PRIVACY, NATIONAL SECURITY, AND GOVERNMENT INTERESTS: THE MANY FACETS OF END-TO-END ENCRYPTION IN INDIA

—Aditi Singh and Ujjwal Agarwal***

Abstract—End-to-End encryption refers to the act of protecting data in motion, i.e., data that is currently being communicated and transmitted over the internet. The legal debate relating to end-to-end encryption rests on the conflict between the perennial desire of the government to monitor and have official oversight over the activities of its citizens and the privacy of the citizens. In its nascent form, this has also been described as a security versus privacy conflict. However, to portray this dispute in such absolute terms would be doing a disservice to the appreciable nuances involved in the conflict. Hence, the authors have undertaken a three-limbed approach to explore these nuances. First, the paper looks at the positive and the negative impacts of end-to-end encryption on several legal rights including, but not limited to, the Right to Privacy, the Right to Freedom of Speech and Expression and the Right to Form Associations and Assemble Peacefully. Second, the paper critically analyses the various bills, amendments and guidelines which have been proposed by the Government over the years to control how end-to-end encryption is used in India, like, Section 84A of the Information Technology (Amendment) Act, 2008, the Information Technology (Intermediary Guidelines) Rules, 2011 as well as the joint statement released in 2020 by India along with the Five Eyes intelligence alliance. Third, the paper posits that the backdoor policy for circumventing end-to-end encryption, which

* Student, 4th Year, BA LLB (Hons), Maharashtra National Law University, Nagpur.
** Student, 4th Year, BA LLB (Hons), Maharashtra National Law University, Nagpur.

is being considered by the Government of India, is flawed as its potential harms outweigh the benefits. The paper concludes by delineating guidelines on how India can balance the dualities of public interest versus private interest and security versus privacy in regulating end-to-end encryption.

Keywords: End-to-Encryption, Information Technology Act, Privacy, Security.

INTRODUCTION

> "*There is a concern that the internet could be used to commit crimes and that advanced encryption could disguise such activity. However, we do not provide the government with phone jacks outside our homes for unlimited wiretaps. Why, then, should we grant government the Orwellian capability to listen at will and in real time to our communications across the Web?*"
>
> —John Ashcroft, U.S. Senator (explaining the importance of encryption)[146]

Data has become one of the most valuable assets in the 21st Century.[147] Some commentators go so far as to equate it with gold and oil.[148] The method of protecting such data from third-party interference and monitoring by making it unreadable through mathematical algorithms is known as "encryption".

End-to-End encryption (*hereinafter* 'E2E encryption') refers to the act of protecting data in motion, i.e., data which is currently being communicated or is transmitted over the internet, by encrypting the messages being sent from one device and decrypting it at the device receiving the data. This method of encryption protects the data by assigning a key at the point of encryption and ensures that the data is not interfered with

---

[146] John Ashcroft, 'Keep Big Brother's Hands Off the Internet' (1997) 2(4) USIA Electronic Journal <www.swans.com/library/art8/zig080.html> accessed 10 February 2021.

[147] Ben Popken, 'Google Sells the Future, Powered by Your Personal Data' (*NBC News*, 10 May 2018) <www.nbcnews.com/tech/tech-news/google-sells-future-powered-your-personal-data-n870501> accessed 8 February 2021.

[148] Thomas Farkas, 'Data Created by the Internet of Things: The NewGold Without Ownership?' (2017) 23 Revista la Propiedad Inmaterial 5.

while in transit and also hides the data from any third party, including the platform on which it is sent. Thus, in the era of the internet, when individuals are constantly online, E2E encryption helps to protect their online data trail.

The legal debate relating to E2E encryption rests on the conflict between the perennial desire of the government to monitor and have official oversight over the activities of its citizens on one hand and the privacy of the citizens on the other hand.[149] In essence, this has also been described as security versus privacy conflict.[150] However, to portray this dispute in such absolute terms would be doing a disservice to the appreciable nuances involved in the conflict, as will be elaborated in Part II of the paper.[151]

Without making excessive usage of scientific terminologies and computer science, the scope of this paper has been limited to analysing the legal aspects of E2E encryption for data in motion in Over-the-top (*hereinafter* 'OTT') Communication platforms, like WhatsApp, Hike, Facebook Messenger etc. In light of this limitation, this paper aims to present a legal analysis of E2E encryption in the Indian context. First, the paper looks at the positive and the negative impacts of E2E on various legal rights and the stakeholders of such rights. Second, the paper critically analyses the various bills, amendments and guidelines which have been put forward by the Government over the years to control E2E encryption in India. Third, the paper puts forward certain guidelines on how India can balance the various concerns of privacy and security surrounding E2E encryption. The paper concludes by pointing out that more research and jurisprudence is needed on this topic before the Indian Parliament can aptly decide on the future of E2E encryption in India.

