, and need decryption help in order for the government to obtain access."

With effect from 2009, the IT Act was modified to permit the central government to specify the encryption techniques or protocols for e-governance and e-commerce.[6] In the interest of defence, national security, and sovereignty as well as the maintenance of public order or the investigation of a crime, another amendment permitted the federal and state governments to monitor, intercept, or decrypt communications.[7] Government agencies must receive assistance from service providers and subscribers in order to obtain data in this way.[8] "The Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009 (also known as the "Decryption Rules") were passed by the government that same year."

The guidelines and protocols for decryption are outlined in the Decryption Rules[9]. Since "decryption assistance" is defined as helping to "allow access, to the extent possible, to encrypted information," end-to-end encrypted platforms may fall beyond the purview of these regulations.[10] The government may order the decryption of "*any information as is sent to or from any person or class of persons or relating to any particular subject*" under the Decryption Rules.[11] Therefore, the clause covers a broad range of data and opens the door for indiscriminate or non-targeted decryption orders. Furthermore, the opportunity for reviewing the government's use of such unilateral power is greatly reduced by the Decryption Rules, which mandate that documents relevant to decryption orders be destroyed within a set six-month period. National security is a common justification used by the government for decryption orders.[12]

[2] Subhajit Basu and Richard Jones, 'Indian Information and Technology Act 2000: Review of the Regulatory Powers under the Act' (2005) 19(2) Intl Rev L Comp & Tech, 209, 219.

[3] IT Act 2000, s 3.

[4] Committee on Internet based Securities Trading and Services, *First Report* (SEBI 2000) 6-7.

[5] *Id.*

[6] Information Technology Act, 2000, s 84-A.

[7] *Id.*

[8] The Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009.

[9] Information Technology (Procedures And Safeguards For Interception, Monitoring Or Decryption Of Information) Rules, 2009.

[10] *Id.*

[11] The Decryption Rules, rule 2(g)(i).

[12] The Decryption Rules, rule 23.

In India, encryption was first openly presented as being incompatible with national security in the wake of the 2008 Mumbai terror attacks. Since the government was unable to keep an eye on the content shared on RIM's BlackBerry devices, the government had previously threatened to ban RIM from the Indian market.[13] The government's hostility against encryption was further heightened by the revelation that the terrorists had used BlackBerry devices.[14] Following protracted talks, RIM consented to site BlackBerry servers in India and gave the government access to user data received over its messaging service; however, government data transferred over BlackBerry Enterprise Server systems was not intercepted.[15] Users' privacy was consequently compromised due to worries that encryption could jeopardise national security.

The first effort at a comprehensive encryption policy was made by the central government seven years later. It published a draft National Encryption Policy in 2015, but it was quickly withdrawn in response to harsh criticism about governmental overreach and privacy concerns from a variety of groups. There were other problematic provisions in the draft.[16] For example, it created serious cybersecurity issues by requiring users and organisations to keep plain text copies of encrypted communications for ninety days. Furthermore, all users and businesses could be forced to use the government-specified key length and algorithm for encryption technologies, which would prevent users from selecting stronger standards and businesses from coming up with new security measures. In an effort to lessen some of the harm, an addendum was released. The encryption policy's updated draft, however, has not yet been made public.

The Intermediary Rules: The Clash between Traceability and Encryption

The Information Technology (Intermediaries Guidelines and Digital Media Ethics Code) Rules, 2021 (the "New Intermediary Guidelines"), which modify India's intermediary liability laws, have brought encryption to the forefront most recently—and perhaps most problematically.[17] These rules represent a significant turning point in the nation's technological policy development and could signal more regulation of encryption due to its perceived inability to facilitate government access to data. The largest democracy in the world's economy will be impacted by the implementation, which will also partly determine whether technology advances or impedes fundamental freedoms and rights. The introduction of the New Intermediary Guidelines was ostensibly done to stop criminals and "anti-national elements"

