EXPERT STAKEHOLDER CONSULTATION REPORT ON THE

INDIAN ENCRYPTION DEBATE

The Dialogue™

INFORM ENGAGE IDEATE

DR. GULSHAN RAI
Former National Cyber Security Coordinator,
Government of India

FOREWORD

The discipline of encryption Technology (so called Cryptology) has assumed significant role in the present Digital age. It has prominent role both maintaining privacy and security of digital information. While cryptography deals with the creation of the encryption algorithm itself, cryptanalysis deals with the decryption and examination of the encrypted information. Law enforcement agencies more are concerned with the latter. India has expertise to create a strong cryptographic system, but have serious gaps with crypto analysis. Infact this issue concerns the entire world. Of the several reasons for such a weak strength, the lack of understanding and clarity is at the forefront. This lack of awareness leads to limited funding by the government. An increase in investment within this space is essential to boost R&D.

In the debate of encryption vs national security, very few look to technology as the answer. Without the appropriate perspective, it is unlikely that the right investments will be made. In order to bring about the balance between privacy and national security, we must first examine the responsibility of those attempting to decrypt private communication. The conventional method of interception has practically disappeared, and decryption has become a lot more challenging.

There exists a legitimate state interest in seeking access to data for law enforcement purposes. The balance between privacy and national security is not bereft of technological or operational solutions. While aiming to achieve them it is crucial that none of the key stakeholders take an extremist position where we end up compromising security and privacy of Indians.

The challenges must be examined from multiple perspectives, with collective decision-making and increased collaboration. The solution cannot come from a single body, but must be the result of unbiased and comprehensive discussions among all stakeholders, including civil society and national security agencies. It is important to remember, in the context of the current debate on privacy and security, that encryption technologies have advanced significantly and any approach that aims to bring a balance between the two cannot be hinged on prescriptive legal texts. We must approach this as a hard cryptographic research problem and adopt a scientific approach to arrive at a solution that doesn't undermine security of Indians and make them more vulnerable to cyber attacks.

In summation, I believe the law has to be cognizant of the technological realities of today and adopt a more principle based approach to regulation that furthers innovation while maintaining the robustness of encryption technologies that protect the sensitive data of all Indians.

(Dr. Gulshan Rai)
Former National Cyber Security Coordinator, Government of India

grai@meity.gov.in | gulshanrai@hotmail.com

TABLE OF CONTENTS

KEY RECOMMENDATIONS

01. A mandate for backdoors to encryption or originator traceability fails to fulfill the Puttaswamy test and must not be implemented.

02. The originator traceability mandate would result in practical complications for the industry, become an obstacle to small businesses and innovation, and the consequent product will be difficult to sell in the international market.Such a mandate should not be implemented without further consultation.

03. Increased awareness is needed on the importance of cybersecurity and the role of encryption within the same.

04. Increased investment in technology is required which will encourage R&D and indigenise the technology.

05. Clarity in policies dealing with cybersecurity is essential to adhere to principles of transparency and accountability.

06. High end encryption is only the first step in tackling cyber-crime and therefore, the discussion cannot be limited and must go further.

07. The implementation of the IT Rules, 2021 should be delayed and technical experts should be consulted to better address the challenges involved and recommend the way forward.

INTRODUCTION

The Dialogue, a New Delhi based Think-Tank, organised three virtual stakeholder consultations to better appreciate the Indian Encryption Debate.

- The first consultation primarily discussed the **Telecom Regulatory Authority of India's (TRAI) recommendations on the Regulatory Framework for Over-The-Top Communication Services**.
- The second consultation revolved around **Enabling a Progressive Cyber Security Regime**, and the role of encryption.
- The third consultation focussed on the **legal and constitutional implications of the IT Rules of 2021**.

The distinguished panellists focussed on finding a way forward within this space and the development of domestic encryption technology and related policies. To do so, they first discussed the broad challenges that act as a hindrance to such development, like **limited financing, lack of awareness, the national security versus privacy debate**, among other issues.

While each speaker made multiple recommendations, there were several that garnered unanimous approval. These included the **need to increase investments** within this sphere to **boost R&D and increase awareness** on how a robust cybersecurity regulation needs to be transparent and accountable to the users in cyberspace. Most importantly, it was understood that **encryption is an essential first step to protect the fundamental right to privacy and online safety, national security, and data security** within various fields like e-commerce, education, health, finance etc. Therefore, **encryption is non-negotiable in any progressive data protection regime**. Without encryption, it is likely that the aforementioned ideals will be compromised. Lastly, the panel pointed out that **encryption and national security are not mutually exclusive and are, in fact, harmonious** to one another.

A. THE GLOBAL ENCRYPTION DEBATE

The advancement of technology in the past few decades has led the public authorities to become wary of the development of encryption technology within the private sector. The argument against encryption, in the United States, began with a case being made in favour of **national security** and **protection against foreign threats**. As a result of this, the **1991 Anti-Terrorism Bill** was passed, which allowed the government backdoor access to encrypted communication. [1]

1 S.266 - 102nd Congress (1991-1992): Comprehensive Counter-Terrorism Act of 1991, S.266, 102nd Cong. (1991), https://www.congress.gov/bill/102nd-congress/senate-bill/266/text.

More recently, the Federal Bureau of Investigation (FBI) attempted to gain access to the iPhone of one of the shooters in the San Bernardino attack.[2] With time, the encryption debate has a new challenge to tackle- the increase in **Child Sexual Abuse Material (CSAM)** online. Accordingly, two bills were introduced in 2020- **Eliminating Abusive and Rampant Neglect of Interactive Technologies Act** and the **Lawful Access to Encrypted Data Act**. The former was drafted to curb online child exploitation, while the latter would directly mandate that U.S. online service providers must build a backdoor into their encryption for law enforcement purposes.[3]

In order to regulate the use of encryption technology for data protection the U.S., United Kingdom and **several European Union member states rely on civil law**. On the other hand, Japan opted for a prescriptive mandate that needs to be followed. **The Act on the Protection of Personal Information (APPI)** mandates that personal information be secured and empowers regulators to enforce the same. Similarly, Russia and China don't rely on civil law alone to act as a sufficient deterrent. The '**Yarovaya Law**' was passed by the Russians in 2016, which permitted the government to decrypt encrypted network traffic.[4] The encryption debate in China has always been heavily influenced by economic development, technological autonomy and national security. However, the past few years have seen increasing concerns regarding individual users, government access to data, and personal information protection in particular.[5]