E2E ENCRYPTION AND ITS IMPACT ON LEGAL RIGHTS

Right to Privacy

Various legal scholars have tried to delineate the definition of 'privacy', but the vast concept makes it impossible to arrive at a single

---

[149] Michael Froomkin, 'The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution' (1995) 143 U Penn L Rev 709, 713

[150] Christopher Babiarz, 'Encryption Friction' (2017) 10 Alb Govt L Rev 351, 352.

[151] Jim Baker and others, 'Moving the Encryption Policy Conversation Forward' (2019) Carnegie Endownment for International Peace <www.carnegieendowment.org/files/EWG__Encryption_Policy.pdf> accessed 4 February 2021.

universal definition.[152] Considering the fact that the debate around E2E encryption is related to law enforcement authorities' access to the information being communicated by an individual, the 'limited access theory' by Ruth Gavison could be said to be the most pertinent theory of this digital age. It provides that privacy is "related to our concern over our accessibility to others".[153] Hence, this definition can serve as the baseline for the meaning of the word 'privacy' throughout this paper.

In the era of smartphones, when every person's mobile and the messages it communicates are effectively a diary of their life,[154] the consequences of a data breach of privacy are enormous. An example of the consequence of data being compromised is the leak of 'Panama Papers' from a law firm in Panama.[155] While this leak was ultimately good from a public perspective as it disclosed various unethical businesses and their dealings, if we were to transpose the facts of this case to an individual's life, the consequences have the potential to be disastorous. Trade secrets of companies, private information regarding people's lives, and other types of sensitive information could ruin a person's or a company's livelihood if leaked due to a data breach. E2E encryption prevents breach of data in motion by ensuring that the data will be in a cypher form and unreadable, even if hackers intercept the data being communicated between any two devices. Hence, the importance of E2E encryption in protecting privacy cannot be overstated.

While the Indian Constitution does not expressly provide for the right to privacy, in the case of *K.S. Puttaswamy v Union of India,*[156] the Supreme Court of India had included the right to privacy within the gamut of Article 21 of the Constitution.[157] The Court had relied on the doctrine of '*every man's house is his own castle*' as recognised in the *Kharak Singh v State of U.P.*[158] The right to privacy has now become inalienable and ought to be protected.

An example of Central Governments trying to access inaccessible information by denying privacy to their citizens was the proposed Clipper Chip in the USA in the 1990s. It was a piece of hardware which, upon

---

[152] Daniel J Solove, 'Conceptualising Privacy' (2002) 90 Cal L Rev 1087, 1090; Dan Feldman and Eldar Haber, 'Measuring and Protecting Privacy in the Always-on Era' (2020) 35 Berkeley Techn LJ 197, 200.

[153] Ruth Gavison, 'Privacy and the Limits of Law' (1980) 89 Yale LJ 421, 523.

[154] *Riley v California* 189 L Ed 2d 430 (2014).

[155] 'What are the Panama Papers?' (*The New York Times*, 4 April 2016) <www.nytimes.com/2016/04/05/world/panama-papers-explainer.html> accessed 5 February 2021.

[156] *K S Puttaswamy v Union of India* (2017) 10 SCC 1.

[157] ibid.

[158] *Kharak Singh v State of U.P.* AIR 1963 SC 1295.

installation on an electronic device, would give the Government and law enforcement agencies access to all the information in that device. The idea was eventually scrapped because the Government conceded that people who were highly incentivised to protect their data, like terrorists and criminals, lest it implicate them in their nefarious activities, would just use other more sophisticated means of encryption to communicate amongst themselves and the Clipper Clip would have no utilisation in preventing crimes.[159] Hence, the Government concluded that digital encryption would be the new norm and installing Clipper Chip would be more harmful to public privacy than it would be beneficial for crime prevention.

Right to Freedom of Speech and Expression

The 21st century brought with it the emergence of smartphones and readily available and affordable internet. This led to more and more people using the internet as a means of exercising the freedom of speech through online communication.[160] Hence, protecting this vital means of online communication becomes increasingly important in a democracy as demonstrated by a report of the Human Rights Council wherein it was said: 'Encryption and anonymity provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks.[161]

The above statement is noteworthy for providing credence to the fact that E2E encryption helps in ensuring that personal beliefs and opinions shared across an online medium do not fall into the wrong hands. The importance of E2E encryption towards protecting freedom of speech and expression can be gleaned from its growing importance in the work of people in anti-establishment or at-risk jobs, like, investigative journalists, advocates fighting against human rights atrocities, civil society leaders, and even marginalised groups who face persecution (*hereinafter* 'at-risk groups').[162] Consequently, it can be concluded that E2E encryption protects and promotes the freedom of speech and expression.

