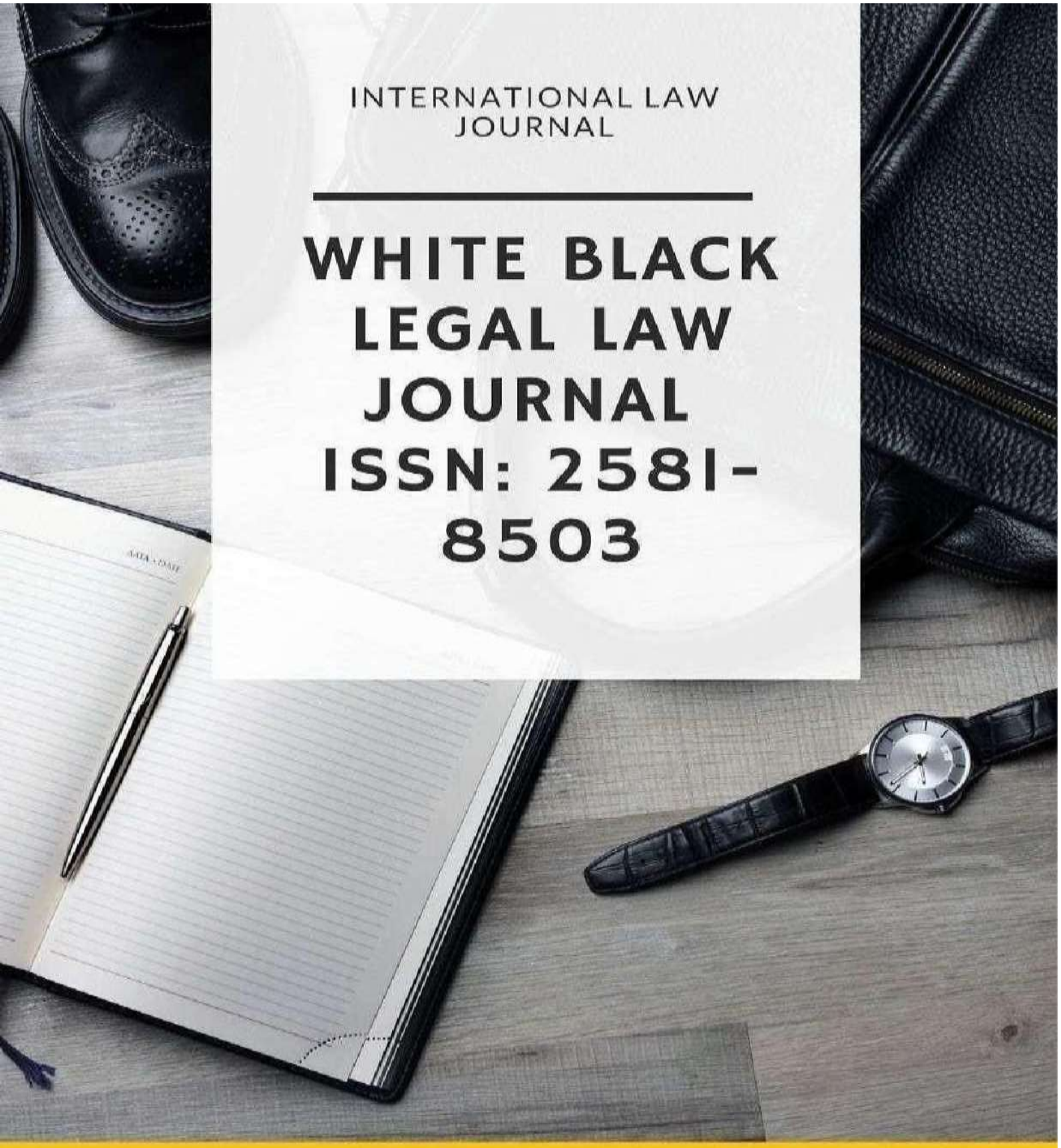

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB, LLM degrees from Banaras Hindu University & PHD from university of Kota. He has succesfully completed UGC sponsored M.R.P for the work in the Ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; PH.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St. Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,
Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing PH.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, PH.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, PH.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on CR.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); PH.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal provide dedicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

TRACEABILITY REQUIREMENT IN INDIA: PRIVACY AND TECHNOLOGY LAW

AUTHORED BY - DHANYAKESARI RAO GURPUR

Chapter I- Introduction

1.1 Background and Problem statement

Consider a hypothetical where Enid writes a coded letter and puts it in a locked box. She gives Nancy the recipient the only key to that specific box and the meaning of the code. She sends the locked box through postal service. The postal service can deliver the box, but they can't open it because they don't have Nancy's key and even if they were able to open it, they could not understand the letter as it was coded. Only Nancy, with her unique key, can unlock the box and read the coded letter. This is the concept underlying end-to-end encryption.