Most recently, the **Five Eyes** along with India and Japan released a communique[6] appealing to the Big Tech to ensure traceability in encrypted platforms. A similar sentiment was echoed by a **Draft Resolution of the Council of the European Union**.[7] Both the Communique and the Draft Council Resolution have been a *cause celebre*. The **Global Encryption Coalition**, released a non-technical paper explaining why breaking encryption is not a solution to terrorism or CSAM proliferation in the cyberspace. The creation of a backdoor will inevitably create a vulnerability within the communication system that will be easy to exploit by criminals or any other unauthorised parties. The deliberate creation of such a vulnerability leaves children, among several others, even more susceptible to online abuse and other cyber crimes.[8] This has been further corroborated by **Europol's SIRIUS Digital Evidence Report** which explicates that in most cases access to content data is not required, and meta data is sufficient. [9] The primary challenge according to the report is the tedious process of obtaining

---

2 Elizabeth Dwoskin &Ellen Nakashima, FBI has accessed San Bernardino shooter's phone without Apple's help, The Washington Post (Mar. 28, 2016) https://www.washingtonpost.com/world/national-security/fbi-has-accessed-san-bernardino-shooters-phone-without-pples-help/2016/03/28/e593a0e2-f52b-11e5-9804-537defcc3cf6_story.html.

3 Riana Pfefferkorn, What's New in the US Crypto Wars, The Centre for Internet and Society, (Oct. 30, 2020) https://cyberlaw.stanford.edu/multimedia/whats-new-us-crypto-wars.

4 Eric Richards et. al., Decrypting the Global Encryption Debate, The Huffington Post, (Oct. 20, 2016) https://www.belfercenter.org/publication/decrypting-global-encryption-debate

5 Lorland Loksai & Adam Segal, The Encryption Debate in China, The Carnegie Endowment for International Peace, (May 30, 2019) https://carnegieendowment.org/2019/05/30/encryption-debate-in-china-pub-79216.

6 The United States Department of Justice, Office of the Attorney General, Press Release no. 20-1,086, International Statement: End-To-End Encryption and Public Safety, (Oct 11, 2020) https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety.

7 Council of the European Union, Draft Council Resolution on Encryption by Council of EU - Security through encryption and security despite encryption, 12143/1/20 REV 1 LIMITE JAI 851 https://files.orf.at/vietnam2/files/fm4/202045/783284_fh_st12143-re-01en20_783284.pdf.

8 Global Encryption Coalition, Breaking Encryption Myths: What the European Commission's leaked report got wrong about online security, Centre for Democracy & Technology (Nov. 19, 2020) https://www.globalencryption.org/2020/11/breaking-encryption-myths/

9 Europol, Transnational Access to Electric Evidence for Criminal Cases: Trends and Latest Developments Within the EU and Beyond, (Dec. 1, 2020) https://www.europol.europa.eu/newsroom/news/transnational-access-to-electronic-evidence-for-criminal-cas-

digital evidence via the Mutual Legal Assistance and the lack of standardisation in the company policies. Similarly, **UNICEF** released a report explaining how encryption is crucial to ensure the safety of children, vulnerable communities and minority groups among others. It is likely that if a platform is not end-to-end encrypted or if the protection is weakened, then the perpetrators will simply shift to another secure platform. The report acknowledged that end-to-end encryption is a necessary first step in ensuring online safety.[10] There is no evidence to show that by weakening encryption Law Enforcement Agencies (LEAs) can always catch the criminals, but by weakening encryption, the privacy of the children will be compromised for sure.

B. THE INDIAN ENCRYPTION DEBATE

The digital revolution spanning the last few decades has seen India as an active participant. There have been significant transformations within the communications sector, financial inclusion, e-commerce and e-governance. Most recently, the encryption debate in India took a remarkable shift with the TRAI coming up with a set of concrete recommendations explaining why breaking encryption would compromise the security architecture of encrypted platforms.[11] 2014 witnessed the creation of a Unique Identity-Aadhar, a national biometric identity programme. It created a centralised database that, in February 2018, contained the personal data of over 1.17 billion citizens.[12] The Supreme Court in the Puttaswamy-I judgement explained that the Government access to personal data for legitimate national security concerns is a reasonable restriction on right to privacy. The Apex Court also reiterated that such exceptions must be narrowly tailored and government practices must be privacy enabling.

Encryption has been part of policies dating back to the 1998, specifically within the **Indian Telegraph Act, 1885**. Section 5 of the Telegraph Act[13] and Rule 419A of the Indian Telegraph Rules, 1951[14] empowered the government to lawfully intercept and monitor communication. The validity of Section 5 of the Act was challenged before the Supreme Court in the case of **PUCL v. Union of India**.[15] The Court refused to strike down the Section, instead listed guidelines to be followed to check arbitrariness in interception orders. Additionally, **Section 84A of the Information Technology Act, 2000**, was introduced through an amendment in 2008. It allowed the government to prescribe modes and methods for encryption to ensure secure use of the electronic medium and promote e-governance and e-commerce. Following a more prescriptive mandate of regulation, **Section 69 of the IT Act, 2000**, allowed the Central and State governments to monitor and collect information through any computer resource for cybersecurity. **Rule 9 of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009**, provided that an order for

es-trends-and-latest-developments-within-eu-and-beyond

10 United Nations, UNICEF Office of Research - Innocenti, Florence, (2020). Encryption, Privacy and Children's Right to Protection from Harm, Innocenti Working Papers no. 2020-14. https://www.unicefirc.org/publications/pdf/Encryption_privacy_and_children's_right_to_protection_from_harm.pdf.

11 Telecom Regulatory Authority of India, Recommendations on Regulatory Framework for Over-The-Top (OTT) Communication Services, (Sept. 14, 2020) https://www.trai.gov.in/sites/default/files/Recommendation_14092020_0.pdf.

