V. ANALYSING THE INTERPLAY BETWEEN END-TO-END ENCRYPTION & PRIVACY: SYMBIOTIC ASSOCIATION OR A MERE FACILITATION?

- Ayush Raj[*]

ABSTRACT

"Privacy is an inherent human right, and a requirement for maintaining the human condition with dignity and respect."- Bruce Schneier

Encryption is a safety wall that protects the confidentiality of data from outside snooping. End-to-end encryption is an integral feature of digital privacy that empowers users to hold their private conversations with themselves without any external interference. Though end-to-end encryptions are not fool-proof, yet they provide the safest structure for data security. With the Central government mandating social media intermediaries to reveal private conversations and their originators for curbing hate speeches, and cyber frauds, and to accelerate cyber patrolling and surveillance, privacy concerns in India have burgeoned. An argument to justify the need for a fragile nature of encryption stems from the restriction posed to enforcement and investigation agencies in conquering digital frauds, piracy, online hate speeches, terror activities, etc. Therefore, it is pertinent to re-evaluate the data protection regime in the country that resonates with the need for individual privacy and balances itself with the obligations of national security and a safe online environment. In this article, at the very outset, the author discusses the history of encryption in India and the landmark Puttaswamy judgment that revitalized the encryption debate in the country. The author, further, deals with the question that whether there is any legally enforceable right of encryption in light of different sector-specific guidelines and the new Data Protection Bill. The paper also delves into the privacy concerns ensuing from weakening encryption and excessive governmental regulation in this regard. In a nutshell, the paper holistically deals with the pros and cons of evading encryption and the author is of the view that personal privacy must not be compromised in any manner and suggests exploring alternative ways to deal with online crimes and ensure online safety rather than breaching encryption arbitrarily.

[*] The author is a third-year student of B.A. LL.B. (Hons.) at Maharashtra National Law University, Nagpur. Views stated in this paper are personal.

I. INTRODUCTION

Encryption is a process of converting plain data into a code, i.e, an unintelligible form that cannot be recovered, and if recovered, would require special arrangements.[1] End-to-end encryption ensures that any third party is restricted to access personal data, thereby ensuring strict confidentiality and privacy in online conversations and transactions. End-to-end encrypted messages can be accessed only by the sender and the receiver and it is coded in the form of a cipher text in transit.[2] The debate surrounding encryption status is of paramount significance because enabling encryption is enabling data privacy while controlling encryption is controlling data flow. What we need is a balance between these extremes that can happen through pre-determined cautious regulation of encryption. It is because there is an imminent need to protect an individual's privacy and at the same time be cognizant of the necessities of law enforcement. The motive should be to safeguard personal interests as well as national interests and therefore, a defined regulation of data and a concrete framework for sharing of personal data becomes quintessential. Pertinently, this regulation must not swing on the docks of executive discretion. Regulating the extent of encryption in a digital ecosystem lands us on the critical question of determining the extent of

[1] Schedule V, Information Technology (Certifying Authorities) Rules, 2000.
[2] Abdalbasit Mohammed & Nurhayat Firal, 'A Review Paper on Cryptography' (7th International Symposium on Digital Forensics and Security, Barcelos, June 2019).

government surveillance on digital service providers. Another intriguing factor, as the supporters of strong encryption claim, is the categorization of activities that would permit enforcement agencies to snoop on someone's private affairs under the pretext of national security.[3]

Encryption, as the proponents of regulating encryption, argue, acts as a digital shield to a host of illicit activities on the web ranging from data breaches and cyber frauds to child pornography and inciting violence.[4] On the other hand, it is also important to note that encryption is not a universal go-to measure for ensuring privacy and confidentiality because many cloud storage firms such as Google need access to unencrypted data, therefore, end-to-end encryption is currently impracticable since it might significantly degrade the present user experience.[5]