The right to freedom of speech and expression is protected by Article 19(1)(g) of the Constitution and is one of the fundamental rights provided

---

[159] Steven Levy, 'Why are We Fighting the Crypto Wars Again?' (*Wired*, 11 March 2016) <www.wired.com/2016/03/why-are-we-fighting-the-crypto-wars-again/> accessed 6 February 2021.

[160] David Kye, '*Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*' (2015), A/HRC/29/32.

[161] ibid.

[162] ibid.

therein.[163] Hence, it can be stated that the continuation of the E2E encryption regime would amount to the promotion and protection of this fundamental right.

Right to Form Associations and Assemble Peacefully

Article 19(1)(b) provides that all Indian citizens have the right to assemble peacefully and without arms, while Article 19(1)(c) provides the right to form associations or unions or cooperative societies to the citizens.[164] These rights are proactively promoted and protected by E2E encryption as it ensures that third parties are not able to intercept messages and hence, not subjected to any possible surveillance.[165] Therefore, it can be reasonably concluded that without E2E encryption, the right to form associations could be increasingly at risk.

An example of curtailing the freedom of association by prohibiting encrypted communication platforms can be found in Iran. During the 2013 presidential elections, when law enforcement was afraid of protests, they decreased the speed of encrypted modes of communication to a mere 5 per cent of the normal internet speed. This resulted in considerable difficulty for the protestors to organise protests. Similarly, in a democratic and a majoritarian country like India, where protests and public demands are an important part of the democratic process,[166] it is in the best interests of the country to continue to have a strengthened E2E encryption regime in OTT Communication.

Does the Reasonable restriction OF "National Security" trump Legal Rights?

The right to freedom of speech and expression, the right to form associations, and the right to protest peacefully are qualified by the reasonable restrictions given in Article 19(2). Additionally, even the right to privacy is not absolute and can be reasonably restricted to protect and effectuate the state's interest.[167] Justice Dr. DY Chandrachud had laid down that the right to privacy could be subjected to the reasonable restrictions on the satisfaction of three tests, which are, first, the restriction must be by law, second, it must be necessary and proportionate and third, it must promote

---

[163] Constitution of India 1950, art 19(1)(g).

[164] Constitution of India 1950, arts 19(1)(b) and 19(1)(c).

[165] Froomkin (n 149) 818-819.

[166] G Sampath, 'No Country for Protesters?' *The Hindu* (2 March 2020) <www.thehindu.com/opinion/op-ed/no-country-for-protesters/article30957829.ece> accessed 3 February 2021.

[167] *Puttaswamy* (n 156).

a legitimate state interest. National security can satisfy all three tests laid down by Justice Chandrachud depending on the facts and the circumstances of each case.

The issue which arises is whether the reasonable restrictions provided in Article 19(2) are enough to restrict or water down the E2E encryption provided by OTT communication services.

Reading the legal rights and the reasonable restrictions together, it would be prudent to say that the legal rights should not come in the way of securing National Security and should be harmoniously construed with the larger public interest. A strong encryption policy wherein E2E encryption does not make any data accessible to the government could easily affect national security by precluding the State from taking action against the criminals by denying the State the data of such people.

Thus, without the necessary data, government agencies will not be able to control, prevent, anticipate, and apprehend many criminal activities as the threat could go undetected and would harm the public at large. That is the reason why India asked Research in Motion (*hereinafter* 'RIM') Blackberry to intercept the encryption and transfer the data of the terrorists involved in the 26/11 terror attacks.[168] The Indian government had strictly asked the RIM to localise its data in India to further strengthen the surveillance process to detect any potential threat in India.[169] Even the Indian Communications and IT Minister Ravi Shankar Prasad had said that encryption should not come in the way of law enforcement agencies and thus the law enforcement agencies must have access to such data to curb any nuisances in the society.[170] This sentiment was also echoed in a statement of the FBI Director James Comey in 2014 wherein he has stated:

> "*Unfortunately, the law hasn't kept pace with technology, and this disconnect has created a significant public safety problem. We call it "Going Dark," and what it means is this: Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful*

[168] Bedavyasa Mohanty, 'The Encryption Debate in India' (2019) (*Carnegei Endownment for International Peace*, 30 May 2019) <www.carnegieendowment.org/files/WP_The_Encryption_Debate_in_India.pdf> accessed 29 January 2021.

[169] ibid.