'*End-to-end encryption (E2EE) is a secure communication process that encrypts data before transferring it to another endpoint. Data stays encrypted in transit and is decrypted on the recipient's device.*'[1]

The number of WhatsApp users in India is projected to reach 795.67 million users by 2025. This indicates the number of users whose privacy is at stake.[2] There is a fundamental conflict between the Governments need to ensure safety and the citizens right to internet privacy. On the one hand we have individuals like Snowden who fear mass surveillance '*If you weaken encryption, people will die*',[3] Dr. Manoj Prabhakaran an IIT professor who deems E2EE necessary to prevent a chilling effect on speech, organizations like IFF that seek to protect user privacy, social media platforms like WhatsApp which deem E2EE fundamental to their operation.

On the other hand, Law Enforcement have national security concerns, FBI Director James Comey, refers to this phenomenon as 'going dark' meaning they are unable to access communications and stored data, even with a lawful warrant. The Indian Government is also

[1] IBM, 'What is End-to-End Encryption (E2EE)?' (22 September 2021) https://www.ibm.com/think/topics/end-to-end-encryption accessed 1 May 2025.
[2] Statista, 'Forecast of the Number of WhatsApp Users in India from 2017 to 2025 (in millions)' *Statista Inc.* (2021) https://www-statista-com.eresources.nls.ac.in/forecasts/1146773/whatsapp-users-in-india accessed 1 May 2025.
[3] Thomas Macaulay, 'Edward Snowden Warns Encryption Is Under Attack' *The Next Web* (21 October 2021) https://thenextweb.com/news/edward-snowden-warns-encryption-is-under-attack accessed 1 May 2025

concerned with secure communication which will hinder investigation in sensitive cases like terrorism and CSAM. Dr. Kamakoti an IIT professor suggests some technical solutions to E2EE and scholars like Etzioni argue that the dangers encryption poses to a free society are considered limited compared to phone taps, while the dangers to public safety and national security from criminals and terrorists having access to uncrackable encryption are deemed particularly high. My research aims to find the least intrusive methods which can help the law enforcement agencies (LEA) conduct investigation.

1.2 Objectives

1. To analyse the traceability requirement in India as per IT Act, 2000 and the IT Rules.
2. To study the response of courts to the traceability provision.
3. To determine the constitutionality of Rule 4 (2) of IT Rules, 2021.

1.3 Scope

This doctrinal study focuses on the traceability rule under the IT Rules, 2021. It looks at why the rule was introduced and how it was shaped by previous drafts. In doing so it will examine cases before the court. It examines privacy concerns related to traceability. This research is limited to studying the Indian legal framework.

1.4 Research questions

1. What are the legal provisions that govern traceability requirements in India?
2. What are the case laws related to traceability in India?
3. Whether Rule 4 (2) of IT Rules, 2021 is constitutional?

1.5 Research Methodology

The researcher will employ the doctrinal reinstatement approach. The sources used will be case laws, legislations, books, research papers, blogs, newspaper articles and reports.

Chapter II- Evolution of traceability provision

2.1 Early conception

The seeds for breaking secure communication were first laid down by the Telegraph Act in the colonial era. Section 5(2) empowers the Government to intercept, detain messages provided it fulfils certain conditions which include public safety, security of the State. It further stipulates that the authority must be '*satisfied that it is necessary or expedient so to do*'. This concept is

further strengthened by Sec 69 of the Information Technology Act. It empowers the government to also monitor and decrypt information. It marks a significant expansion of necessary conditions to include for the investigation of any offense. The obligation rests heavy on the shoulders of intermediaries to provide technical assistance for decryption.

IT ACT, 2000 Sec 2(w) defines an intermediary. They provide a platform to receive stores or transmit record or provides any service with respect to that record. It includes telecom service providers, internet service providers, search engines, online payment sites etc.

The procedural aspects of encryption have been laid down in Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009. They answer the technical feasibility of decryption assistance to allow access to the extent possible which meant in instances where intermediaries have control over the decryption keys.

Blackberry prides itself on the trust it has built by ensuring secure communications in its devices. It assures that all calls, messages and files on the device are encrypted. The Indian Government raised concerns over this level of encryption particularly in the case of national security concerns such as the 26/11 attacks.[4]Rahul Mattan highlights that such concerns are valid but that imposing a mandate on Blackberry to break their secure communication is not the solution as similar encryption systems to facilitate secure communications could be easily replicated.[5] The maker of blackberry finally gave in to the demands of the government and provided decoded communication records of the customer provided that there was legal authorisation. They claim that this does not extend to their coveted Blackberry Enterprise Services which enables secure corporate emails.[6] On taking a step back from the national security versus the consumer privacy debate what concerns me the most that there is no truly secure communication in the cyberspace.