12 Bedavyasa Mohanty, The Encryption Debate in India, The Carnegie Endowment for International Peace, (May 30, 2019) https://carnegieendowment.org/2019/05/30/encryption-debate-in-india-pub-79213

13 The Indian Telegraph Act, §5, No. XIII, Acts of Parliament, 1985, (India).

14 Indian Telegraph Rules, Rule 419A (1951).

15 Peoples' Union for Civil Liberties v. Union of India & Anr., (1997) 1 SCC 301.

decryption could relate to any information sent to or from a 'person or class of persons' or relate to 'any subject matter'.
India, similar to other countries, has been apprehensive of the increase in encrypted technology because of its alleged role in impeding national security investigations.

It was in this atmosphere that the **National Encryption Policy was formulated in 2015**. However, it didn't manifest to a statutory law because of the criticism it received. Critics opined that it was more of a 'decryption' policy, because it only allowed platforms to function if they complied with the mandatory regulatory mechanism.[16] The policy was said to simply secure government access to encrypted data, rather than securing user data. **The Draft Intermediary Guidelines of 2018** which were expected to have a significant impact on encryption policies, had also received comments from all concerned stakeholders pertaining to the onerous traceability requirement introduced. More recently, this argument was expanded to include the threat to public order due to proliferation of fake news on encrypted platforms, which at times would lead to lynchings and the challenges pertaining to CSAM on the internet.

The notification of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, jolted the Indian encryption ecosystem. Rule 4(2) of the IT Rules, 2021 mandated originator traceability for all Significant Social Media Intermediaries (SSMIs) providing messaging services. While on one hand we have the Kamakoti solutions and the proposal for Alphanumeric Hashing, on the other we have experts and organisations explaining the legal technical and policy challenges associated with implementing the same.

It is in this background that we invited expert stakeholders in the Indian encryption space to declutter the debate and propose a way forward.

16 Livemint, What was the draft encryption policy and why it was withdrawn (Sept.22, 2015) https://www.livemint.com/Politics/RZtAGhM6IjDBWujiK6ysEP/What-was-the-encryption-policy-and-why-it-was-withdrawn.html

TRACING THE INDIAN ENCRYPTION DEBATE

1999

Kargil Review Committee
Recommended the use of encryption and decryption by intelligence agencies.

Department of Telecommunications
Prohibited the use of 40-bit key length without prior authorisation. The ISP's were expected to obtain permission and submit decryption keys to the government.

2000

Information Technology (Certifying Authorities) Rules, 2000
Introduced the use of Public Key Infrastructure (PKI) for encrypting, signing and authenticating transactions in order to increase online security.

SEBI's Report on Internet Trading
Recommended that a 64/128-bit encryption standard to secure transactions and online trading must be available for free use.

2001

Reserve Bank of India Internet Banking Guidelines
Recommended the use of 128-bit Secure Socket Layer (SSL) encryption as an alternative to PKI for increased browser security.

2008

Information Technology Act Amendment (Section 69)
Authorised the Central and State governments to intercept, monitor or decrypt information necessary for the security and/ or sovereignty of the country, for preserving public order or investigating crime.

2009

Information Technology Act Amendment (Section 84A)
Provided for the modes and methods for encryption to promote e-governance and e-commerce.

Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (Rule 9)
Allowed decryption orders to relate to any information sent to or from "a person or class of persons" or "relate to any subject matter".

2010

SEBI circular on "Securities Trading using Wireless Technology"
Provided that the Department of Telecom will govern mandatory use of encryption for internet-based trading.

2011

Information Technology (Intermediary Guidelines) Rules, 2011
Mandated that intermediaries must trace the originator of information on their platform when ordered to do so by an authorised government agency.

2015

Draft National Encryption Policy, 2015
Permitted the use of encryption subject to several obligations imposed on businesses and citizens alike. Ensured LEA's and other authorities had the power to enforce decryption.

2018

Draft Information Technology (Intermediary Guidelines) Rules, 2018
Mandated proactive monitoring of illegal content and ensure traceability of originator of the content.

2019

Personal Data Protection Bill, 2019 (Clause 24)
Mandated the use of encryption by every data fiduciary and processor, among other measures, to secure personal data.

2020

Report of the Ad hoc Committee in the Rajya Sabha
Recommended breaking end to end encryption to avail safe harbour as a result of the Committee's examination of pornography on social media and it's effect on children and society as a whole.

POCSO Rules on Child Safety, 2020
Listed the types of information to be shared by intermediaries with LEA's to check CSAM.

A communique released by Five Eyes along with India and Japan
Recommended the Big Tech to ensure traceability in end-to-end encrypted platforms.

TRAI Recommendations on Regulatory Framework for Over-The-Top (OTT) Communication Services
Recommended that no regulatory intervention was required in the security architecture of end to end encrypted platforms, as meddling with the same may lead to cyber vulnerabilities.

Janani Krishnamurthy v. Union of India
Transferred to the Supreme Court, the case deals with the extent of liability of the Intermediaries to provide information regarding user generated content.

2021

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
Rule 4(2) mandated Originator Traceability for Significant Social Media Intermediaries.

REVISITING THE REGULATORY MODELS UNDER THE INFORMATION TECHNOLOGY ACT

Dated: October 30, 2020

Keynote Speaker: Dr. Gulshan Rai, India's First National Cyber Security Coordinator

Moderator: Mr. Saikat Datta, Strategic Advisor to The Dialogue and NullCon

Key Discussants:

- Mr. Yashovardhan Azad, Former Special Director, Intelligence Bureau, Secretary (Security) Government of India, and Central Information Commissioner;
- Mr. Vinayak Godse, Vice President, Data Security Council of India;
- Dr. Debayan Gupta, Asst. Prof. of Computer Science, Ashoka University;
- Mr. Anand Venkatanarayanan, Independent Cybersecurity Researcher;
- Ms. Sreenidhi Srinivasan, Senior Associate, Ikigai Law;
- Mr. Udbhav Tiwari, Public Policy Advisor, Mozilla Foundation.