[170] Special Correspondent, '"Encryption Cannot Allow Rumours", says Ravi Shankar Prasad' *The Hindu*, (New Delhi, 14 October 2019) <www.thehindu.com/news/national/encryption-cannot-allow-rumours-says-ravi-shankar-prasad/article29683034.ece> accessed 3 February 2021.

> *authority. We have the legal authority to intercept and access communications and information according to a court order, but we often lack the technical ability to do so.*"[171]

Additionally, in *Riley v California*, the US Supreme Court shed light on how the widespread use of technology has aided criminals and how it can be helpful for law enforcement to decrypt it:

> "*Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost.*"[172]

The above-mentioned statement showcases the costs which the Governments will have to bear if the right to privacy is given precedence over national security. Such costs can also be showcased by the recent example of a growing dispute between the Federal Bureau of Investigation (*hereinafter* 'FBI') and Apple. Apple had denied FBI's requests to give them the decryption key of an iPhone belonging to Mohammed Saeed Alshamrani who was behind the shooting in Pensacola, Florida, and had links with Al Qaeda,[173] similar to another incident involving a Bernardino terrorist attack[174]. In May 2020, the FBI announced that they had decrypted the phone themselves. It is worth noting that if the FBI did not have the technical capability to decrypt the device or had not managed to do it for any reason, a terrorist might have got away with his crime and would have been a potential future threat to peace, public safety and national security of the citizens. This sentiment can be aptly described in the words of David Anderson QC, who stated in his report that *«the deaths of UK nationals through terrorism have not*

---

171 James B Comey, 'Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?' (*Federal Bureau of Investigation*, 16 October 2014) <www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course#:~:text=With%20Going%20Dark%2C%20those%20of,plan%2C%20and%20execute%20an%20attack> accessed 1 February 2021.

172 *Riley* (n 154) [2493].

173 David Shortell & Evan Perez, 'FBI Finds Al Qaeda Link After Breaking Encryption on Pensacola Attacker's IPhone' (*CNN*, 19 May 2020) <www.edition.cnn.com/2020/05/18/politics/pensacola-shooting-al-qaeda/index.html> accessed 31 January 2021.

174 Brian Barrett, 'The FBI Backs Down Against Apple—Again' (*Wired*, 5 October 2020) <www.wired.com/story/fbi-backs-down-apple-encryption-pensacola-iphones/> accessed 5 February 2021.

been more numerous owes something to luck ... and a great deal to the capabilities of the intelligence agencies and police».[175]

Interestingly, contrary to Apple's policy in the USA, Apple had transferred the data of Chinese users to a state-run company in China and had also stated that this will enable the Chinese firm to have access to all data of Chinese users.[176] The duplicity of Apple in denying the data of its users in the USA to the law enforcement authorities while simultaneously providing it to the Chinese authorities showcases how the company reacts towards the rights of its consumers in different political climates. This sets a dangerous precedent for the right to privacy of its users as it points out how reasonable restrictions might not be the only possible threat to the privacy of its users and sheds light on how political climates and other external factors also play a role.

While the FBI and Apple's example talks about data in rest, i.e., the data being stored and which is not in use, the same principles could be transposed to issues involving data in motion. One such example involving similar issues concerning data in motion in India was the recent controversy involving WhatsApp, a multi-national OTT communications platform. Recently in 2018, the Government of India had attributed various mob lynching incidents to misinformation and false information being forwarded on WhatsApp messenger. Thereafter, the Ministry of Electronics and Information Technology (*hereinafter* 'MEITY') had condemned such messaging services which use E2E encryption and said that OTT communication providers cannot 'evade accountability and responsibility' for spreading rumours.[177] WhatsApp had expressed its inability to provide any data to the government as it follows E2E encryption, but it had rolled out 6 new measures to curb the spread of such fake information.[178]

A beneficial approach would be to balance the competing rights and interests through dedicated legislation, as the President of the Hon'ble Supreme Court of the United Kingdom had stated.[179] Thus, the right to

---

[175] David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* (H M Government 2015).

[176] Nick Statt, 'Apple's iCloud Partner in China will Store User Data on Servers of State-Run Telecom' (*The Verge*, 18 July 2018) <www.theverge.com/2018/7/18/17587304/apple-icloud-china-user-data-state-run-telecom-privacy-security> accessed 30 January 2021.

[177] Bedavyasa Mohanty, 'Let's not Shoot the WhatsApp Messenger' (*The Wire*, 6 July 2018) <www.thewire.in/government/whatsapp-rumour-lynching-regulation> accessed 6 February 2021.

[178] ibid.

[179] Lord Neuberger of Abbotsbury, 'Is Nothing Secret? Privacy and Confidentiality, Privacy, Freedom of Information and Whistleblowing in the Internet Age' (2016) 28

privacy of an individual and the larger public interest should be balanced and compatible with each other.