In light of the aforesaid and due to the recent policy altercations with respect to governing privacy, in India and worldwide, it is imminent to engage in discussions regarding personal privacy the data protection. This paper seeks to serve such a purpose and present a multi-dimensional analysis of this bone of contention. The author has adopted a streamlined approach to discuss the status quo of the Indian data protection regime and suggest measures for strengthening privacy as well as aiding state authorities. He has also attempted to predict the fate of encryption based on recent developments. The paper at the very beginning provides an overview of the Indian encryption regulations

[3] Trisha Ray, 'The Encryption Debate In India: 2021 Update' (*Carnegie Endowment for International Peace*, 31 March 2021) <https://carnegieendowment.org/2021/03/31/encryption-debate-in-india-2021-update-pub-84215> accessed 1 June 2022.
[4] ibid.
[5] Google Cloud, *How Google Workspace Uses Encryption To Protect Your Data* (Google Cloud Whitepaper, August 2020).

and based on judicial precedents, explores the right to encryption and traceability. In this context, the author has examined the current data protection laws, identified their loopholes, and presented potential solutions to bridge the gap between the need for fair privacy legislation and the exigency of law enforcement agencies to create a better digital environment. Lastly, the paper highlights some key concerns and tries to come up with some significant considerations that can be looked up to while framing a modern data protection law.

II. INDIAN ENCRYPTION LAW: INTERMEDIARY'S POSITION

The scope of information and decryption requests is limited by Rule 13(3) of the Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009,[6] to the extent that the intermediary has control over the instruments for decryption and information. As a result, the clause, when read in conjunction with the regulations, does not hold intermediaries liable for information that they were unable to get in the first place. Rule 2(g) of the Decryption Rules supports this view, defining "decryption assistance" as enabling access "to the extent practicable, to encrypted information." As a result, the intermediary's responsibilities regarding decryption requests are constrained. This stipulation is especially important in the case of end-to-end encrypted messaging service providers because intermediates do not have access to messages or decryption keys. It is pertinent to highlight these revisions, in the form of Rules and Notifications, in privacy policies as they evidently clarify that the government has increased its regulation, in a phased manner, to curb hate speeches and

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

promote a healthy discourse on digital platforms, and hold the intermediaries liable for the content posted on their platforms and mandate taking down any content, as and when requested by the government in a prescribed time.

A. Puttaswamy Case & Traceability

When we discuss encryption and the legal implications surrounding encryption, we must look toward the decision in *Justice Puttaswamy (Retd.) v. Union of India* (**"Puttaswamy case"**)[7] as a parameter to define the contours of privacy. It is pertinent to analyse and examine the tests put forward by the Apex Court in that case, i.e., any action having any effect on individual privacy must be tested on the grounds of legality, legitimacy, suitability, and necessity. Moreover, the data principal must have adequate safeguards against its exploitation and unwanted decryption.[8]

Coming to legality, it is a settled principle that any executive order must comply with the ingredients of a valid law otherwise it is deemed to be a type of delegated legislation.[9] In this regard, we must first examine whether the government has the lawful authority to intrude into the privacy of an individual by enabling traceability, as privacy has been declared a fundamental and an inalienable natural right under Article 21.[10] The government can only issue content removal orders to intermediaries under Section 69A of the IT Act,[11] and it has no regulatory jurisdiction to authorize any breach of privacy. Section 7 of the Act provides for procedural

[7] *Justice K.S. Puttaswamy and Anr. v Union of India (UOI) and Ors.*, (2017) 10 SCC 1.
[8] ibid.
[9] *E.P Royappa v State of Tamil Nadu and Anr.*, (1974) 4 SCC 3.
[10] *Justice K.S. Puttaswamy and Anr. v Union of India (UOI) and Ors.*, (2017) 10 SCC 1.
[11] The Information Technology Act, 2000 (Act 21 of 2000), s 69.

requirements that are required to be followed by the intermediaries with proper due diligence. Third-party actions are excluded from the ambit of this Section, thus, exempting intermediaries' liability.[12] What is noteworthy, in these Sections is that they impose restrictions on freedom of speech; whether these restrictions possess reasonability or not, can be a matter of discussion, however, they don't allow the government to decode personal conversations in any manner. Therefore, if tested from this parameter, traceability and decryption have a strong case against legality.