The virtual stakeholder consultation was held to deliberate upon the TRAI recommendations on Regulatory Framework for Over-The-Top (OTT) Communication Services. The discussion featured various stakeholders belonging to the public and private sector in order to gain multiple perspectives. In their discussion of this regulation, they examined the economic, social and security aspects of the same. While most believe that encryption only weakens a country's national security, the panellists viewed encryption from a different lens where its deployment furthers the interests of national security. While it's important to find meaningful solutions to cater to the legitimate needs of the LEAs, it was noted that backdoor access is not the solution. The panellists stated that the overarching security and safety concerns that arise out of the creation of backdoors were enough to make a case against the same. Moreover, it was agreed that increased transparency and accountability within the regulatory authorities would be extremely beneficial in developing trust among the users.

The discussion raised some extremely pertinent issues around the following themes:

A. CHALLENGES AROUND ENCRYPTION

The most hotly debated challenge pertaining to encryption at the global stage is that of its alleged threat to LEAs access to communication. The common misunderstanding is that without access to encrypted data, LEAs won't be able to perform their duties efficiently. While catering to such requirements the State must **balance the interests of the users in the digital space**, such as their right to

privacy and free speech, with the need to share data with government authorities. It is equally noteworthy that users have no guarantee of their data being safe due to the **lack of a robust data protection regime**. In order to appreciate the need for such a regime, the case study of the Minnesota Database queries was discussed.[17] In Minnesota, more than 62% of police officials were reported to use the surveillance capabilities of the State to surveil over their ex-wives and ex-girlfriends, forming an apt example of this threat. **Without a robust data protection regime, it is indeed precarious for citizens to trust institutions that collect and store their data.**

While the aforementioned issues are being debated at a global stage, India has the drawback **of limited awareness on the need for encryption technology**. This extends not just to the working of the technology but also to the functionality of institutions that deploy and monitor encryption technology. As a result of this, there is a **lack of investment** in this field which does not encourage R&D. India has also failed to develop institutions with **well-defined roles and responsibilities** that could facilitate institutional strength and promote trust in the ecosystem. The nurturing of the traditional surveillance capabilities of LEAs, though crucial in nature, cannot be done to the extent that it creates cyber vulnerabilities open to exploitation by hostile actors.

Breaking encryption would merely empower a broken system which needs to be overhauled. In other words, if gaining backdoor access to encrypted data is the only way an investigative agency can successfully identify perpetrators, it points to a much larger problem within the criminal justice system. In this context, a stakeholder discussed that even when the NSA had access to call logs of the entire country, the most they could achieve was the identification and flagging of a wire transfer of $8500 between those belonging to a Somalian terrorist group.[18] There is little to no research to support claims relating to the absolute necessity of intercepted or decrypted data actually aiding investigations and assisting LEAs in bringing this evidence before Courts. It was pointed out that decrypting platforms may not lead to much success, as perpetrators are likely to simply switch to another encrypted platform for communication.[19] Therefore, the introduction of backdoors, without fundamental regulatory changes to the traditional systems of LEAs, will do little to curb cybercrime or ensure national security. Accordingly, it was agreed that there is a legitimate need to ensure transparency and accountability within the LEAs, and providing blanket power to any institution is not a plausible solution.

B. BACKDOOR ACCESS TO ENCRYPTED DATA

It was pointed out that the **deliberate introduction of a vulnerability is a security hole for everyone** in the system and is not exclusive to any one party. It was agreed that weakening encryption would be tantamount to weakening India's national security. The Greek Watergate Scandal was discussed in this respect. In what is also popularly known as the *Athens Affairs*, the political and military elites of Athens were spied on using a vulnerability introduced for lawful interception.[20] Accordingly, breaking

17 CBCS News, Police sometimes misuse confidential work databases for personal gain: AP, CBCSN, (Sept. 30, 2016) https://www.cbsnews.com/news/police-sometimes-misuse-confidential-work-databases-for-personal-gain-ap/.
18 Charlie Savage, NSA Chief Says Surveillance Has Stopped Dozens of Plots, New York Times, (Jun. 18, 2013) https://www.nytimes.com/2013/06/19/us/politics/nsa-chief-says-surveillance-has-stopped-dozens-of-plots.html
19 Robert Graham, How Terrorists Use Encryption, CTC Sentinel, Vol. 9 Issue 6, CTCS 20 (June 2016) https://www.ctc.usma.edu/how-terrorists-use-encryption; See also Daniel Castro, Why New Calls to Subvert Commercial Encryption Are Unjustified, Information Technology and Innovation Foundation, (Jul 13, 2020) https://itif.org/publications/2020/07/13/why-new-calls-subvert-commercial-encryption-are-unjustified
20 Vassilis Prevelakis and Diomidis Spinellis,The Athens Affair: How some extremely smart hackers pulled off the most audacious

encryption can render a State susceptible to cyber vulnerabilities. Among the various arguments cited against weakening end-to-end encryption, the most important have been highlighted below:

- The high-end encryption technology protects not just users and businesses, but also Critical Information Infrastructures (CII) of the government like those of Aadhar and Aarogya Setu among others. In the *Aadhar judgement*[21] the Government stated that in keeping with security principles[22], and ensuring 'security of data and protection of breach[23] encryption, has been employed as a part of UIDAI. As part of Atmanirbhar Bharat, the Army has also recently released an end-to-end encrypted messaging App called 'SAI', i.e., Secure Application for Internet.[24] Thus, the importance of high-end encryption to protect domestic interests cannot be emphasized enough.

- In addition to that, a vulnerability would create the impression that the technology sold in India is compromised, which would discourage foreign companies from buying or investing in the same.

- Another aspect that deserves due consideration is that of **cross border data flows**, which would be adversely affected with the creation of backdoor access to encrypted data.

The experts also discussed the recommendations by TRAI to the Department of Telecommunications, wherein the former opined that the security architecture of end-to-end encrypted platforms must not be tinkered with in order to ensure the safety and security of the platform. The experts pointed out that creation of backdoors would render the platform accessible to the government but also render it vulnerable to attack by hostile actors.