[4] Zack Whittaker, 'BlackBerry Encryption Too Secure? National Security vs Consumer Privacy' (ZDNet, 29 July 2010) https://www.zdnet.com/article/blackberry-encryption-too-secure-national-security-vs-consumer-privacy/ accessed 1 May 2025.

[5] Rahul Matthan, 'Cracking the BlackBerry' (*Indian Express*, 7 August 2010) https://indianexpress.com/article/opinion/columns/cracking-the-blackberry/ accessed 2 May 2025.

[6] Joji Thomas Philip, 'BlackBerry Maker Research In Motion Agrees to Hand Over Its Encryption Keys to India' (*The Economic Times*, 2 August 2012) https://economictimes.indiatimes.com/industry/telecom/blackberry-maker-research-in-motion-agrees-to-hand-over-its-encryption-keys-to-india/articleshow/15319701.cms accessed 2 May 2025.

National draft encryption policy 2015 reflected the stance of the government taken in the blackberry case. The Draft NEP outlined a high-level regulatory framework for encryption that applied broadly to include Central and State Government Departments, businesses, and all citizens. It excluded sensitive government departments performing sensitive and strategic roles. It applied to intermediaries in a broad sense to those service providers located within and outside India. Some of the key obligations for intermediaries were facilitating mandatory plain text storage, providing readable plain text on demand, registration and agreement with Government and vendor registration and software submission.[7]

Sunil Abraham's critique argued that provision of readable plain text was 'unworkable' for E2EE based platforms and would create a honeypot for attackers. The registration requirement was deemed to be near impossible to enforce. It could negatively impact the IT/ITES/BPO/KPO industries (key intermediaries) in India that handle foreign data protected under other jurisdictions, as clients might fear government access to confidential information and move their business elsewhere. However, he does find some merit in the policy that encouraged digital signatures, setting up testing infrastructure, and initiating research into indigenous algorithms.[8]

NASSCOM notes emerging international discussions about framing service providers obligations through a concept of 'duty of care' to prevent online harms. This could potentially include providing decryption assistance.[9] The draft NEP faced severe criticism and central to it was the mandatory plain text retention. Ultimately the draft was withdrawn and unfortunately no subsequent draft was introduced.

2.2 Draft Intermediary Guidelines Rules, 2018 and its impact

The next wave of decryption demands started by the introduction of traceability under Rule 3(5) Information Technology [Intermediary Guidelines (Amendment) Rules], 2018. The purpose of the rules was to mitigate the violence and misinformation spread on social media platforms.[10] It wanted to unveil the secret identity of perpetrators who hid behind keyboards.

[7] Vijayashankar Na, 'Comments on the Draft National Encryption Policy from Naavi' (*Naavi.org*, 19 September 2015) https://www.naavi.org/wp/comments-on-the-draft-national-encryption-policy-from-naavi/ accessed 5 Apr 2025.
[8] Sunil Abraham, 'Hits and Misses with the Draft Encryption Policy' (*The Wire*, 26 September 2015) https://thewire.in/tech/hits-and-misses-with-the-draft-encryption-policy accessed 5 Apr 2025.
[9] NASSCOM, *The Road Ahead for Encryption in India* (Discussion Paper Series, December 2020).
[10] *Rajya Sabha Parliamentary Debates*, Official Report, vol 246, no 7 (July 2018).

Rule 3 prescribed due diligence to be observed by intermediary. Rule 3(5) obligated intermediaries to trace originators when requested by a lawful order. The window for compliance was 72 hours from the request. The purpose could be security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security.

It is concerning that the rule does not mention the specific government agencies or the rank of officials who would be legally authorised to issue a lawful order mandating information and assistance from intermediaries. A clear delineation of due process is essential for accountability and transparency, even in sensitive situations requiring expediency. The rule lacks clear legally established tests or safeguards and grievance redressal mechanisms.[11]

It continues a trend of a notice and take-down regime without any provision for judicial oversight. The presence of this rule alongside other pre-existing regulations (like those for ISPs under the Indian Telegraph Act, 1885, and under Section 69(1) of the IT Act, 2000) highlights an additional burden on intermediaries.

Another drawback is the narrow and restrictive list of circumstances where the intermediary shall provide assistance. To overcome this, it is suggested that other circumstances be added to the list with a flexible timeline. Further tracing requirement be clarified to specify the extent of the intermediary's role in tracing.[12]

The Prajwala Case concerns the circulation of videos depicting sexual violence. A committee was formulated to address these issues. It outlines the responsibilities of content hosting platforms (CHPs), search engines and social media platforms like Facebook, Google and WhatsApp. One of their key recommendations was for immediate content removal when videos depicted Child Pornography (CP) and Rape/Gang Rape (RGR) content. CHPs, Search Engines, and the Government of India should work together in formulating processes for proactively verifying, identifying and initiating take down of all CP/RGR content.[13]

[11] Digital Empowerment Foundation, *Submission of Comments on MEITY's Draft Information Technology (Intermediary Guidelines (Amendment) Rules), 2018* (2018).
[12] BananaIP, *BananaIP's Comments on the Draft Intermediary Rules, 2018* (26 February 2019) https://www.bananaip.com/intellepedia/bananaips-comments-on-the-draft-intermediary-rules-2018/ accessed 10 Apr 2025.
[13] In re, Prajwala Letter (Videos of Sexual Violence & Recommendations), (2018) 17 SCC 79.