That said, one may argue that Section 69[13] provides for government surveillance in certain conditions and they themselves prove the presence of a legitimate state aim and national interest. As discussed, the conditions specified in the Rules are sufficient enough for a legitimate state aim; however, the expansive nature of the Rules and the discretionary power of the executive must be guided by a set of legal principles.

The third test mandated under the Puttaswamy case is that of suitability and necessity and it must be a matter of genuine concern to evaluate whether these measures of decryption could help the government in securing national security, digital safety, and crime control or not.

The criterion for traceability and breaking encryption indicates a state's intent in penalizing creators (originators) while disregarding distributors. It is pertinent to refer to Madras High Court's observation in the case of *S Ve Shekhar v. Inspector of Police*: "the act of forwarding a message amount to accepting and endorsing a message. However, the traceability

[12] Gurshabad Grover, Tanaya Rajwade & Divyank Katira, 'The Ministry And The Trace: Subverting End-ToEnd Encryption' (2002) 14 NUJS L Rev 2.
[13] ibid.

requirement seemingly ignores the culpability of forwarding parties."[14] Thus, the traceability obligation can play a part in developing a culture of impunity in message recipients, who may share the content without critically evaluating it, and still be shielded from the actions of law enforcement agencies as there is an evident loophole in the law. Information recipients play a vital in countering the spread of disinformation and rumours and are able to do the contrary as well, there is a need to balance the position of law that places an equal burden of responsibility on everyone and helps achieve the intended goal. Moreover, when we say that decryption is essential to effectuate actions against cyber frauds or child pornography, there is a lacuna in our approach. This is because, while traceability and decryption might help to find out the originator but they may not help in preventing the propagation of these crimes. The gist of the above argument is to create clarity over the need for traceability to facilitate law enforcement as it does not create any barrier to the crime, but rather only touches a part of surveillance in those cases. Therefore, traceability may not be mandatory in this regard as any common approach cannot be applied to every sort of illegal activity.

III. RIGHT TO ENCRYPTION

Pursuant to the above discussions and descriptions of digital and online privacy, the most important question that pops up is whether there exists any right to encryption in the Indian legal system. In this regard, another parameter that is required to be examined is the scope of the Puttaswamy case on encryption debates. We can reasonably infer, both from the Puttaswamy case,

[14] *S Ve Shekhar v Inspector of Police*, 2018 SCC OnLine Mad 13583.

as well as, by looking at data breaches on various online service providers,[15] that both state and non-state interference can be a potent threat to one's privacy. The Pegasus controversy has interlinked national security and privacy in a novel manner and it also raises serious concerns regarding our privacy legislation.[16]

The terms 'Right to Encryption' and 'Right to Privacy' arise out of the same concept. The state's legal authority to undertake surveillance only goes as far as one's right to privacy. Any governmental action weakening public encryption would be a violation of the right to privacy and would have to pass the Puttaswamy test in order to comply with the Supreme Court's interpretation of the right to privacy.

One may argue that a strong encryption policy protects the right to freedom of speech and expression of an individual and that the power to trace the first originator, as argued, creates conflicts with Article 19. Additionally, one may claim that traceability hinders the independent authority to express on digital platforms as the sender can be subject to unreasonable and biased action against him. It is because one can claim to be in the constant threat of surveillance if it goes against the set norms. However, it is pertinent to note that this connection is flawed because encryption is concerned with privacy and confidentiality rather than free speech. Hence, breaking or weakening

---

[15] Aditi Agrawal, 'Traceability and end-to-end encryption cannot co-exist on digital messaging platforms: Experts' (*Forbes India*, 15 March 2021) <https://www.forbesindia.com/article/take-one-big-story-of-theday/traceability-and-endtoend-encryption-cannot-coexist-on-digital-messaging-platforms-experts/66969/1 accessed> 24 April 2022.