CRITICAL ANALYSIS OF INDIAN LAWS ON E2E ENCRYPTION

The Current Indian Legal Landscape on E2E Encryption

Section 84A of the Information Technology (Amendment) Act, 2008 (*hereinafter* 'IT Act') gives the Central Government powers to formulate rules for encryption over an electronic medium.[180] The provision provides that this power accedes to the Government to promote network security and e-governance. Under this Section, the Government had published a draft proposal encryption policy in 2015,[181] which was widely criticised for two main reasons. First, for watering down strong encryption rules and secondly, for a general lack of care from the government's side for the threat to privacy and freedom of speech it would bring about for its citizens.[182] Thereafter, the Government withdrew the policy, and it hasn't published a new one till date.

Interestingly, on September 14th 2020, the Telecom Regulatory Authority of India (*hereinafter* 'TRAI') released a report on the 'Recommendations on Regulatory Framework for Over-The-Top Communication Services'.[183] In this report, TRAI recommended that a comprehensive regulatory framework for the encryption regime of OTT Communication services would not be the correct step at this point of time as such regulations are only at the nascent stage throughout the world and it would be more beneficial for India to wait and watch. Further, the report stated that no regulatory interventions are necessary to deal with the privacy and security of OTT platforms, yet the Report has not ruled out the possibility of regulatory intervention, rather it has stated that an intervention might be done at a later "appropriate" stage of time.

SAcLJ 1, 4.

[180] The Information Technology Act 2000.

[181] Department of Electronics and Information Technology, 'Draft National Encryption Policy' (2015) <https://netzpolitik.org/wp-upload/draft-Encryption-Policyv1.pdf> accessed 28 November 2020.

[182] BhairavAcharya, 'The Short-lived Adventure of India's Encryption Policy', (*The Centre for Internet & Society*, 27 November 2015) <https://cis-india.org/internet-governance/blog/the-short-lived-adventure-of-india2019s-encryption-policy> accessed 29 November 2020.

[183] Telecom Regulatory Authority of India, 'Recommendations on Regulatory Framework for Over-The-Top (OTT) Communication Services' (2020). <www.trai.gov.in/sites/default/files/Recommendation_14092020_0.pdf> accessed 29 November 2020.

Hence, it is apparent that no specific legislation or rules exist for E2E encryption in OTT communication in India currently.

A Critical Appraisal of the Proposed Amendments to Regulate E2E Encryption

In December 2018, the Ministry of Electronics and Information Technology proposed certain changes concerning E2E encryption to the Information Technology (Intermediary Guidelines) Rules, 2011 (*hereinafter* 'intermediary rules').[184] A strong incentive has also been provided to ensure that the OTT Communication platforms adhere to these rules if they come into force: if the companies do not follow the rules, then the 'safe harbour' law ceases to apply to them. Safe harbour law essentially states that the companies will not be responsible for the content posted by their users. Hence, it can be stated that the companies are in a Catch-22 situation i.e., either they follow the rules and significantly weaken their encryption system, or they lose the protection of the safe harbour law and potentially become liable to whatever the users post on their platform. This shows that it is important for the Government that the proposed changes in the intermediary rules are followed.

One of the key changes is that the Government mandated intermediaries, including OTT communications platforms, to assist within 72 hours whenever "any government agency" requests data. The draft rules have not provided for any court orders or any authorisation process that needs to be followed to grant access. Hence, any government agency can request data on any person without a court order or a warrant. This proposed amendment is by far the most concerning one as it has gone directly against the 2009 recommendation of the Data Council of India which particularly noted: "*foreign companies are likely to restrict outsourcing to India if plain text is asked for by law enforcement agencies without due process and/or court orders*".[185] Hence, the lack of an authorisation process will not only create the possibility of surveillance features over at-risk individuals, but it could also prevent the Indian public from being the recipient of updated technologies as tech conglomerates may refuse to provide services.

It is noteworthy that encryption software is always designed by the private companies which use it. Hence, asking them to assist in providing information to the law enforcement authorities would significantly

---

[184] Ministry of Electronics and Information Technology, 'The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018' (2018).

[185] Recommendations for Encryption Policy u/s 84A of the IT (Amendment) Act (2008) 11.

cut down on the resources spent by such authorities to work around such encryption to access the information.[186] However, while this provision would appeal to the enforcement authorities, it would be directly against the interest of the compelled OTT platform as helping the authorities to decrypt E2E encryption would require the platforms to water down the E2E encryption which they designed,[187] as Apple's CEO Tim Cook has previously noted.[188] Additionally, certain companies which market themselves as being 'secure' messaging services would be going against their brand image to help the government and this could significantly hamper their market prospects.