This led to the formation of the Ad-Hoc Committee Report on Online Pornography (2020).[14]Among its many recommendations it suggests that Law enforcement agencies be permitted to break end to end encryption to trace distributors of child pornography. This can be viewed as a push towards stricter intermediary guidelines.

2.3 The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

Rule 3 of the IT Rules, 2021 provides for due diligence to be followed by intermediaries and establishes a grievance redressal mechanism. Rule 4(2) of the IT Rules, 2021 places a significant obligation on 'significant social media intermediaries' (SSMIs). The government has fixed fifty lakh registered users as the threshold for defining SSMI. The key requirement is for SSMIs to enable the identification of the first originator of information on their platform. They must do so based on a judicial order passed by a court of competent jurisdiction or an order passed under Section 69 of the Information Technology Act, 2000.

The provisos introduce significant safeguards and limitations on when and how this tracing can be mandated. The conditions for passing an order are specific, serious offenses related to Sovereignty and integrity of India and so on and includes offenses related to rape, sexually explicit material, or child sexual abuse material. To, cater to privacy concerns there is a mandate to consider whether less intrusive methods are effective in identifying the originator before issuing an order under this rule. In complying with such orders, SSMIs are explicitly not required to disclose the contents of any electronic message. Any other information related to the first originator beyond the identification itself. Any information related to its other users. The aim is to limit the scope of information that needs to be shared.

The deemed first originator is a peculiar concept introduced which states that if the actual first originator is located outside India, the first originator of that information within India shall be deemed to be the first originator for the purpose of this rule. This attempts to address jurisdictional issues where the offender is not within the reach of the law enforcement. This proviso has been criticised for its odd interpretation of first originator.

[14] Ad-Hoc Committee, Rajya Sabha, January 2020.

The threshold for SSMIs is designed to protect intermediaries operating at smaller scale from crushing compliance burden. However, given Indian internet population it is not a very high threshold.

2.4 Sector specific encryption standards

Historically, the Department of Telecommunications (DoT) required Internet Service Providers (ISPs) and Telecommunications Service Providers (TSPs) to obtain prior government approval for deploying encryption beyond a key-size of 40 bits and prohibited bulk encryption. This was intended to ensure lawful interception.

Currently, the Unified License (UL), which covers telecom and internet services, prohibits the deployment of 'bulk encryption'. The term bulk encryption is undefined but could refer to stronger, high-level, or large-scale encryption. The government also retains the right to evaluate encryption used by licensees. This restriction on encryption deployment by TSPs and ISPs is a part of their license agreements with the DoT.

The Reserve Bank of India (RBI) prescribes encryption standards for financial sector data. The RBI recommended the deployment of a minimum of 128-bit Secured Socket Layer (SSL) encryption for the sensitivity of financial information infrastructure. Non-Banking Financial Companies (NBFCs) providing mobile financial services are required to use end-to-end encryption technology. NBFCs using social media platforms must use encryption to secure transactions. RBI directs Payment Aggregators and Payment Gateways to use data security standards like encryption, and recent guidelines mandate encryption without specifying parameter.

Similarly, SEBI prescribes a 128-bit encryption standard for data in transit for securities trading using wireless technology and internet-based trading.

The Electronic Health Record Standards, 2016, specify that all personally identifiable recorded patient data must be encrypted and decrypted using the best available key strength (minimum 256-bit), especially during transmission.

Clause 247 of the proposed Income Tax Bill, 2025, allows authorities to override access codes and break into virtual digital spaces, when tax evasion is suspected. This would set a dangerous

precedent as there is no demarcated limit on what information the authorities can access. It is a privacy violation which does not include any judicial oversight.

Chapter III- Jurisprudence of traceability

The Madras High Court examined a PIL which sought the linking of Aadhaar with Social Media accounts.[15] On closer scrutiny the actual contention seems to create a mechanism to curb cyber bullying.

