The Dialogue™
INFORM ENGAGE IDEATE

IAMAI
Internet And Mobile Association Of India

IT RULES, 2021: A REGULATORY IMPACT ASSESSMENT STUDY

Volume 1 | July 2022

IT RULES, 2021: A REGULATORY IMPACT ASSESSMENT STUDY

Volume 1 | July 2022

Date of publication of this report is **4th July, 2022.**

Recommended Citation: Shreya S. & Tiwari P. (2022, July 4). *IT Rules, 2021: A Regulatory Impact Assessment Study* (Vol. 1). New Delhi. The Dialogue and Internet And Mobile Association of India.

This page has been left blank intentionally

AUTHORS

Shruti Shreya is a Programme Manager for the Platform Regulation vertical at The Dialogue. A lawyer by training with a Gold Medal from Symbiosis International University, she is engaged in conducting interdisciplinary research on varied aspects of social media governance and online safety.

Pranav Bhaskar Tiwari researches on intermediary liability and encryption. A lawyer by training, Pranav conducted research-based advocacy on privacy, platform regulation, and the future of work. A Gold-Medalist in international law and diplomacy from the Indian Society of International Law and analyse international affairs from a globalisation perspective.

Editors:
Kazim Rizvi, Founding Director, The Dialogue™
Yash Razdan, Assistant Manager, Internet and Mobile Association of India

Research Assistants:
Garima Saxena
Vaishanavi Sharma

Creative Visualisation:
Divya Vishwanathan

Designer:
Diksha Kumari

This page has been left blank intentionally

TABLE OF CONTENTS

Index of Abbreviations **i**
List of Figures **iii**
List of Tables **iii**
Acknowledgement **iv**
Executive Summary **v**
Research Methodology **viii**
i. Research Design viii
ii. Scope ix
iii. Stakeholder Universe ix
Introduction **xi**
1. Context Setting-Analysing Challenges that the rules seek to resolve **01**
1.1. Fake News and Disinformation 01
1.2. Child Sexual Abuse Material 02
1.3. Seditious and Terrorism Related Content 02
2. Analysing Experiences from the ground-Part II of the IT Rules, 2021 **04**
2.1. Creation of differential obligations based on platform size 04
2.2. Due Diligence & Grievance Redressal by Digital Intermediaries 06
2.2.1. Timeline for content takedown and assisting the LEAs 06
2.2.2. Timeline for Grievance Redressal 08
2.2.3. Timeline for Mandatory Data Retention 08
2.3. Additional Due Diligence Requirements for Significant Social Media Intermediaries 10
2.3.1. Appointment of Additional Personnels and their Personal Liability 10
2.3.2. Originator Traceability 11
2.3.3. Proactive Monitoring 15
2.3.4. User Verification 16
3. Revamping the IT Act: Feedback from stakeholders **18**
3.1. Enabling a progressive intermediary liability regime 18
3.2. Instilling procedural safeguards in provisions for law enforcement assistance, search and seizure 18
3.3. Enabling a progressive encryption regime 19
3.4. Furthering a uniform and transparent content blocking regime 19
3.5. No corporate criminal liability 19
3.6. Enhancing cybersecurity 20
3.7. Extensive Multi Stakeholder Consultation 20
3.8. Capacity building 20
4. Policy Recommendations **21**

INDEX OF ABBREVIATIONS

AI	Artificial Intelligence
CCO	Chief Compliance Officer
CERT-In	Indian Computer Emergency Response Team
CrPC, 1973	Code of Criminal Procedure, 1973
CSAM	Child Sexual Abuse Material
Decryption Rules, 2009	Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009
Draft Intermediary Liability Rules, 2018	The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018
EoDB	Ease of Doing Business
IAMAI	Internet and Mobile Association of India
IPC, 1860	Indian Penal Code, 1860
IL Guidelines, 2011	Information Technology (Intermediaries Guidelines), 2011
IT Rules, 2021	The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
KYC	Know Your Customer
LEAs	Law Enforcement Agencies
MeitY	Ministry of Electronics and Information Technology
NCRB	National Crime Records Bureau
NCA	News and Current Affairs Content
NetzDG Act	The Network Enforcement Act
NGO	Non-governmental organisation
OTT	Over-the-top