The legal experts on the panel deliberated on whether **backdoors would stand the tripartite test set forth in Puttaswamy judgement**. The three prongs of the Puttaswamy Case to restrict fundamental right to Privacy have laid down that (a) the action must be sanctioned by law; (b) the proposed action must be necessary in a democratic society for a legitimate aim; (c) the extent of such interference must be proportionate to the need for such interference. The Puttaswamy judgement also requires a case-by-case analysis on whether the intrusion is valid. Breaking encryption would render the whole population susceptible to cyber-vulnerabilities. Thus, creation of backdoors, which are open not just to the government but also to other hostile actors, compromises the privacy of all. Secondly, there are other less privacy-invasive means to obtain the necessary information required by LEAs, such as by accessing meta-data rather than content data, which means such laws fail the necessity test as well. A blanket ban on encryption, by introducing vulnerabilities to ensure traceability would entail major threats of mass surveillance and instances of curbing dissent. Thus, the traceability requirement renders the entire citizenry vulnerable and fails the 'proportionality' test too.

cell-network break-in ever, IEEE Spectrum, (Jun. 29, 2007, 14:07 GMT)
21 K.S. Puttaswamy v. Union of India, (2019) 1 SCC 1.
22 Ibid, p 153.
23 Ibid, p 227.
24 Government of India, Ministry of Defense, Army Launches Secure Application for Internet (SAI), (Oct. 29 2020 12:49PM) https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1668346.

RECOMMENDATIONS

1. **Defining responsibility** is crucial. The roles and limitations of the LEAs must be defined in order to increase transparency and accountability. This will also help re**duce the trust deficit**.

2. **Increased investment** in technology is essential to not only understand the working of the technology but to also encourage R&D.

3. **Development of cryptography** in a collaborative manner is essential. While cooperation with tech giants can be beneficial, the role that startups can play cannot be ignored. This is primarily because India already has the necessary expertise, but the Government needs to **improve its outreach.**

4. **Recently developed sectors** must be taken into consideration before creating backdoors. Sectors such as **health, digital products and digital payments systems** necessitate the deployment of encryption, and without encryption, the digital ecosystem will witness stagnation.

5. **Nurturing a secure cyber infrastructure** is crucial to ensuring safety and security of the users. Creation of backdoors will render the users vulnerable to cyberattacks by hostile actors. Thus, TRAI's recommendation that the security architecture of end-to-end encrypted platforms must not be tinkered with, should be adhered to else it will lead to more challenges than it seeks to resolve.

6. The focus needs to be on **capacity building for the LEAs** to conduct meta-data analysis through meaningful cooperation by the Big Tech, the industry and academia, instead of breaking encryption and rendering the content data of all citizens susceptible to cyber-attacks.

SECURING INDIA'S CYBER SPACE: THE ROLE OF ENCRYPTION

Dated: November 20, 2020

Keynote Speakers: Lt. Gen. (Dr.) Rajesh Pant, National Cybersecurity Coordinator

Moderator: Mr. Saikat Datta, Strategic Advisor to The Dialogue and NullCon

Key Discussants:

- Dr. Debayan Gupta, Asst. Prof. of Computer Science, Ashoka University;
- Ms. Arya Tripathi, Partner, PSA Legal;
- Mr. Aseem Jakhar, Co-Founder, Nullcon and Director, Payatu

The pandemic induced r**apid adoption of the digital ecosystem** and triggered an urgency to secure the online space. Various technologies such as the Aarogya Setu App, e-commerce, online banking, ed-tech or telemedicine, all rely on encryption enabled cyber security to ensure user privacy and secure connectivity in a post-COVID India. The consultation was held in order to discuss ways to mitigate cybercrime and to create a strong cybersecurity regime.

In order to ensure a well-rounded discussion, various stakeholders from the public as well as the private sector were invited as speakers. It was pointed out that encryption was an essential part of cybersecurity. However, the panellists emphasised that encryption alone was not enough to create a safe cyberspace. Increased accountability and transparency on part of the regulatory authorities and increased awareness and investments were key in developing a robust cybersecurity policy.

The key issues raised in the course of the discussion were as follows:

A. THE NEED TO TACKLE CYBERCRIME

Cyber security has become critical to the security of a country, both offline and online. It was pointed out that there has been **a loss of approximately $2 billion**[25] on a global scale as a result of cyber crime. India is one of the top 5 countries that is targeted by cybercrimes and **ranked 23rd in the United Nations Global Cybersecurity Index**.[26] It is also the country with the third highest number of internet users.

25 Intel Security & McAfee, Net Losses: Estimating the Global Cost of Cybercrime, (2014) https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_McAfee_PDF.pdf.
26 PTI, India Ranks 23rd among 165 nations in cybersecurity index, The Economic Times, (Jul 06, 2017, 10:14 PM IST) https://economictimes.indiatimes.com/tech/internet/india-ranks-23rd-among-165-nations-in-cybersecurity-index/articleshow/59478111.cms?from=mdr.

The panellists observed that one of the most basic requirements of combating this is to **increase the use of high-end encryption and promote R&D on the same**. Encryption makes cybersecurity more resilient, while also maintaining the privacy of the users. One of the reasons for India's 23rd rank on that Index was said to be that India has not developed encryption technology of its own. The panellists believed that one of the reasons cybersecurity has not seen much development in India is because cybercrime is not perceived to be an imminent threat.

There were several perspectives brought to light throughout the discussion:

- Ms. Arya Tripathi pointed out that the common approach taken within the country is to replicate foreign technology. While replication of technology is easy, it does very little in developing a robust cybersecurity regime. In order to have an effective cybersecurity regime, a robust policy that is receptive to society and the dynamic nature of technology is essential.

- Building on the importance of a robust cyber security regime, Mr. Aseem Jakhar explained that it is like a doctor recommending to drink water as a part of a healthy diet. Its necessity is obvious and should be a given whenever cybersecurity is talked of, but encryption alone is not enough.

- Dr. Debayan Gupta pointed out that there is a need to take cybersecurity as seriously as we take our finances. At present, it remains an afterthought. While regulatory mandates are commonly posed as effective solutions, unless there is actual awareness created regarding cybersecurity, people will deal with the regulation within their PR campaign.