Another key change that is proposed is that the intermediaries will be required to trace the 'originator' of any information. If implemented, this would have the consequence of obliterating E2E encryption as it stands.

In its current form, E2E encryption provides for a decryption key through which the message communicated by a sender can only be decrypted with the help of the key by the receiver; even the OTT platform itself does not have the key to decrypt such messages.[189] E2E encryption effectively means that even with a Court order, the OTT platforms cannot give over data on their users as they do not the decryption key.[190] In such a situation, tracing the originator of a message or giving over data to comply with the request of the government agency would require the OTT Platforms to either have a 'backdoor' or to have a decryption key with themselves which would effectively corrode E2E encryption and increase the fear of mass surveillance.

In February 2020, it was reported that the draft intermediary rules would be made following the finalised version of the recent Personal Data Protection Bill, 2018 (*hereinafter* 'PDP Bill') after it is passed.[191] In November 2020, the Joint Parliamentary Committee, while scrutinising

---

[186] Orin S. Kerr, 'Internet Surveillance Law After the USA Patriot Act: The Big Brother that isn't' (2003) 97 Nw U L Rev 607, 621.

[187] Orin S. Kerr & Bruce Schneier, 'Encryption Workarounds' (2018) 106 Geo LJ 989, 1015.

[188] Tim Cook, 'A Message to Our Customers' (*Apple*, 16 February 2016) <www.apple.com/customer-letter/> accessed 28 November 2020.

[189] Andy Greenberg, 'Hacker Lexicon: What is End-to-End Encryption?' (*Wired*, 25 November2014) <www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/> accessed 29 Nov 2020.

[190] Urs Gasser and others, 'Don't Panic. Making Progress on the "Going Dark"' (*The Berkman Klein Center for Internet & Society at Havard University*, 1 February 2016) <https://cyber.harvard.edu/publications/2016/Cybersecurity/Dont_Panic> accessed 29 November 2020.

[191] S. Ronendra Singh, 'Intermediary Guidelines' for Net platforms Likely to be Delayed' *The Hindu Business Line* (New Delhi, 14 February 2020) <www.thehindubusinessline.

the PDP Bill had strongly supported data localisation,[192] which is the process of storing data of citizens in their home country for processing and is based on the concept of data sovereignty.[193] Through data localisation, it becomes easier for law enforcement authorities to demand access to the data stored in the servers or to encrypted files. Hence, data localisation ensures the jurisdiction of Indian authorities over data breaches and strengthens the Indian economy.[194] This indicates that after the enactment of the PDP Bill, all the OTT communication providers including WhatsApp, to operate in India have to mandatorily localise the data of around 400 million Indian users in India, which might provide significant assistance to law enforcement authorities in India. This could prove to be another nail in the coffin for E2E encryption in India.

Alternatively, the above-mentioned absurd requirements by the Government may be altered. However, it is hard to believe that the Government would move away from its stance of asking OTT platforms to provide information through a backdoor. This has also been reaffirmed by the release of the recent Joint Statement by India and Japan along with the Five Eyes intelligence alliance, as discussed below.

Legal Analysis of Backdoor Policy

On October 11, 2020, India joined the Five Eyes intelligence alliance to issue a joint statement on the negative impact of E2E encryption on public safety as it precludes official oversight. The statement has effectively demanded 'backdoors' to be installed in E2E encrypted systems run by the global tech conglomerates.[195] Even President Obama has talked about implementing a modern version of the Clipper Chip i.e., backdoors in encryption systems. He said:

---

com/info-tech/intermediary-guidelines-for-net-platforms-likely-to-be-delayed/article30801754.ece> accessed 29 November 2020.

[192] Gyan Varma, 'Nothing 'Personal' About Data Protection Bill as JPC Proposes to Expand Scope' (*Mint*, 24 Nov2020), <www.livemint.com/news/india/nothing-personal-about-data-protection-bill-11606194232029.html> accessed 29 November 2020.

[193] Maahi Mayuri, 'Data Localisation: What's in it for Us?' (*Mondaq*, 1 June 2019) <www.mondaq.com/india/x/820350/Data+Protection+Privacy/Data+Localisation+Whats+In+It+For+Us> accessed 29 November 2020.

[194] Justice Srikrishna Committee, *'Report on A Free and Fair Digital Economy Protecting Privacy, Empowering Indians'* (2017) 83.