POCSO	Protection of Children from Sexual Offences
SSMIs	Significant Social Media Intermediaries
SMIs	Social Media Intermediaries
UN	United Nations
UNCITRAL	United Nations Commission on International Trade Law

LIST OF FIGURES

Figure 1: Research Design viii
Figure 2: Stakeholder Universe ix
Figure 3: Data Collection Methods x
Figure 4: Timeline of the Indian Safe Harbour Regime xii
Figure 5: Ramifications of breaking encryption 12

LIST OF TABLES

Table 1: Key Insights on creation of differential obligations based on platform size 6
Table 2: Key Insights on due diligence and grievance redressal mandates for inter-mediaries under Rule 3 9
Table 3: Key Insights on additional due diligence for SSMIs under Rule 4 and compliance requirements under Part II of the IT Rules, 2021 17

ACKNOWLEDGEMENT

We would like to thank all the stakeholders whose valuable inputs formed the basis of this report. We interviewed a total of 82 stakeholders as part of the study. In this first volume of the study pertaining to Part II of the IT Rules, 2021, 70 stakeholders were interviewed. These includes, amongst others, Dr. Anuradha Rao; Founder, CyberCognizanz, Ms. Arnika Singh, Co-Founder, Social Media Matters; Ms. Arya Tripathy; Partner, PSA; Ms. Asheeta Regidi; Associate Director, Policy, Cashfree; Dr. Avik Sarkar, Visiting Professor, Indian School of Business; Dr. Joan Barata; Non Residential Research Fellow, Stanford Centre for Internet and Society; Mr. Manuj Garg, Co- Founder, My Upchar; Mr. Prateek Waghre; Policy Director, Internet Freedom Foundation; Mr. Samraat Basu; Lecturer in Law and Technology, Tilburg University; Mr. Siddharth Pillai Co-Founder and Director, Aarambh India; Dr. Subhajit Basu, Associate Professor of Law, University of Leeds; Mr. Udbhav Tiwari, Senior Manager, Global Public Policy, Mozilla.

We would also like to thank Mr. Kazim Rizvi, Founding Director, The Dialogue and Mr. Yash Razdan, Assistant Manager, Internet and Mobile Association of India for their continued guidance and support towards the completion of this research.

We also extend our gratitude to Ms. Garima Saxena and Ms. Vaishnavi Sharma for their research assistance, and Ms. Diksha Kumari for the thematic designing of the report.

EXECUTIVE SUMMARY

Given the rise in online harms, the MeitY introduced the Information Technology (Intermediary Guidelines & Digital Media Ethics Code) Rules, 2021 in February 2021. While many provisions addressed some of the safety challenges, the lack of public consultation obviated the Rules to resolve the primary concerns. Towards this, The Dialogue in collaboration with Internet and Mobile Association of India undertook an impact study to determine the ease of doing business, safety and privacy implications of these Rules.

The study has been conducted in two volumes - the first volume focuses on Part II of the IT Rules envisaging the regulation of intermediaries and the second volume will focus on Part III of the IT Rules which governs the over the top platforms (OTT). This is the first volume. The research is primarily qualitative in nature, based on inputs of 82 stakeholders. Out of these 82 stakeholders, 70 gave inputs for volume 1 which includes all kinds of intermediaries regulated by Part II of the Rules, civil society organisations, women and child safety bodies, lawyers, public policy professionals, and cybersecurity experts. The study addresses the key operational and implementational aspects of the IT Rules, 2021 in not just ensuring a safe online space but also furthering ease of doing business in India.