[13] Damien McElroy, 'Mumbai attacks: Terrorists Monitored British Websites using BlackBerry Phones' (*The Telegraph*, 28 November 2008) <https://www.telegraph.co.uk/ news/worldnews/asia/india/3534599/Mumbai-attacks-Terrorists-monitored-coverage-on- UK-websites-using-BlackBerry-phones-bombay-india.html> accessed 20 April 2024

[14] Sahil Makkar & Shauvik Ghosh,'India Renews Threat toban BlackBerry Services'(*LiveMint*, 29 July 2010) <https://www.livemint.com/Home-Page/H0ZmePNYWQk7Tv6NkNAefK/India-renews-threat-to-ban-BlackBerry-services.html>accessed 20 April 2024.

[15] Apurva Chaudhary, 'BlackBerry's Tussle with Indian Govt Finally Ends; BB Provides Interception System' (*Medianama*, 10 July 2013) <https://www.medianama. com/2013/07/223-blackberrys-tussle-with-indian-govt-finally-ends-bb-provides-intercep- tion-system/> accessed 20 April 2024.

[16] 'FAQ: Legal Position of Encryption in India' (*SFLC.in*, 11 November 2017) <https://sflc.in/ faq-legal-position-encryption-india> accessed 12 November 2020; Nandita Mathur, 'What was the Draft Encryption Policy and Why it was Withdrawn?' (*LiveMint*, 22 September 2015) <https://www.livemint.com/Politics/RZtAGhM6IjDBWujiK6ysEP/What-was-the- encryption-policy-and-why-it-was-withdrawn.html> accessed 21 April 2024.

[17] Comments Invited on Draft of Intermediary Guidelines 2018' (*Ministry of Electronics & Information Technology*, 2018) <https://www.meity.gov.in/comments-invited-draft-inter- mediary-rules> accessed 21 April 2024.

from misusing social media and to stop fake news from spreading online. These are unquestionably significant issues that affect legal systems throughout.

The New Intermediary Guidelines replace the previous 2011 rules that intermediaries (like social media platforms) had to follow under the IT Act. Failure to comply with those guidelines could make intermediaries ineligible for the legal protection or "safe harbor" under Section 79 of the IT Act, which exempts them from liability for third-party content as long as certain conditions are met. End-to-end encryption limits how much platforms can moderate content, so this liability protection is crucial for them to operate and for users' free expression.

In 2018, a draft amendment proposed making intermediaries trace any content's origin if required by the government. This "traceability" requirement would undermine encryption and threaten privacy, security and free speech, as companies may over-comply to avoid liability. Despite opposition during public consultation, the new rules make "significant social media intermediaries" (over 5 million Indian users) and any designated intermediary enable tracing the "first originator" of any information via court order or under Section 69, for offenses against security, public order, etc. However, tracing orders cannot be passed if other less intrusive means are available, messaging content need not be disclosed, and the first Indian originator counts if the global first originator is outside India.[18]

In the event that certain requirements are met, the traceability provision requires SSMIs and other intermediaries designated by the government to facilitate the identification of the "first originator" of any information that may be required by a judicial order or an order passed under section 69 of the IT Act.[19] Section 69 gives the Federal and State governments, or any of their designated representatives, the authority to order any government organisation to keep an eye on, intercept, or decrypt data.[20]

For the purpose of preventing, detecting, investigating, prosecuting, or punishing an offence, or inciting an offence, relating to the state's sovereignty, integrity, and security, foreign relations, public order, rape, sexually explicit material, or child sexual abuse material, an order requiring the identification of the first originator must be passed.[21] Violation of this order could result in a minimum of five years in prison. Additionally, Rule 4(2) specifies that a traceability order shall not be passed and that compliance with an order shall not necessitate the "significant social media intermediary" ("SSMI") disclosing the content of any message if other, less invasive methods of identifying the originator are successful. Lastly, for the purposes of this provision, the first originator located in India will be considered the first originator even if the first originator is located outside of India.[22]

[18] Ministry of Electronics and Information Technology, Notification Dated 25 February 2021 <https://www.meity.gov.in/writereaddata/files/Gazette%20Significant%20social%20media%20threshold.pdf> accessed 18 April 2024.