[195] 'India joins Five Eyes, Japan in Demanding Backdoor into WhatsApp End-to-End Encrypted Chats' *India Today* (New Delhi, 12 October 2020) <www.indiatoday.in/technology/news/story/india-joins-five-eyes-japan-in-demanding-backdoor-into-whatsapp-end-to-end-encrypted-chats-1730681-2020-10-12> accessed 29 November 2020.

> *"If it was technologically possible to make an impenetrable device where there›s no door at all, then how do we apprehend the child pornographer? How do we disrupt a terrorist plot? ... There has to be some concession to get into that information somewhere... We can›t fetishise our phones above every other value. The dangers are real. This notion that sometimes our data is different and can be walled off from these other tradeoffs is incorrect."*[196]

The back door should be created only if its benefits outweigh the costs.[197] However, the authors feel that the disadvantages that accompany the creation of a backdoor would outweigh its potential benefits. This is because, while the backdoor may be used by law enforcement agencies, it may also create a vulnerable situation that could be exploited by hackers and foreign governmental agencies thus leading to mass surveillance and breach of the right to privacy.[198] In E2E, the data is highly secured and can only be accessed by the users. As mentioned earlier, even the messaging service provider has no access to the contents of the messages exchanged between two users. Therefore, a backdoor could destroy the security and privacy benefit offered by E2E encryption[199] and thus backdoor decryption based on a case-to-case basis would be more viable as opposed to general backdoor decryption.

Potential abuse of a backdoor was noticed in Greece in 2005, popularly known as 'Athens Affair'. The incident led to the tapping of the cell phones of at least 100 government officials including the president and prime minister of Greece.[200] It is widely believed that the National security Agency (*hereinafter* 'NSA') had collaborated with the Greek law enforcement agency to oversee the 2004 Olympic games as a defence mechanism to evade any potential terrorist attack after the brutal terrorist attacks of 9/11 in the year 2001.[201] However, after the successful

---

[196] Christian Zibreg, 'DOJ Threatened to Seize iOS Source Code Unless Apple Complies with Court Order in FBI Case' (*iDownloadBlog*, 14 March 2016) <www.idownloadblog.com/2016/03/14/dos-threats-seize-ios/> accessed 29 November 2020.

[197] Charles Duan and others, 'Policy Approaches to the Encryption Debate' (133) R Street Pol'y Study <http://2o9ub0417chl2lg6m43em6psi2i.wpengine.netdna-cdn.com/wp-content/uploads/2018/03/133.pdf> accessed 29 November 2020.

[198] Yoni Heisler, 'Here's Apple's Long-Awaited Legal Response to The FBI' (*BGR*, 25 Feb 2016) <http://bgr.com/2016/02/25/apple-vs-fbi-legal-filing/> accessed 29 November 2020.

[199] Mohanty, 'The Encryption Debate in India' (n 168) (6).

[200] James Bamford, 'A Death in Athens' (*The Intercept*, 29 September2015) <https://theintercept.com/2015/09/28/death-athens-rogue-nsa-operation/>.

[201] Trevor Timm, 'The "Athens Affair" Shows Why We Need Encryption without Backdoors' (*The Guardian*, 30 September 2015) <www.theguardian.com/

completion of the Olympic games, the NSA, which was supposed to wrap up the entire operation, continued spying on government officials through Greek's largest cellular service provider – Vodafone Greece, which even led to the suspicious death of techie employed at Vodafone Greece. Thus, it can be observed how a backdoor could help a foreign government spy on top government officials of any country and lead to violation of the right to privacy.

An interesting point to note is that there exists no parallel in the physical world wherein the Government is not able to access cryptography.[202] In the past, if the government was unable to crack a certain type of cryptography, it would just employ cryptographers to crack it. If the government needed to listen to conversations, they would just wiretap ordinary telephones. If there was a safety deposit box that the government needed to access, it would have just used brute force to open it. Hence, the advent of digital encryption has found government across the world in an unknown and uncertain situation. Hence, the Government must tread carefully into this unknown realm of digital encryption regulation and make provisions after due consideration.

Additionally, the former Director of the FBI, Mr. James B. Comey had agreed that a backdoor may be exploited by foreign adversaries and hackers, and thus, instead of a back door, they seek the use of front door i.e., decryption with clarity, transparency, and clear guidance provided by law.[203] Thus, it can be seen that in most cases, the benefits of a backdoor do not outweigh the costs and that a backdoor system could lead to potential harm and thus should not be vouched for.

FUTURE OF E2E ENCRYPTION IN INDIA

While E2E Encryption ensures maximum protection of the right to privacy, the Indian Government considers the benefits of privacy weak against the costs of national security and public safety, as is evident from its Joint Statement with the Five Eyes Alliance. Thus, we propose a few guidelines to balance the interest of both the government and the OTT Communication applications who vouch for E2E encryption to ensure maximum privacy to their users.