The key findings and recommendations of the research are as follows:

I. GREATER PLATFORM ACCOUNTABILITY

Finding: Several civil society organisations and women and child safety bodies noted that delineation of specific timelines for acknowledgement and redressal of user grievance has been very helpful in ensuring better responsiveness from the intermediaries. The publication of monthly transparency reports was also lauded.

Policy Recommendation: Sustained consultation with civil society and technical experts is encouraged to drive global best practices for platform accountability in the Indian regime.

II. ONEROUS THRESHOLD

Finding: Majority of the intermediaries noted that in a country like India with a population of 1.3 billion setting a threshold of 5 million users to be designated as a significant social media intermediary is quite onerous from an ease of doing business standpoint.

Policy Recommendation: The threshold should be revisited in accordance with the global best practices and India's economic interests, and a clear method should be prescribed for its computation.

III. TIMELINES FOR CONTENT TAKEDOWN AND INFORMATION ASSISTANCE

Finding: Majority of the intermediaries dealing with large amounts of user generated content noted that singular timelines for takedown of all grades of harmful content is overwhelming and impacts investment.

Policy Recommendation: A risk based content gradation mechanism should be adopted and response timelines for takedowns and information assistance should be decided accordingly.

IV. PRIVACY CONCERNS IN THE DATA RETENTION MANDATE

Finding: Several legal and technical experts highlighted the inconsistency of the data retention mandate with the principles of data minimisation.

Policy Recommendation: A 90+ 90 days approach should be adopted where the intermediaries may store the data for the original 90 days, and then if needed, the dataset may be retained further, or else deleted**.**

V. RAMIFICATIONS OF PERSONAL LIABILITY

Finding: The personal liability mandate is inconsistent with established criminal law principles and has led to excessive compliance burden impacting ease of doing business for the intermediaries.

Policy Recommendation: Remove the personal liability provision considering its legal infeasibility and economic repercussions and replace it with corporate financial penalties as the norm.

VI. INFEASIBILITY OF ORIGINATOR TRACEABILITY

Finding: Technology experts explained that implementing originator traceability is technically infeasible and will weaken end-to-end encryption.

Policy Recommendation: Do not implement the traceability mandate and enhance meta data analysis capabilities of the law enforcement ecosystem.

VII. PROACTIVE MONITORING

Finding: Majority of the intermediaries highlighted that proactive monitoring has emerged as a critical tool for tackling the deluge of harmful content.

Policy Recommendation: SOPs should be developed to guide the deployment of tools for proactive monitoring on a best effort basis. Moreover, intermediaries should also invest in developing more innovative tools to ensure online safety.

VIII. SAFE HARBOUR

Finding: Majority of the stakeholders highlighted that the compliance requirements envisaged in the IT Rules, 2021 is ostensibly diluting safe harbour jurisprudence established by the Apex Court.

Policy Recommendation: Uphold the broad immunity protection for intermediaries in accordance with the Shreya Singhal mandate to preserve the free, open and secure nature of the internet

IX. IMPACT OF THE RULES ON EASE OF DOING BUSINESS

Finding: More than 3/4th of the intermediaries as well as other key stakeholders including lawyers, public policy professionals, civil society organisations and academics noted that the mandates under Part II of the Rules may create entry barriers and impact ease of doing business in India.

Policy Recommendation: Clear and implementable Standard Operating Procedures should be published with expert inputs to address all the operational concerns impacting the smooth implementation of the Rules as discussed above.

X. PROPOSED OVERHAUL OF THE IT ACT

Finding: With drastic change in how society interacts in the digital realm, it is necessary to revisit the existing IT Act to cater to the challenges of cybersecurity and online safety while promoting digital innovation.

Policy Recommendation: Institutionalise multi stakeholder approach for policy making and adopt a collaborative Rule making approach for the revamp of the IT Act, 2000.