[19] Nojeim, Greg; Maheshwari, Namrata; and Miglani, Eduardo (2021) "Encryption in India: Preserving the Online Engine of Privacy, Free Expression, Security, and Economic Growth," Indian Journal of Law and Technology: Vol. 17: Iss. 1, Article 2. DOI: 10.55496/LPNZ6069 Available at: https://repository.nls.ac.in/ijlt/vol17/iss1/2

[20] Dr. Prabhakaran, On a Proposal for Originator Tracing in WhatsApp, *Antony Clement Rubin v Union of India* 2018 SCC OnLine Mad 13519, *see*: <https://drive.google.com/file/d/1B2ShWywwVpPX1zTz25UgPMSOokZbcJBx/view>

[21] Supra note 28.

[22] Government notifies Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021' (*Ministry of Information & Broadcasting*, 25 February 2021) <https://www.pib.gov.in/PressReleseDetail.aspx?PRID=1700766> accessed 18 April 2024.

The Encryption Conundrum: How Traceability Requirements Compromise Security With the development of technology, encryption has enabled a wide range of important financial and commercial services as well as the fulfilment of a fundamental human need: the ability to speak without being overheard. Law enforcement organisations and governments, however, frequently see the usage of encryption, especially E2EE, as contributing to a "going dark" issue, whereby data is hidden in ways that limit the government's access to it. Encryption "backdoors," which would enable governmental bodies and law enforcement organisations to evade the authentication procedure and eavesdrop on encrypted communications, have been demanded by governments worldwide.

The New Intermediary Guidelines effectively provide intermediaries a Hobson's choice: they can choose to be held legally responsible or keep design elements that promote security and privacy. It is blatantly anti-democratic to penalise platforms for selecting to put users' rights and freedoms first.

Government representatives arguing that the New Intermediary Guidelines do not compromise encryption are likely to use the third clause in the traceability section of the guidelines. It says that "no significant social media intermediary shall be required to disclose the contents of any electronic message in order to comply with an order for identification of the first originator."[23] There isn't much comfort in this clause regarding the integrity of the encrypted message.

First, government representatives typically need to already have access to the pertinent message's content if they are trying to identify the original sender of a problematic message. Second, there's a difference between saying intermediaries don't have to 'disclose' a message's content and saying they don't have to 'access' it at all.

The second caveat, which says that if there are less intrusive ways to identify the information's originator, no tracing order shall be granted, is likewise insufficient to constitute a significant restriction. This restriction is in effect while the order is being issued by a court or a duly authorised government body.[24]

These authorities would not benefit from hearing from experienced professionals or the intermediary that would have to abide by the order, as they lack the technical know-how to decide whether other, less invasive procedures are possible. No opportunity is given to an intermediary to propose less intrusive alternatives. As a result, this restriction has little practical use and is unlikely to significantly lower the number of such requests that are approved.

If the only practically possible way to comply with a traceability requirement is to build a new mechanism that allows access to end-to-end encrypted communication, then a more relevant constraint would exempt SSMIs from doing so. The traceability requirement cannot be fully implemented by tagging the information of the originator, using alpha-numeric hashes, or employing other techniques involving digital attribution through signatures attached to each message88 and increased metadata collection and storage. These methods are also susceptible to misuse and impersonation by malicious actors. As a result, inaccurate attributions may arise. Moreover, the traceability mandate outlined in the New Intermediary Guidelines would

[23] Dr. Prabhakaran, On a Proposal for Originator Tracing in WhatsApp, *Antony Clement Rubin v Union of India* 2018 SCC OnLine Mad 13519.

[24] Supra note 28.

compromise encryption even in situations where the government does not require access to message content.

Adding features that allow for the access to and storing of additional data on users and their communications is tantamount to adding vulnerabilities that leave private information open to unwanted access by outside parties. Whether intentional or not, the end result will be a general weakening of the privacy and security features that are the cornerstones of E2EE platforms that enable secure communication, as well as an erosion of the data minimization principle as platforms are forced to track and store more data.