[16] Ankita Shethy, 'Pegasus and the Law' (*Mondaq*, 1 September 2021) <https://www.mondaq.com/india/privacy-protection/1107548/pegasus-and-the-law> accessed 4 May 2022.

encryption cannot be essentially termed an attack on free speech. At this juncture, it is pertinent to mention the Puttaswamy case at the center, as the Apex Court held privacy to be a part of personal liberty under Article 21 instead of making it a subordinate of Article 19. Another striking indicator of a clear distinction between freedom of speech and the 'right to encryption' is the close resemblance of exceptions to free speech under Article 19(1) to exceptions for state surveillance under the Personal Data Protection Bill (**"PDP Bill"**).[17] Therefore, it goes both ways; freedom of speech must not be absolute but the state must also ensure that the privacy of an individual is not infringed which tackles the extended application of 'freedom' of speech.

The Srikrishna Committee[18]on data protection was constituted by the central government to examine the issues of privacy, data protection, and artificial intelligence. The PDP Bill was based on the report of this Committee, which was constituted in response to the Supreme Court's ruling in the Puttaswamy case, in August 2017 and submitted its report in July 2018. The Committee acknowledged the need for de-identification and encryption for data fiduciaries. It explicitly mentioned encryption as a digital safeguard but it didn't lay any proper procedural framework for decryption. While the Committee strongly recommended that the Puttaswamy test must be applied in cases of government surveillance and there must be a proper judicial or legislative supervision over the same; however, it failed to define what valid and lawful decryption is. Moreover, currently, the data protection regime of

[17] The Personal Data Protection Bill, 2019 (Bill No. 373 of 2019).
[18] Committee of Experts under the Chairmanship of Justice BN Srikrishna, *A Free and Fair Digital Economy – Protecting Privacy, Empowering Indians*, (July 2018) 55.

the country lacks the necessary safeguards and shields against any possible exploitation of decryption by the government.

The Committee, however, did not attempt to rectify this flaw in the Personal Data Protection Bill, instead advocated that the Central Government enact new legislation to oversee intelligence collection. According to the committee, any non-consensual access to personal data should be subject to both legislative monitoring and judicial clearance to guarantee both ex-ante and ex post facto responsibility. This advice has yet to be implemented by the executive.

IV. THE PERSONAL DATA PROTECTION BILL: A ROLLER COASTER RIDE

Prior to discussing the PDP Bill, it is important to take cognizance of the formulation of the National Encryption Policy, 2015.[19] This policy was redacted due to massive opposition; however, it is pertinent to mention that the Policy consisted of regulations and protocols for encryption, digital signatures, etc. It stipulated that the encryption service providers should retain the data for a prescribed period of time to facilitate law enforcement. Additionally, it also required that those service providers enter into an agreement with the government for sharing the data.[20] The above two requirements sufficiently clarify the reasons for its withdrawal.

The 2018 version of the Data Protection Bill sought to acknowledge the role of encryption and decryption and attempted to carve their boundaries. The Bill, under Section 42 stipulated that lawful decryption by enforcement

[19] The Draft National Encryption Policy, 2015.
[20] The Draft National Encryption Policy, 2015.

agencies is permitted on account of the 'security of the state' and that decryption must be proportionally just and approved by law.[21] Furthermore, decrypting personal data also came under the ambit of Section 4 which mandated fair and reasonable use of personal data. Sections 29, 30, and 31 deal with maintaining proper transparency and providing adequate security safeguards in cases of processing of personal data by data fiduciary.[22]

A. The 2019 Version

In 2019, a new version of the Bill was submitted, with Section 35 expanding the extent of the immunity granted to government entities for data processing. It gave the government the authority to exclude any or all of its agencies from Bill's restrictions. It removed the words 'necessity' and 'proportionality,' and expanded the grounds to include the "interest of India's sovereignty and integrity, the security of the State, friendly relations with foreign States, and public order; or for preventing incitement to the commission of any cognizable offense pertaining to India's sovereignty and integrity, the security of the State, friendly relations with foreign States, and public order",[23] i.e., aligning with the exemptions under Article 19 and thereby giving more discretionary powers to the government to act upon data protection and privacy.