For Antony, one of the parties, it stems from his personal experience of facing cyber bullying and finding no recourse in the law.[16] The court clarifies at the outset that based on the proportionality test established in Puttaswamy, noting that it is imperative to strike a balance between freedom of speech and protection. This standard requires considering whether proposed measures, like mandatory authentication, are proportional to the aim and whether less restrictive alternatives could achieve the same goal without causing undue harm. In the State Government's report on responses for requests made to social media platforms they illustrate the practical difficulties in obtaining information from platforms under the current system. The low furnishing rates for certain information requests, particularly from Whatsapp, highlight the challenges law enforcement faces. The Court considers leveraging scientific technology to address the problems faced by the public and investigating agencies.

Dr. Kamakoti suggested two main remedies, the originator's number is visible in forwarded Whatsapp messages is presented as a potential technical application. Encrypting the sender's phone number in the message metadata, which could be decrypted by WhatsApp only upon receiving relevant court orders. Dr Kamakoti's remedies were heavily criticised by Whatsapp, IFF and other experts. His suggestions were seen as erroneous and not feasible. It would tantamount to fundamental changes to WhatsApp and undermine E2EE.[17] Experts stated that end-to-end encryption and traceability cannot co-exist. A major criticism was that the proposals would not correctly identify the originator of unlawful content in common sharing scenarios.
Dr. Manoj Prabhakaran stated that Kamakoti's proposals would erode users' privacy. This

[15] *Antony Clement Rubin v Union of India* WP 20774 of 2018.
[16] Arun Janardhanan, 'Social media should share info on users who abuse online' (*The Indian Express*, 21 August 2019) https://indianexpress.com/article/india/social-media-users-link-aadhaar-number-antony-clement-rubin-petition-madras-high-court-5922005/ accessed 15 Apr 2025.
[17] Aditi Agrawal, 'Exclusive: WhatsApp's response to Dr Kamakoti's recommendation for traceability in WhatsApp' (*MediaNama*, 21 August 2019) https://www.medianama.com/2019/08/223-exclusive-whatsapps-response-kamakotis-submission-2/ accessed 15 Apr 2025.

would lead to a chilling effect on the right to free speech, particularly for personal messages. Vulnerable groups like whistleblowers, activists, journalists, abuse survivors, and marginalized groups would be disproportionately impacted due to the risk of harm if their identity is publicly disclosed.[18] Traceability was argued to be not a very effective means of fighting fake news. Traceability would likely spur commercial services for untraceable messaging. It would primarily only be useful for apprehending users with limited resources. Alternatives like fact-checking, spam filters, education, and media literacy were suggested as more effective and less restrictive.

Then Facebook sought relief from the SC and requested that the matters pending before Madras HC on Aadhaar linking to social media be heard by the Apex court. The court accounts for the two opposing views by Dr Kamakoti and Dr Manoj and specifically states that the court shall not engage with the scientific aspects of encryption debate. The court acknowledged the merit in arguments made for encryption as well as decryption. It also highlights that '*For purposes of detection, prevention and investigation of certain criminal activities it may be necessary to obtain such information. De-encryption and revelation of the identity of the originator may also be necessary in certain other cases, some of which have been highlighted hereinabove*.'[19]
In *Shreya Singhal* the Apex Court with respect to intermediary liability, upheld the validity of Section 79, subject to "*Section 79(3)(b) being read down to mean that an intermediary upon receiving actual knowledge from a court order or on being notified by the appropriate government or its agency that unlawful acts relatable to Article 19(2) are going to be committed then fails to expeditiously remove or disable access to such material ...*".
The Kerala High Court heard a PIL which sought to ban WhatsApp owing to its non compliance with IT Rules, 2021. It had the potential for user-end manipulations and its inability to trace the origin of messages. It was contended that WhatsApp's own privacy policy contradicted the end-to-end encryption claim by stating it would store messages in certain circumstances and would store and use various user information and activities, including accessing contact lists and identifying non-users, which is viewed as violating privacy. The petition was dismissed as the High Court found that the petitioner failed to demonstrate any arbitrariness or illegality on the part of the respondents justifying interference under Article 226 of the Constitution of

[18] Aditi Agrawal, 'Kamakoti's proposals will erode user privacy, says IIT Bombay expert in IFF submission' (*MediaNama*, 27 August 2019) https://www.medianama.com/2019/08/223-iff-response-kamakoti-submission-traceability-2-2/ accessed 15 Apr 2025.
[19] *Facebook Inc. v Antony Clement Rubin* TP (C) 1943-46/2019 (Diary No.32478-2019).

India.[20]

Praveen, a free and open-source software (FOSS) developer and part of the Free Software Community of India (FSCI) filed for quashing Part II of the Information Technology Rules, 2021. The petitioner, along with other volunteers, runs privacy-respecting, federated social media services based on FOSS principles, offering alternatives to centralized proprietary applications like Facebook, Zoom, and WhatsApp. These services run on donations and volunteer efforts, not for profit. The petitioner's services fall within the definition of an intermediary under the Information Technology Act, 2000. The rules fail to draw an intelligible differentia between not-for-profit FOSS communities and for-profit proprietary companies. Applying the same heavy compliance burden to both is argued to be unfair and arbitrary.