No matter how intermediaries' systems are redesigned to meet the traceability requirement, encryption will suffer as a result, and technology will be diverted from formats that prioritise privacy and adhere to data-minimization standards. Such privacy-by-design architecture would have to be drastically altered in order to comply with the traceability mandate, which would also reveal previously private information to service providers of E2EE platforms and maybe other parties.

Compromising Security: The Downside of Traceability Requirements

Once the ability to trace communication threads is created by weakening encryption, there is no failsafe way to ensure only the intended party (service provider or government) can exploit the traceability mechanism. Requiring a capability for government access to encrypted online information essentially mandates insecurity. End-to-end encrypted platforms keep information secure indiscriminately from all third parties, including the platform creator, providing robust privacy protection. Introducing any vulnerability significantly increases the risk of data breaches and malicious attacks. Weakening internet security to supposedly strengthen national security is counterproductive and contradicts the guidelines requiring intermediaries to reasonably secure information. Additionally, the assumption that the government is universally a "good" actor is flawed - repressive regimes often surveil citizens, and encryption offers freedom from such surveillance. Traceability would empower repressive regimes to identify anyone interacting with dissenting or protest-encouraging messages, regardless of context. Particularly in a democracy, the right to privacy is inextricably linked to fostering freedom of expression and inclusive growth.

Traceability vs. Right to Privacy: Navigating the Conflict of Rights

The traceability requirement, by permanently attributing an identity to private communications, would jeopardize internet users' fundamental rights to privacy and freedom of expression under the Indian Constitution. Anonymity, privacy, and free expression are inextricably linked and instrumental to a healthy democratic society. Anonymity enables people to debate controversial subjects without fear, and the internet revolutionized enabling anonymity. The perception of lack of privacy has a chilling effect on free expression, and imposing traceability will inevitably lead to this undesirable outcome. Claiming to want traceability without compromising encryption or privacy is disingenuous - traceability inherently comes at the cost of privacy and encryption, even if just through metadata.

A traceability mandate would need to pass the four-pronged proportionality and necessity test established by the Supreme Court in the Puttaswamy case because of its inevitable detrimental effect on the right to privacy[25]. The Court unanimously held that the right to privacy is an inalienable natural right inherent to life and liberty under Article 21 and the fundamental rights

[25] (2017) 10 SCC 1.

in Part III of the Constitution. As a natural right not bestowed by the State, privacy cannot be taken away. Any statute infringing this inalienable privacy right without countervailing public interest would be void.

The proportionality and necessity test as outlined by the court:[26]
(i) the action must be sanctioned by law; (ii) the proposed action must be necessary for a democratic society for a legitimate aim; (iii) the extent of such interference must be proportionate to the need for such interference; and (iv) there must be procedural guarantees against abuse of such interference. If such interference satisfies a "pressing social need," is proportionate to the legitimate objective pursued, and the justifications offered are "relevant and sufficient," it is deemed "necessary in a democratic society" in pursuit of that legitimate aim. Essentially, the test's goal is to find a balance between an individual's interests and the interests of the public.

On a critical review, it can be argued that the traceability requirement in the New Intermediary Guidelines does not comply with the standards outlined in the Puttaswamy ruling on privacy rights by the Supreme Court. One could argue that it is not a proportionate or necessary measure to achieve the goals of avoiding fake news, maintaining law and order, or safeguarding national security.

Drawing from European Court of Human Rights jurisprudence cited in Puttaswamy, for a restriction to be "prescribed by law" it must be adequately accessible and formulated with sufficient precision to enable reasonable foreseeability of consequences[27]. The traceability provision lacks this precision - the circumstances for government demanding originator tracing and procedural requirements are not clearly defined with adequate limitations. This makes it an opaque provision devoid of reasonable predictability and safeguards.