---

[21] 'Some Points On Lawful Interception Or Monitoring Or Decryption Of Information Through Computer Resource' (*Press Information Bureau, Government of India*, 21 December 2018) <https://pib.gov.in/Pressreleaseshare.aspx?PRID=1556945>.
[22] The Personal Data Protection Bill, 2019 (Bill No 373 of 2019).
[23] ibid.

V. INFORMATION TECHNOLOGY (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS CODE), RULES, 2021: VIOLATING ARTICLE 21

The latest addition to this data protection debate is the Intermediary Guidelines, 2021 which further gave a free hand to the government. It holds the intermediaries liable for the content posted on their platforms and mandate taking down any content, as and when requested by the government in a prescribed time.[24] Permitting the originator of messages exchanged on digital platforms such as WhatsApp and Telegram to be traced and tracked is a violation of the right to privacy, which the Supreme Court declared a fundamental right under Article 21 in the Puttaswamy case. This argument essentially bases itself on the concept that exposing the first originator of a message is tantamount to exposing the privacy of that individual and infringing his right to speech. Tracing the original source in response to an executive or court order might jeopardize the basic right to privacy by interfering with end-to-end encryption of private communication. A comprehensive reading of the Rules also signals the overturning of the *Shreya Singhal* decision, in which the Supreme Court invalidated Section 66-A of the Information Technology Act, 2000, which penalized "offensive" information on the basis of arbitrariness.[25] It is because these guidelines are meant to keep a strict eye on the content being published on social media intermediaries and while Shreya Singhal's judgment sought to create a free online atmosphere, the former tends to bring a multi-layered regulation on online content. It is also important to analyse the judicial trend and the progress of privacy

[24] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
[25] *Shreya Singhal v Union of India*, (2013) 12 S.C.C. 73.

jurisprudence in the country. While some High Courts have partially invalidated these Rules[26] but overall judicial inclination in privacy-related matters tends to be pro-state as the data protection scheme is quite nascent and national interest and integrity are prioritized.

VI. CONCERNS REGARDING WEAK ENCRYPTION

A comprehensive and holistic analysis of the Data Protection when read in consonance with the Intermediary Guidelines, 2021 will lead us to infer that the law wants data protection to be stern and effective but the same law excludes government agencies from its domain. Therefore, there is a clear dichotomy in the government's approach regarding this. Furthermore, the Rules snatch the discretion and flexibility of the intermediaries to allow or disallow a specific content and now the government can mandatorily ask the intermediary to take down any content if the same is interfering with the peace and security of the country.

In light of the above-stated contradiction, there is an imminent need to balance the need for surveillance and to guard the privacy of the citizens. Encryption, in particular, is of paramount significance as the digital economy constantly needs strong vigilance over transactions and communications. So, strong encryption is not only required to protect private conversations on social platforms such as WhatsApp but is equally necessitated for facilitating a hassle-free digital transaction. Master Direction on Digital Payments Security Controls released by the Reserve Bank of India (**"RBI"**) also

[26] *Agij Promotion of Nineteenonea Media Pvt. Ltd. v Union of India, W.P. (L) No 14172 of 2021*; *Nikhil Mangesg Wagle v Union of India,* P.I.L. (L) No 14204 of 2021.

provides for multiple layers of protection such as encryption, authentication, digital certificates, etc.[27]

Another troubling aspect of interfering with the mechanism of encryption is that it is quite complex and any change in this mechanism to lower its standard might attract fraudulent cyber-attacks on it. This concern is specifically problematic as India still lags way behind in ensuring global cyber security protocols.[28] Prior channels that were modified to meet similar government needs ended up being risky and prone to cyber malice, to the point that flaws were exploited for years before they were discovered.[29] By breaching the nondisclosure assurance and making the ingredients of all users' messages perceptible to messaging providers, employees and contractors of the service provider garner unauthorized access to individuals' personal conversations, and a large central cache of extremely sensitive information is created, which might be a tempting target for threat actors. No technology created to enable special access for surveillance and law enforcement has been sufficient to evade generating significant faults so far. There are several other reasons why this selective exemption should not be given effect to. Exemption of every government agency from the scope of the data protection law also strengthens the possibility of political opponents being placed under the

[27] 'Internet Banking In India – Guidelines', (*RBI*, 2001) <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=414&Mode=0> accessed 04 May 2022.