---

commentisfree/2015/sep/30/athens-affair-encryption-backdoors>.

[202] Froomkin (n149) (1) 871.

[203] Comey (n 171).

Decryption based on previous criminal conduct

The surveillance of history sheeters or "goondas" is an old age practice and is continuing since the colonial period.[204] This assists the law enforcement authorities to keep a check on such history sheeters and enables them to protect public peace and tranquillity. Furthermore, with the advent of technology, the government had brought National Intelligence Grid (*hereinafter* 'NATGRID') and Criminal Tracking Network System (*hereinafter* 'CCTNS'). The NATGRID focuses upon collecting the data from individual police stations and is accessed by several government law enforcement agencies while the CCTNS links up all the police stations in the country and facilitates the sharing of data amongst them.[205] Thus, the technology helps the law enforcement agencies to keep track of the history sheeters.

The E2E Encryption as provided by the OTT Communication platforms could hamper the functioning of law enforcement agencies while collecting evidence. Thus, allowing law enforcement agencies to access the decryption key of selected history sheeters could be useful for surveillance as this will satisfy the concerns of privacy enthusiasts who criticise mass surveillance as well as the government whose focus is national security.

Evidence-based Decryption

To avoid any potential privacy breach by law enforcement agencies, there could be a procedure for evidence-based decryption ordered by a judicial authority. Thus, according to such an approach the law enforcement agency must produce sufficient evidence before the judicial authority, in order to convince the judges that there is a necessity of decryption. Ideally, it is only after the proper judicial order that the decryption should be allowed. The European Court of Human Rights has in the case of *Klass v. Germany*[206] while dealing with mass surveillance, observed that "*the Court considers that, in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for a democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge*".[207] Thus, right to privacy being a sensitive issue, judicial entrustment could be a possible method to satisfy the competing

---

[204] Mrinal Satish, 'Bad Characters, History Sheeters, Budding Goondas and Rowdies: Police Surveillance Files and Intelligence Databases in India' (2011) 23(l) National Law School of India Review 133, 135.

[205] ibid.

[206] *Klass v Germany* (1978) 2 EHRR 214.

[207] ibid.

interests of privacy and national security. Furthermore, to deal with time-sensitive cases, the judicial authority could be granted to the fast track or mobile courts.

Setting up of Privacy Ombudsman

After *Puttaswamy,* the right to privacy is considered to be included within Article 21 of the Constitution of India and thus, demands special protection. While the legislature is in progress to enact specific legislation to govern such a right, a privacy ombudsman could be an effective method to oversee that the government does not abuse its power. A similar practice is followed in the UK wherein the Investigatory Powers Tribunal (*hereinafter* 'IPT') is a judicial body responsible for limiting the government's power of surveillance and ensures that any individual's right to privacy is not infringed upon by unnecessary government surveillance. In the case of *Weber v Germany,*[208] the European Court of Human Rights while interpreting Germany's G10 Act, had observed that the interception of communication by the law enforcement agency will be valid provided that there should be sufficient safeguards and supervision by a member who is qualified to hold a judicial office. Thus, a similar practice could be brought into India wherein, a privacy ombudsman could be appointed who can supervise the governmental action to avoid any abuse of power.

CONCLUSION

India's tryst with E2E encryption has just begun, and there have already been numerous controversies. It is imminent that once the amended draft intermediary rules are released and the PDP Bill goes through the Parliament, there are bound to be many more controversies. Through all this, it is essential to keep in mind that the privacy of India's entire 1.3 billion population rests on what India decides in the coming days. Being the largest democracy in the world, the Indian Parliament must ensure that it stands as a role model to other countries on how to protect the privacy of its citizens while simultaneously dealing with the competing interests of national security. It is imperative to mention here that till now, no research or study has been conducted which talks about how much having access to the encrypted messages on OTT platforms will help the Government in maintaining law and order. It is merely assumed by all people involved in this debate that it will have a positive impact on national security.[209] However, it is debatable whether the

[208] *Weber v Germany* 2006 ECHR 1173.
[209] Kerr, 'Encryption Workarounds' (n 187).

privacy of Indian citizens should be risked over an assumption. Hence, rigorous research still needs to be conducted to provide empirical evidence of how much benefit will occur to national security after watering down encryption rights. At present, the Indian Government is certainly not happy with the current status quo of how E2E encryption stands, as is evident from its numerous attempts over the years to change the status quo and impose data localisation on OTT communication platforms. Sooner or later, however, the Parliament will pass a law changing the current status quo on E2E encryption and when that happens, it will be necessary that a balanced viewpoint is reached, without isolating any one side of the encryption debate.