B. ENCRYPTION DEBATE: PRIVACY VS. SECURITY

The speakers noted that it was a myth that encryption and national security cannot work in collaboration with one another. One of the examples cited by Mr. Kazim Rizvi, Founding Director of The Dialogue, to justify this claim included the Personal Data Protection Bill, 2019, which recommends the use of encryption vide Clause 24 while also focussing on national security. There exist multiple such examples on why encryption is crucial to ensure security. The Indian Army developed a communication platform called SAI with end-to-end encryption, and various platforms that emerged during the COVID-19 pandemic, like Zoom, also turned to encryption when questions were raised about its lack of privacy and security. Even the communique released by the Five Eyes and the Draft Resolution of the Council of the EU acknowledge the crucial role that encryption plays in securing the users' right to privacy. Afterall, **collective user security furthers national security.**

One of the questions raised during the consultation was whether encryption and interception are mutually exclusive concepts. Ms. Arya Tripathi answered that **encryption and interception are concepts that go hand-in-hand and more importantly, should go hand-in-hand**. The building block of a country is its citizens and the citizens are entitled to informational privacy. The right to informational privacy has been elevated to the status of a fundamental right allowed for the natural inclusion of checks and balances. **However, if interception was to be separated from this fundamental right,**

you take away the checks and balances that were instituted as well. Therefore, it must be kept in mind that in case of interception, the intercepting party must always sufficiently justify their claims. She pointed out how when it comes to police surveillance, a warrant is essential to obtain access. The technology space deserves the same respect and protection.

C. DOMESTIC ENCRYPTION ECOSYSTEM

India was the leader in policy making with regards to the Information Technology (IT) sector. However, the panellists observed, since 2013 India has been left behind. New threats within cyberspace, and the development of Industry 4.0 technologies like Internet of Things (IoT) etc. have not received enough attention. Therefore, there is a need for a robust national cybersecurity policy, which can revive India's commitment towards a secure cyberspace.

There are several reasons for the limited development within this field. Firstly, there is a **lack of awareness**. The average citizen is not concerned with 'privacy' in the online sphere for various reasons, with poverty and lack of education topping the list. Access too is a significant problem, the digital divide in India, though shrinking slowly, the average Indian still does not have access to secure online space. Access to the internet, through mobile phones or computers, is disproportionate. Women and people belonging to lower income groups have limited access to the same.[27] Their main priority is to earn their livelihoods, so they are not as bothered with a lack of data protection as a more privileged individual would be. The panellists pointed out that both physical hygiene and cyber hygiene are important and they need to be looked at in the same manner. They are concepts that must be taught in formative years in order to develop the culture of being cyber aware. It must be moulded and accepted as a survival skill.

Secondly, there is a **lack of infrastructure**. This ties into the **lack of research and funding**. As a result of the lack of awareness, there is limited interest to fund R&D projects within this space. Therefore, the technology has barely advanced within India. Mr. Aseem Jakhar pointed out that startups and SMEs have little to no scope for development within this space. Lastly, there is also a **lack of effective communication** and limited collaboration between the various stakeholders. There also exists a legitimate need to build the capacity of the LEAs. To this end it is crucial that the State, academia, and the technology companies work together to find innovative solutions to the challenges faced by the LEAs and build their cyber-capabilities.

27 Anushree Verma, Bridge the #DigitalDivide: On chronic inequalities in internet access, Internet Freedom Foundation, (Jan. 7, 2021) https://internetfreedom.in/on-chronic-inequalities-in-internet-access/.

RECOMMENDATIONS

1. Encryption must be identified as the **fundamental building block** in the cybersecurity space. In addition to that, it's important to introduce **cybersecurity metrics** and have a robust **cyber insurance** regime in place.

2. Regulations must **highlight the manner of reporting cybercrimes and sharing metadata in a more efficient and user friendly manner**. The regulations must focus on ease of access, and provide all procedural details in order to ensure transparency and accountability, while all requests must also adhere with the standards laid down in the Puttaswamy judgement.

3. A **cybersecurity policy** must be drafted with absolute clarity. There must be no ambiguity with regards to what the policy seeks to achieve, the principles in place, the processes and protocols etc. **Increased transparency** will lead to more accountability and better security of the state and its citizens.

4. **Encryption is the first line of defense**. There must be further development of technology in order to increase security and mitigate risks. For example, honey encryption which creates a 'honey trap' so that a hacker cannot find his way around it.

5. **Civil liability must be clarified** (intermediary, hardware manufacturer etc.) Collective liability is another aspect that warrants analysis.

ORIGINATOR TRACEABILITY: ANALYSING THE IMPACT OF IT RULES, 2021

Dated: April 23, 2021

Moderator: Mr. Saikat Datta, Strategic Advisor to The Dialogue and NullCon

Key Discussants:

- Mr. Shivam Singh, Advocate, Supreme Court of India
- Mr. Vasudev Devadasan, Independent Lawyer
- Mr. Anand Venkatanarayanan, Independent Cybersecurity Expert

The discussion on originator traceability was held as a part of a virtual stakeholder consultation held to analyse the impact of the IT Rules, 2021, on India's platform regulation ecosystem. Originator traceability was recognised as an important point of discussion in light of the weaponisation of fake news and misinformation in recent times, and the debate on balancing privacy with national security concerns.

The discussions featured legal, technical and policy experts to analyse the need and effectiveness of the updated rules relating to traceability and encryption, as well as how they hold against legal standards. During the discussion, the rules were considered in light of the privacy jurisprudence propounded through the Puttaswamy judgment, and there was consensus on their failure to satisfactorily fulfill the proportionality test laid down by the court. It was also noted that traceability would be hard pressed to fulfill its desired purpose for the law enforcement in identifying perpetrators for the defined offences and providing concrete evidence against them in courts. This was specifically emphasised alongside the far-reaching adverse consequences that enforcing originator traceability would have on end-to-end encryption.

Finally, the discussion highlighted various practical issues that would be faced by the industry in implementing the provisions, and it was agreed that the various compliance standards could potentially hinder innovation and meaningful access to liberty. Accordingly, more conventional forms of tracing a perpetrator through methods that didn't break encryption were agreed on to be useful alternatives that needed better implementation.

The key issues raised in the course of the discussion were as follows:

A. TRACEABILITY VIS-A-VIS ENCRYPTION

End-to-end encryption was identified as a very crucial aspect of maintaining confidentiality in technologically driven communications. It came in response to the need to avoid the snooping of third

parties in private conversations, and with it came the concept of 'cryptographic deniability'[28] as per which information on the contents of conversation is denied even to the intermediary hosting the communication.