Rule 4(2) for significant social media intermediaries mandates tracing the first originator of information. It is argued that this violates the fundamental right to encryption, which is a subset of the right to privacy protected under Article 21, as affirmed by *Puttaswamy* judgment. This requirement allegedly cannot be met without breaking end-to-end encryption and forces intermediaries to snoop on private communication, which is a '*flagrant violation of the right to privacy*'. This is argued to fail the four-pronged test for permissible state infringement on privacy laid down in *Puttaswamy.*[21]

WhatsApp LLC v Union of India, primarily challenges the validity of Rule 4(2) of the Information Technology Rules, 2021. WhatsApp operates an end-to-end encrypted messaging service used by hundreds of millions of users in India. Its encryption system is based on the Signal Protocol and is designed to prevent third parties and WhatsApp itself from accessing messages or calls in plaintext. WhatsApp states that its encryption has no 'Off Switch'. Impugned Rule 4(2) mandates intermediaries to enable the identification of the first originator of information. WhatsApp argues this requirement directly violates the fundamental right to privacy, which includes the right to encryption. WhatsApp states they cannot break E2EE without weakening encryption or creating 'back-doors'.

It reiterates that such a requirement fails the four-pronged test for permissible state infringement on privacy established by the Supreme Court in *Puttaswamy*. It specifically lacks

[20] *Omanakuttan.K.G v Union Of India* AIR 2021 KERALA 173.
[21] *Praveen Arimbrathodiyil v Union of India* WP (C) No. 9647 of 2021.

judicial review before the privacy invasion occurs, which is deemed necessary against arbitrary state action. Further the rules are criticized for failing to draw an intelligible differentia between different types of intermediaries, applying potentially onerous obligations universally.[22]

Chapter IV- Analysing the constitutionality of traceability

Failure to comply with the traceability provision can result in the intermediary losing its indemnity (safe harbour protection) under Section 79 of the IT Act.

The makers of our constitution debated the 'Right to Secrecy of Correspondence' as a fundamental right. It stated that provision may be made by law to regulate the interception or detention of articles and messages transmitted by post, telegraph, or otherwise on the occurrence of any public emergency or in the interests of public safety or tranquillity. After weighing the pros and cons the clause was deleted.

Telephone tapping is permissible in India under Section 5(2) of the Telegraph Act, 1885. In *PUCL* it was held that '*Telephone conversation is an important facet of a man's private life. Right to privacy would certainly include telephone-conversation in the privacy of one's home or office. Telephone-tapping would, thus, infract Article 21 of the Constitution of India unless it is permitted under the procedure established by law.*' The court issued procedural safeguards to be observed before resorting to telephone tapping under Section 5(2) of the Act.

Similarly, call data records can be extracted based on judicial orders, which violates privacy and is saved by due procedure.

The Supreme Court's landmark judgment *Puttaswamy (Retd.)* established the right to privacy as a fundamental right intrinsic to Article 21. This judgment also laid down a four-fold test that any law infringing upon the right to privacy must satisfy to be constitutionally valid. Critics of decryption argue that traceability violates all four folds of this test (Art.21) and the Government defends it stating that privacy is not an absolute right and subject to reasonable restrictions (Art 19(2)).

[22] *WhatsApp LLC v Union of India W.P.* (C) NO. _____ OF 2021.

To account for both of the arguments the researcher applies the double proportionality test established in *Electoral Bonds* to balance fundamental rights. It is clear that the Constitution does not create a hierarchy between the rights in conflict. It can be argued that traceability is not a suitable means for furthering privacy and suitable to further the State's interest of tracing crime. It is also not the least restrictive means for furthering both the rights. It has a disproportionate impact on both privacy of user and on State interest. The balancing act requires a careful consideration of the potential harms to privacy against the benefits for state security, and in this analysis, the traceability measure appears to tilt heavily towards infringing upon privacy.

Chapter 5 – Recommendations and Conclusion

Less restrictive alternatives to traceability could include strengthening LEA capabilities in Metadata Analysis. The Central Government had previously suggested technological changes to WhatsApp, such as introducing a digital fingerprint system, to trace messages to the originator. WhatsApp has already implemented measures like the forward label to encourage users to think before sharing and to reduce forwarding behaviour. Instead of focusing on accessing data as it is transmitted an alternative approach suggested is to limit the scope of decryption to information stored on a particular mobile phone that is in the possession of law enforcement. This focuses on data at rest. Technical solutions like a local key escrow can be used for this approach.