[28] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (*UNHRC* 2015) <https://www.undocs.org/A/HRC/29/32> accessed 04 May 2022.

[29] Bedavyasa Mohanty, 'The Encryption Debate in India' (*Carnegie Endowment for International Peace*, 30 May 2019) <https://carnegieendowment.org/2019/05/30/encryption-debate-in-india-pub-79213> accessed 04 May 2022.

scanner and can aid the government in pursuing its illegitimate political motives.

The government should not compel the service providers to execute traceability rather the focus should be to enact laws that are, in principle, aligned to the concept of data minimalization i.e. states should create laws that force companies to collect the least amount of user information that they need to operate and provide their service.[30] The problem with traceability and decryption is that it contradicts the above principle and therefore, facilitates not just state surveillance, but encourages more private surveillance i.e bad actors with ulterior motives. Hence, the traceability obligation interferes with the security and privacy of the majority sans good cause, ostensibly to apprehend a few malicious activities who can easily cheat these technologies and sustain their activities.

VII. THE WAY FORWARD

Keeping in view the need for a balanced data protection law, an overreaching encryption guideline can be issued that will serve dual objectives. Firstly, it will clear the conundrum regarding encryption and decryption and lay down a procedural framework, and secondly, it will curb the jurisdictional conflict between different regulatory bodies and enforcement agencies that arise due to sector-specific overlapping guidelines. In this regard, introducing a local key for accessing personal data and unlocking encryption can be a useful measure. The main element behind this 'key' is that it should be kept in the device only and therefore, agencies can access the key only

[30] Andrew Grosso, 'Mandatory Key Escrow Encryption – What's Wrong with the Governments Argument in Favor of It' (1999) 14 Crim Just 34.

when they are in possession of the device.[31] This can be implemented to curtail the unlawful decryption of personal data on arbitrary and vague grounds. Moreover, if the Rules intend to curb and restrict hate speeches from spreading through online platforms, it can be interesting to explore and carve out possibilities to trace the first originator of the message without breaking the encryption. In this respect, metadata collected by online platforms can be taken into consideration for surveillance and investigative purposes without breeching encryption. This method is already utilized by several platforms.[32] However, this large-scale use of this metadata is subject to technological and economic viability.

If we compare the data protection laws of India with that of the United States of America (**"USA"**), the European Union (**"EU"**), and Australia, we can easily figure out some similarities as well as differences. The USA doesn't have a nationalized data protection guideline rather it has federal laws and sector-specific guidelines for different industries. Likewise, Australia also has different state privacy legislations. Notably, Australia has a National Protection Authority that is currently lacking in India. Furthermore, it is recommended that India should also have a specific online privacy regulation with respect to cookies, location data, and advertising.[33] Lastly, a comparison of the EU's General Data Protection Regulation with India's proposed privacy law shows that the ambit of Indian law is wider in terms of its applicability. However, the most significant distinction between both laws lies in the way

[31] Chinmayi Arun, 'Paper-Thin Safeguards and Mass Surveillance in India' (2014) 26 National L School of India Rev 105.
[32] ibid.
[33] Harmanpreet Singh, 'Data Protection and Privacy Legal-Policy Framework in India: A Comparative Study vis-à-vis China and Australia', (2018) 2 Amity J of Computational Sciences 22.

they treat anonymous data. While GDPR does not govern anonymous data, the Indian law empowers the central government to direct organizations to disclose anonymized personal data and even non-personal data.[34] Therefore, access to non-personal data is a cause of concern that needs to be addressed and the government should consider removing this provision as it is subject to abuse on the grounds of political, social, and economic interests. Moreover, data portability is also a feature on which these two legislations differ. The Indian deviation in this respect is that the right to data portability is independent of any legal basis while as per the GDPR data portability is only allowed when it arises out of a legal contract.[35]

Moreover, reliance on sector-specific encryption policies, particularly in the finance sector can be of utmost utility in formulating a national encryption guideline. In this regard, SEBI and RBI have their own guideline to secure digital transactions, for example, the former follows 64/128-bit encryption[36] and the latter follows 128-bit SSL encryption[37] in their respective digital operations.