The discussion brought out how this meant that people could now have conversations with another person with no proof that could be brought in a court of law to show that the messages were exchanged. The panelists observed that this characteristic of end-to-end encryption goes at direct odds with the new rules enforcing traceability, which aim to identify the originator of problematic content on OTT platforms. It was also highlighted that traceability itself is an ineffective tool for LEAs and can easily be spoofed, which is considered highly relevant in light of how this would dismantle encryption - an essential shield for the protection of user privacy.

On the topic of alternative methods of enforcing originator traceability that didn't call for decryption, it was noted that solutions such as the use of hashes and the one proposed by Dr. Kamakoti amounts to mere wishful claims with little scientific backing and proof in algorithmic theory.[29] Any valid way to rework the complex algorithm for end-to-end encryption, which would allow traceability, was seen to require the same level of rigorous research and fault proofing as had gone behind putting the former model in place. The conversation highlighted how rushing in with ill-formed mechanisms around encryption tends to provide dangerous loopholes to our security framework, and should thus be viewed with a critical eye.

B. THE LEGAL IMPLICATIONS OF TRACEABILITY ON THE RIGHT TO PRIVACY AND THE LAWS ON EVIDENCE

Introducing traceability entails weakening encryption, and thus must be viewed with the lens of user privacy. To that end, the discussion attempted to measure the IT Rules 2021[30] on tracing the first originator against the privacy jurisprudence propounded in the Puttaswamy judgement.

Mr. Shivam Singh systematically laid down an analysis of the rules in light of a four-part test to determine the validity of restrictions on privacy, which calls for the existence of a legitimate aim, suitability or rational nexus, necessity, and a balance. He made a point-wise observation on how the new rules seem to fail on all four accounts.

- The **legitimate aim of preventing the threat to national security** was considered **too wide and too vague** to be an appropriate articulation of the aim;

- The **suitability** of using orginitator traceability for **catching cybercriminals** was countered by

28 Moxie Marlinspike & Trevor Perrin, The X3DH Key Agreement Protocol, Signal, (Nov. 4, 2016) https://signal.org/docs/specifications/x3dh/.
29 Anand Venkatanarayanan, Dr Kamakoti's Solution For WhatsApp Traceability Without Breaking Encryption Is Erroneous And Not Feasible, Medianama, (Aug. 13, 2019) https://www.medianama.com/2019/08/223-kamakoti-solution-for-traceability-whatsapp-encryption-madras-anand-venkatanarayanan/?fbclid=IwAR3s_Gp7UPGrICGR1y_Yf4biU5OF4-N68aTRKtJPpRPvoDTE_Y42Wc051pk.
30 Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, Rule 4(2), No. G.S.R. 139(E), Acts of Parliament, 2021, (India).

laying emphasis on the **option of simply shifting to the various small alternate platforms** that would continue to provide encryption;

- The argument for the **necessity** of the specific approach of traceability was shunned for being a '**one-size-fits-all approach**' that could not be the least restrictive measure; and

- It was shown to be the **absence in the balance of the use of backdoors** to fulfill the **purpose** of the rules.

In a similar vein, Mr. Vasudev Devadasan shed light on the constitutional perspective to this issue and showed how the **widely worded law failed the proportionality test**. In addition to the same, it was observed that the question on can there be traceability without decryption was already giving too much leeway to the government where the question should be on whether the government should be allowed traceability at all. Using the same against disinformation, sedition, and fake news on WhatsApp was seen to not fall in line with the articulation of the specific categories of offences in the rules.

The discussion also brought out how there may in fact be less restrictive measures to trace and catch cybercriminals through basic subscriber information of user profiles and other legally collected information through geolocating and the Telegraph Act in specific cases. Additionally, it was noted that while the new IT rules attempt to provide safeguards for privacy in the text of the law itself, they are largely ineffective and rendered meaningless in light of the lack of transparency or oversight and judicial scrutiny.

The **efficacy of traceability was also scrutinised for its use as a form of digital evidence**, in light of the need to establish a chain of custody under Section 65B of the Evidence Act. The panelists observed that while the technicalities around concretely tracing a perpetrator should make its use as an evidence complicated, various such procedural requirements often don't translate as strictly in implementation, and proceeded to point to a hands-off approach with reliance even on expert opinion on digital evidence.

Finally, the discussion pointed to a need to work on the lack of transparency that exists in the new framework, and the importance of making an understanding of issues around encryption, privacy, and traceability more accessible to the citizens and the judiciary alike.

C. IMPACT OF THE RULES ON START-UPS AND INNOVATION

The legal framework regulating an industry often plays the dual role of protecting both the citizens of the country that interact with the services offered as well as protecting the enterprises that invest resources in building that industry. Accordingly, the regulations and compliance standards enforced can have concrete economic ramifications for a country, as they determine the ease of doing business in that nation. In this light, the panelists pointed to how the **IT Rules 2021 could adversely impact small scale start-ups that may now be excessively caught with grievance redressal**, leaving them little time for content creation and innovation.

Implementing the rules on traceability were identified as problematic even from a coding perspective, in light of how complicated the process of finding the true first originator can be for any platform with the highly sophisticated tech available at the user's disposal. Finding backdoors to encryption for traceability also calls for a reworking of the algorithms from the platform's end. Accordingly, with the increasingly privacy preserving laws on a global scale, such an updated product could prove to be hard to sell in other countries.

RECOMMENDATIONS

1. **Originator traceability fails to fulfill the Puttaswamy test. It should not be implemented given its impact on end-to-end encryption** and considering the crucial protection provided by the latter against cyber threats to national security.

2. **Alternatives to decryption for tracing originators** of problematic content exist under the present legal framework and should be given preference.

3. **Technical knowledge needs to be provided in courts through experts** more meaningfully for just use of evidence gained through tracing.

4. **The Mandate for originator traceability should be delayed and technical experts should be consulted** to understand the challenges involved in implementing the originator traceability mandate and recommend the way forward.

5. **Rules on originator traceability result in practical complications for the industry** and become an obstacle to small businesses and innovation. Encrypted platforms with traceability features or backdoors will be extremely difficult to sell in the international market. It's impact on the business in India must be acknowledged and adequately addressed.