Utilizing existing legal and international cooperation mechanisms such as Mutual Legal Assistance Treaties (MLATs) while cumbersome represent an existing legal framework for cross-border data access. US CLOUD Act Framework enables faster access for non-US jurisdictions to data stored within the US via orders. It offers a faster process compared to MLATs but raises concerns about the applicability of domestic laws without the checks and balances provided by mechanisms like the judicial review. Existing law requires a court warrant to search an individual's device. Legally accessing stored data on devices is considered a less intrusive alternative. Under existing Interception Rules, service providers must provide technical assistance for interception requests to the extent they are capable.

In the long term traceability has a disproportionate impact on the State, while E2EE intended to enhance the state's ability to address crime, the disproportionate impact on privacy could

erode trust in digital platforms and potentially drive illegal activity to less transparent channels, undermining the effectiveness of the measure. Any use of back door mechanisms too means that more users would succumb to privacy risks.

Sector-specific requirements often prescribe minimum standards for data protection and cybersecurity, particularly in areas like communications, internet-based trading, and online financial transactions. Some requirements also place limits on encryption strength or aim to enable government access for lawful interception. Instead of a uniform, sector-agnostic framework for regulating encryption in India analysing sector-specific requirements should continue, potentially with revised or removed key-size limits.

Therefore, only after exhausting less intrusive means encryption can be circumvented after judicial order is passed for the same. It must be done only when it is absolutely necessary and even then, the context must be specified. The conditions for doing so must fall within the 8 enumerated grounds of reasonable restrictions in Art 19(2). Additionally, a sunset clause of 72 hours after which the information can no longer be used must be added.

BIBLIOGRAPHY

List of cases

Antony Clement Rubin v Union of India WP 20774 of 2018

Association for Democratic Reforms v Union of India, 2024 SCC OnLine SC 150

Facebook Inc. v Antony Clement Rubin TP (C) 1943-46/2019 (Diary No.32478-2019)

In re, Prajwala Letter (Videos of Sexual Violence & Recommendations), (2018) 17 SCC 79

Justice K S Puttaswamy (Retd.), and Anr. v Union of India And Ors. [2017] 10 S.C.R. 569

Omanakuttan.K.G v Union Of India AIR 2021 KERALA 173

People's Union Of Civil Liberties v Union Of India (Uoi) And Anr AIR1997SC568

Praveen Arimbrathodiyil v Union of India, WP (C) No. 9647 of 2021

Shreya Singhal v Union of India MANU/SC/0329/2015: 2015 INSC 257

WhatsApp LLC v Union of India, W.P. (C) NO. _____ OF 2021

List of Legislation, Acts, and Rules

Constitution of India, 1951

Electronic Health Record Standards, 2016

Income Tax Bill, 2025

Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009:

Information Technology [Intermediary Guidelines (Amendment) Rules], 2018 (Draft):

National Draft Encryption Policy, 2015

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules, 2021):

The Information Technology Act, 2000:

The Telegraph Act, 1885

United States Congress Clarifying Lawful Overseas Use of Data Act H.R. 4943 (2018)

Books

Etzioni A, *The Limits of Privacy* (Basic Books 1999).

Jain M P, *Indian Constitutional Law* (9th edn, LexisNexis 2024)

Nappinai N S, *Technology Laws Decoded* (1st edn, LexisNexis 2017)

Rao B S, *The Framing of India's Constitution: Select Documents*, vol II (The Indian Institute of Public Administration 1967)

Seth K, *Computers, Internet and New Technology Laws* (3rd edn, LexisNexis 2024)

Committee Report and Discussion Papers

Ad-Hoc Committee, Rajya Sabha, January 2020.

Data Security Council of India (DSCI), Encryption and the Digital Economy: Balancing Security, Privacy and National Security (2021).

Digital Empowerment Foundation, Submission of Comments on MEITY's Draft Information Technology (Intermediary Guidelines (Amendment) Rules), 2018 (2018).

Internet Freedom Foundation, 'IFF Releases Legislative Brief on Digital Rights for the Monsoon Session of the Parliament' (24 July 2021).

NASSCOM, The Road Ahead for Encryption in India (Discussion Paper Series, December 2020).

Rajya Sabha Parliamentary Debates, Official Report, vol 246, no 7 (July 2018).

Vasudev Devadasan, Report on Intermediary Liability in India (Centre for Communication Governance, December 2022).