The least invasive and most effective course of action is required if at all there is a necessity. On both counts, the traceability mandate is ineffective. First, its effectiveness is questionable - the originator is not necessarily the content creator, sender signatures can be spoofed, discerning malicious intent is dubious, and it attributes culpability devoid of sharing context. Further, it could force some providers to abandon end-to-end encryption, exposing users while malicious actors simply use other encryption methods.

Second, it is an extremely intrusive measure undermining anonymity essential for fear-free communication. It could require providers to attach sensitive originator fingerprints/hashes to each message that create new vulnerabilities.

Moreover, it disproportionately threatens all internet users' privacy and chills free expression by undermining anonymity, without demonstrating how it would practicably achieve its aims. Lawmakers must consider if identifying some bad actors is worth imperiling constitutional rights of millions. It fails the "necessary in a democratic society" test without proportionality or sufficient justification.[28] Crucially, there are no meaningful safeguards - no limiting conditions, notice requirements, or adequate judicial redress mechanisms for affected

[26] (2017) 10 SCC 1 [180-81].

[27] Judgment in the *Sunday Times v United Kingdom*, No. 6538/74, 26 April 1979, para 49.

[28] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (22 May 2015) A/HRC/29/32.

individuals. The severe harms to the fundamental privacy right far outweigh any hypothetical benefits.

The government seems intent on pushing traceability and weakening encryption, as seen in recent statements with Five Eyes nations. Whether enshrined in law remains to be seen, but the Supreme Court's evolving jurisprudence on the interaction of encryption, traceability and privacy rights will significantly inform the future of encryption in India.

Why Safeguarding Encryption is relevant in contemporary India

It has been felt that the introduction of the idea of monitoring the first inventor under Rule 5(2)[29] is a bit controversial and concerning. It makes it possible for important social media middlemen that offer messaging services to give the enforcement mechanism access to the original source of any content. This is an attempt to stop the dissemination of false information and illicit actions occurring via messaging services. Cyber experts worry that this might eventually lead to end-to-end encryption being bypassed, making it possible for a surveillance state to be established. Major privacy breaches are what most messaging apps take pride in, and this one could be their undoing.

In order to prevent or look into an offence pertaining to the sovereignty, integrity, or security of the State, the authority to follow the originator may also be imposed. What the Rules don't address is the unfathomable potential for abusing such a broad and discretionary jurisdiction.

Furthermore, the media community highlights how the Rule's application erodes the right to free speech. In examining the grievance redressal system, the administration has the power to determine whether media material is appropriate through the Oversight Mechanism. This is a novel approach that could be interpreted as going beyond the bounds of the Constitution.

It may not be in the best interests of free speech and journalistic freedoms for the interministerial committee of bureaucrats to decide cases pertaining to these rights. Without the safety of encryption, people would be reluctant to send or receive private messages online if they suspect they are being watched. As such, human expression is restricted to the realm of what is seen appropriate through the surveillance lens.

Encryption allows for a safe space protecting users' rights to privacy and free expression. It prevents them from becoming vulnerable to unfettered surveillance and malicious or repressive actors.[30] It preserves communicational privacy (restricting access to communications), intellectual privacy (freedom to develop ideas without monitoring), and informational privacy (secrecy, anonymity, control over information).

Recommendations

1. Enact robust legislation to protect strong encryption standards: The Indian government should enact comprehensive legislation that enshrines the right to use and implement strong encryption protocols without fear of legal repercussions. This would send a clear signal that India values privacy, free speech, and cybersecurity.

[29] The Information Technology (Intermediaries Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 5, cl. 2.

[30] Supra note 28.

2. Foster public-private collaboration on encryption policies: The government should actively engage with the private sector, civil society organizations, and technical experts to develop encryption policies that strike the right balance between national security concerns and individual privacy rights.

3. Invest in cybersecurity education and awareness: To promote responsible encryption use, India ought to fund cybersecurity awareness and education initiatives aimed at the general public, corporations, and governmental organisations. This could include initiatives to improve digital literacy and train professionals in encryption best practices.

4. Support open-source encryption projects and research: The government should allocate funding and resources to support open-source encryption projects and academic research in the field of cryptography. This would not only enhance the security of Indian digital infrastructure but also contribute to global advancements in encryption technologies.