6. The **privacy safeguards** incorporated in the new rules on the use of originator traceability leave little space for **transparency and judicial scrutiny** and should be reassessed.

KEY TAKEAWAYS

01. A mandate for backdoors or originator traceability fails to fulfill the Puttaswamy test. It should not be implemented given its impact on end-to-end encryption and considering the crucial protection provided by the latter against cyber threats to national security. Overarching powers to surveil do not align with our constitutional mandate. A backdoor into an encrypted platform would render the entire population susceptible to cyber vulnerabilities and disproportionately restrict their fundamental right to privacy and free speech. Moreover, backdoor access leads to challenges like mass surveillance, data theft, identity theft among others, and fails to meet the Puttaswamy test laid down by the Hon'ble Supreme Court.

02. Rules on originator traceability result in practical complications for the industry and become an obstacle to small businesses and innovation. Encrypted platforms with traceability features or backdoors will be extremely difficult to sell in the international market. It's impact on the business in India must be acknowledged and adequately addressed.

03. Increased awareness regarding the importance of cybersecurity and the role of encryption is essential in creating more opportunities within this space. Without proper understanding of the technology, the policies and technology that is developed will fall short of the ideal standard.

04. Increased investment in technology is essential to not only understand the working of the technology but to also encourage R&D. Equally important is the development of cryptography in a collaborative manner. While cooperation with tech giants can be beneficial, the role that startups and smaller research organisations can play cannot be ignored.This will, therefore, encourage development of technology and will only strengthen India's cybersecurity regime. There is also a need to indigenise encryption technology, the Indian start-ups have potential to make a mark in the global encryption market and this will also help better protect domestic interests.

05. All policies pertaining to cybersecurity must be formulated with absolute clarity. This not only encourages positive regulation but also helps in curtailing the trust deficit that exists between the regulators and users. The roles and limitations of the LEA's must be defined in order to increase transparency and accountability. These regulations must provide information regarding the manner of reporting a threat or event, the relevant authorities and the approved authorities to share personal information.

06. While encryption is essential, it is important to remember that it cannot be the only measure taken to tackle cyber crime. Encryption is a necessary line of defence, but there is a need to nurture a more robust cybersecurity space.

07. The implementation of the IT Rules, 2021 should be delayed and technical experts should be consulted to better address the challenges involved and recommend the way forward. Haste in implementing the Rules could create more challenges than what they seek to resolve.

EXPERT SPEAK

"The State may have reasons in the legitimate interest of national security to seek access to information. A blanket measure to seek access which renders the entire platform susceptible to attacks by hostile actors must not be relied on. Implementing such a measure will not only compromise user privacy but also national security. The State must assess the technical feasibility of the measures it directs the platforms to implement to effectuate exceptional access while also ensuring that the measure does not fail on the anvil of the Puttaswamy test."

Mr. Yashovardhan Azad
Former Secretary (Security) and Special Director, Intelligence Bureau

"We need to devise technology and frame policy keeping in mind the realities of the technology in place today. While there is a call for bringing about balance, it is easier said than done"

Dr. Gulshan Rai
Former National Cyber Security Coordinator, Government of India

"The Idea that Encryption is merely locking something in a safe and putting it away is an archaic one that has been obsolete for decades now. Encryption today is a lot more complex and it does a lot of things like putting guarantees on the way my data will be processed even after giving you that data or sharing data without revealing too much private information or blocking it from being used for any other purpose than the one it was collected for".

Dr. Debayan Gupta
Assistant Professor of Computer Science, Ashoka University

"There is technical dichotomy between end to end encryption and that of tracing the originator for a message as the new rule states as a mandatory requirement."

Dr. Aruna Sharma
Former Secretary, Ministry of Communication and Information Technology, Government of India

“From our Industry and the country's standpoint, I can say that the ROI on research in this field is not realized at the pace it should be. Cyber security innovation, unfortunately comes with a hefty price in terms of initial investment. It's certain that we have the research capabilities as well as the right expertise locally, however, accessibility to the required funds is not easy and is the primary inhibitor to growth.”

Mr. Aseem Jakhar
Co-Founder, Payatu and NullCon

“Encryption is required at multiple levels whether it be making the cyber space more resilient, for enabling organisations to maintain price sensitive information having an economic impact, or even a more granular level where I come from, having a peace of mind that I can interact on an encrypted platform”

Ms. Arya Tripathi
Partner, PSA Legal Counsellors

“We need to see whether these backdoors to encryption meet a balance with privacy, and ask if there is a possibility of ensuring that what the regulator is seeking is even possible to achieve with the balance, or is it just a case of very suave legal jargon being hurled at people.”

Mr. Shivam Singh
Advocate, Supreme Court of India

"We need to arrive at a middle ground where we improve legal processes around data sharing instead of weakening technology, which will lead to an outcome that is bad for everyone.”

Mr. Udbhav Tiwari
Public Policy Advisor, Mozilla Foundation

"It must be seen if backdoors or any other government action that weakens encryption can meet the test laid down by the Supreme Court in the Puttaswamy case, which is that the action is based in law, it is needed for a legitimate state aim, and the means are proportionate to the aim."

Ms. Sreenidhi Srinivasan
Principal Associate, Ikigai Law

"Using traceability, can the government prosecute somebody who they allege is spreading disinformation and fake news? The answer is 'highly unlikely'. Traceability can be spoofed so it doesn't meet the threshold of beyond reasonable doubt. It is also unclear whether the offences the government wants to prosecute meet the minimum punishment thresholds to justify invoking the traceability requirement"

Mr. Vasudev Devadasan
Independent Lawyer

"Most hacks and attacks are done by disabling the encryption or working around the same. In today's time, hackers understand that fooling people is far more easier than breaking encryption so they workaround the same through fake OTPs and other parallel systems to gain access to encrypted devices. If the objective of the Government is to stop these attacks, it is possible through targeted attacks and interceptions and there is no real need for a blanket policy of a backdoor that affects everyone instead of just the offender. Your policy cannot be about making 99% of the population safe from the 1% by making all 100% of them unsafe"

Mr. Anand Venkatanarayanan
Independent Cyber Security Professional