Journal Articles

Biyani Neeti and Choudhury Amrita 'The 2021 Indian Intermediary Guidelines and the Internet Experience in India' (2021)

Etzioni Amitai 'End to End Encryption, the Wrong End' (2016) 67 Supreme Court Law Review 561

Grover Gurshabad, Rajwade Tanaya and Katira Divyank 'The Ministry and the Trace: Subverting End-to-End Encryption' (2021) 14 NUJS Law Review 223

Nojeim Greg, Maheshwari Namrata and Miglani Eduardo 'Encryption in India: Preserving the Online Engine of Privacy, Free Expression, Security, and Economic Growth' (2021) 17 Indian Journal of Law and Technology 1 Article 2

Raj Ayush 'Analysing the Interplay between End-to-End Encryption & Privacy: Symbiotic Association or a Mere Facilitation?' (2022) RGNUL Financial & Mercantile Law Review 2022 99

Sarkar Torsha et al 'On the Legality and Constitutionality of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021' (Centre for Internet and Society, 2021)

Thakkar Maharshi and Srivastava Shreshthraj 'The Concept of Originator in Terms of Information Technology Rules 2021 and its Implications on the Right to Privacy' (2021) 4(3) International Journal of Law, Management & Humanities 6113

Websites

Abraham Sunil, 'Hits and Misses with the Draft Encryption Policy' (*The Wire*, 26 September 2015) https://thewire.in/tech/hits-and-misses-with-the-draft-encryption-policy accessed 5 Apr 2025

Agrawal Aditi, 'Exclusive: WhatsApp's response to Dr Kamakoti's recommendation for traceability in WhatsApp' (*MediaNama*, 21 August 2019) https://www.medianama.com/2019/08/223-exclusive-whatsapps-response-kamakotis-submission-2/ accessed 15 Apr 2025

Agrawal Aditi, 'Kamakoti's proposals will erode user privacy, says IIT Bombay expert in IFF submission' (*MediaNama*, 27 August 2019) https://www.medianama.com/2019/08/223-iff-response-kamakoti-submission-traceability-2-2/ accessed 15 Apr 2025

BananaIP, *BananaIP's Comments on the Draft Intermediary Rules, 2018* (26 February 2019) https://www.bananaip.com/intellepedia/bananaips-comments-on-the-draft-intermediary-rules-2018/ accessed 10 Apr 2025

IBM, 'What is End-to-End Encryption (E2EE)?' (22 September 2021) https://www.ibm.com/think/topics/end-to-end-encryption accessed 1 May 2025.

Janardhanan Arun, 'Social media should share info on users who abuse online' (*The Indian Express*, 21 August 2019) https://indianexpress.com/article/india/social-media-users-link-aadhaar-number-antony-clement-rubin-petition-madras-high-court-5922005/ accessed 15 Apr 2025

Macaulay Thomas, 'Edward Snowden Warns Encryption Is Under Attack' *The Next Web* (21 October 2021) https://thenextweb.com/news/edward-snowden-warns-encryption-is-under-attack accessed 1 May 2025

Matthan Rahul, 'Cracking the BlackBerry' (*Indian Express*, 7 August 2010) https://indianexpress.com/article/opinion/columns/cracking-the-blackberry/ accessed 2 May 2025

Ministry of Information Technology FAQ Intermediary Rules 2021 (2021) https://www.meity.gov.in/writereaddata/files/FAQ_Intermediary_Rules_2021.pdf accessed 1 Apr 2025

Na Vijayashankar, 'Comments on the Draft National Encryption Policy from Naavi' (*Naavi.org*, 19 September 2015) https://www.naavi.org/wp/comments-on-the-draft-national-encryption-policy-from-naavi/ accessed 5 Apr 2025

Philip Thomas J, 'BlackBerry Maker Research In Motion Agrees to Hand Over Its Encryption Keys to India' (*The Economic Times*, 2 August 2012) https://economictimes.indiatimes.com/industry/telecom/blackberry-maker-research-in-motion-agrees-to-hand-over-its-encryption-keys-to-india/articleshow/15319701.cms accessed 2 May 2025

Rai Ankush Decrypting Rule 4(2) 10 August 2018 https://lawandotherthings.com/decrypting-rule-42/ accessed 5 Apr 2025

Rizvi Kazim and Singh Shivam Does The Traceability Requirement Meet The Puttaswamy Test? https://thedialogue.co/does-the-traceability-requirement-meet-the-puttaswamy-test/ accessed 10 Apr 2025

Statista, 'Forecast of the Number of WhatsApp Users in India from 2017 to 2025 (in millions)' *Statista Inc.* (2021) https://www-statista-com.eresources.nls.ac.in/forecasts/1146773/whatsapp-users-in-india accessed 1 May 2025.

Udbhav Tiwar India's New Intermediary Liability and Digital Media Regulations Will Harm the Open Internet (2 March 2021) https://blog.mozilla.org/en/internet-health/indias-new-intermediary-liability-and-digital-media-regulations-will-harm-the-open-internet/ accessed 7

Apr 2025

Whittaker Zack, 'BlackBerry Encryption Too Secure? National Security vs Consumer Privacy' (ZDNet, 29 July 2010) https://www.zdnet.com/article/blackberry-encryption-too-secure-national-security-vs-consumer-privacy/ accessed 1 May 2025

WHITE BLACK LEGAL