It should be evidently clear from the above discussion that encryption cannot be interfered with by inserting vague and arbitrary clauses. All

---

[34] Poulomi Sen, 'EU GDPR and Indian Data Protection Bill: A Comparative Study' (*SSRN*, 26 April 2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3834112> accessed 04 May 2022.

[35] Kurt Wimmer, CIPP/E, CIPP/US, Gabe Maldoff & Diana Lee, 'Indian Personal Data Protection Bill vs. GDPR' (*International Association of Privacy Professionals*, March 2020) <https://iapp.org/resources/article/comparison-indian-personal-data-protection-bill-2019-vs-gdpr/> accessed 04 May 2022.

[36] 'Committee on internet based securities trading and services – first report' (*SEBI*, 2001 <https://www.sebi.gov.in/sebi_data/commondocs/99290report_p.pdf> accessed 20 April 2022.

[37] 'Internet Banking in India – Guidelines', (*Reserve Bank of India*, 14 June 2001) <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=414&Mode=0> accessed 04 May 2022.

programs that assist online communications should be permitted to use an end-to-end encryption scheme. India needs unique legislation that addresses individual privacy and, therefore, a clear law that establishes clear guidelines for companies, law enforcement agencies, and people on how to manage user data is needed. Existing rules and regulations must be updated immediately to address the rise of secure communication services.[38] This would be accompanied by an increase in the general level of internet security to promote free expression and e-commerce. India should also focus on finding and implementing worldwide best practices in information security and data protection, which it may learn from the EU Data Protection Directives.[39]

VIII. CONCLUSION

In the new digital world order, it is pertinent to stress upon the fact that anonymity seldom acts as a pre-condition for free speech as it prevents unwanted and biased personal responses. At the same time, it is equally paramount to take care of a nation's security and integrity from technological weapons because advancement in technology has been a boon, both, for pursuing one's legitimate as well as illegitimate interests. In this respect, it is imminent upon the parliament to extensively discuss the issue of privacy and come up with a clear and concise law that leaves no space for ambiguous interpretation and misuse by any of the stakeholders. The parliament can

[38] 'Srikrishna Committee Data Protection Bill and Artificial Intelligence in India', (*The Centre for Internet & Society*, 03 September 2018) <https://cis-india.org/internet-governance/blog/the-srikrishna-committee-data-protection-bill-and-artificial-intelligence-in-india> accessed 04 May 2022.

[39] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

reorganize the joint parliamentary committee and open the draft Bill for public review and comments. Another interpretation of end-to-end encryption is to further security interests. The partial deterioration of law enforcement instruments should not be used to undermine other critical national security concerns.

The author is of the stern opinion that law enforcement and individual privacy can complement each other and go hand-in-hand without causing any hindrance. The author reiterates that overreaching legislation is required to tackle the issue of data protection to generate uniformity in privacy jurisprudence. The use of technological equipment such as encryption in certain pre-defined circumstances coupled with the use of metadata can possibly serve the purpose. It is also worth noting that end-to-end encryption allows for safe network connection anywhere in the globe, regardless of data storage location or service provider. Several data breaches in the recent past have also re-ignited the need to have a strong encryption policy.[40] Advancement in technology has led to people oversharing their information digitally, for example, sharing live locations and keeping their personal documents on social platforms, all of this is empowered and enabled by encryption only. Therefore, the need of the hour is to devise a harmonious way to deal with the privacy of individuals, albeit, ensuring strict vigilance against cyber frauds and other online crimes i.e., a data protection law that guards individual privacy and empowers institutional grip against new-age digital crimes.

[40] Devansh Kaushik, 'Deciphering Encryption Rights In India: The Road Ahead' (2021) Global Privacy L Rev (Wolters Kluwer).