5. Promote international cooperation on encryption standards: India should actively participate in international forums and discussions surrounding encryption policies and standards. This would allow India to share its perspectives, learn from other nations' experiences, and contribute to the development of global encryption norms.

6. Establish clear guidelines for lawful access to encrypted data: While respecting the importance of encryption, the government should establish clear and transparent guidelines for lawful access to encrypted data in cases involving national security threats or serious crimes. These guidelines should be subject to robust oversight and accountability mechanisms to prevent misuse.

7. Encourage the adoption of end-to-end encryption: The Indian government should actively encourage the adoption of end-to-end encryption in various sectors, including messaging applications, cloud storage services, and online communication platforms. This would significantly enhance the privacy and security of digital communications for individuals and businesses.

8. India can position itself as a leader in the realm of digital privacy, free speech, and cybersecurity, while fostering an environment conducive to innovation, economic growth, and the protection of fundamental rights.

Conclusion

Policies that could jeopardise encryption, such as the traceability mandate, are being proposed to address serious issues including “fake news,” child sexual abuse material, crimes against national security, public order, and sexually explicit material. The proposals get credibility and immediacy from these goals. Proposals that, if implemented, would break encryption with the stated goal of accomplishing any such goal, however, are more rhetorical than practical. Undermining encryption is not simply an ineffective solution to any of these issues; on the contrary, it has detrimental effects on cybersecurity, human rights, the public interest, and the economy.

The internet realm is no longer a supplement to society's offline realities. Rather, we conduct our social and political lives over the internet. We exercise our freedoms and liberties there. Governments, groups, and people can all have a private online space that is protected from both known and unknown risks of manipulation and spying thanks to encryption. People can interact and work together to create a democratic society that is enhanced rather than undermined by the pervasiveness of technology. The fundamental principles of a democracy, the right to privacy and the right to free speech, need the preservation and enhancement of encryption.

Regarding encryption and its effects on security and privacy, Carissa Véliz of Oxford University makes the following observations about privacy: "Social decisions regarding privacy will impact how political campaigns are conducted, how corporations make money, the authority that governments and private enterprises may possess, the progress of medicine, the pursuit of public health objectives, the risks we face, the ways in which we interact with one another, and lastly, whether our rights are upheld in the course of our everyday lives." The way the government handles encryption will have a significant impact on the rights and liberties that contribute to India's current state of democracy.

Strong encryption must be supported and encouraged if the nation and the government are to secure cyberspaces, preserve individual liberties and rights, and foster technological innovation and economic prosperity. Put simply, the costs to society of having weaker encryption standards are too great.

In today's digital age, encryption has become the cornerstone of online privacy, free expression, and cybersecurity. As India continues its rapid digitalization journey, it is imperative that the nation upholds strong encryption standards to protect the fundamental rights of its citizens and foster an environment conducive to innovation and progress.

The ongoing debate surrounding encryption policies has far-reaching implications that extend beyond individual privacy concerns. A weakened encryption regime could jeopardize the security of critical infrastructure, cripple the growth of the digital economy, and undermine India's position as an emerging global technology hub.

Striking the right balance between national security interests and safeguarding civil liberties is a delicate task, but it is one that must be approached with utmost care and foresight. By embracing robust encryption protocols and promoting a culture of responsible encryption use, India can cement its position as a leader in the digital realm, while upholding the democratic values enshrined in its constitution.

Ultimately, the preservation of encryption is not just a matter of technological convenience; it is a fundamental necessity in preserving the online engine of privacy, free expression, and security – the bedrock upon which a thriving digital society is built. India's future as a global technological powerhouse hinge on its ability to navigate this crucial issue with wisdom and unwavering commitment to the principles of democracy and individual liberty.

CITE THIS ARTICLE: Ms. Anamika Singh, Fortifying India's Digital Landscape: Encryption as a pillar for Privacy, Freedom and Cybersecurity, Justice and Law Bulletin, 3(1), pp. 34-46, (2024).