RESEARCH METHODOLOGY

I. RESEARCH DESIGN

The promulgation of The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 under the Information Technology Act, 2000 marked the inception of a new regime for the regulation of digital platforms in India. While certain provisions have been effective in addressing some of the critical online safety challenges, many stakeholders have voiced the need for an expert consultation and promulgation of Standard Operating Procedures (SOPs) to address the technical and operational challenges impacting the smooth implementation of the Rules. In response to this, The Dialogue in collaboration with IAMAI conceptualised this impact study to determine the ease of doing business, privacy and safety implications of the IT Rules, 2021, and explore evidence-based recommendations for envisioning a truly safe and trusted platform regulation regime.

This study is primarily qualitative in nature. It entails a secondary analysis of existing literature under the IT Act, 2000 and the IT Rules, 2021 made thereunder for the regulation of intermediaries. This is complimented by an analysis of the global frameworks such as the Manila Principles and the Santa Clara Principles. The secondary analysis not only helped identify the key stakeholders for the primary study but also shed light on the key challenges faced by the stakeholders, as well as the political economy of the sector, which subsequently defined the scope of this research.

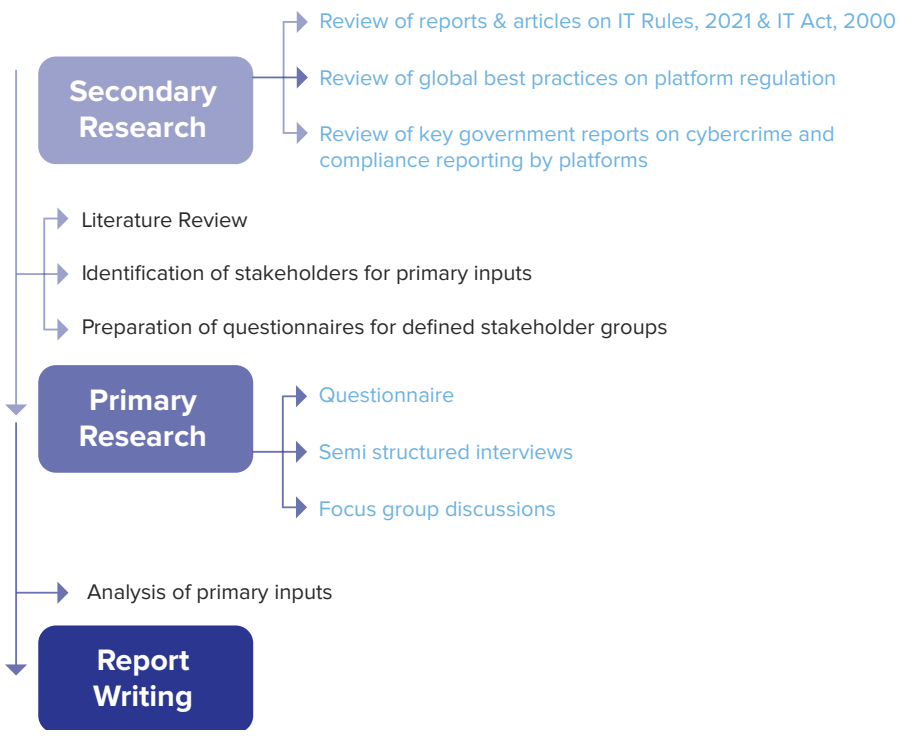


FIGURE 1: RESEARCH DESIGN

II. SCOPE

The scope of the study was limited to appreciate four core aspects:

- The compliance regime before and after the enactment of the IT Rules, 2021;
- Impact of the IT Rules, 2021 on the ease of doing business and innovation;
- Impact of the IT Rules, 2021 on the digital rights and safety of the users; and
- Best practices for the Indian IT law regime given the ongoing discussions around the IT Act amendment.

III. STAKEHOLDER UNIVERSE

After conducting an extensive literature review, and analysing court judgements and compliance reports, the research team embarked on defining the stakeholder universe under expert advice. Thereafter, questionnaires were prepared for all defined stakeholder groups.

The research team relied on maximum variation sampling within purposive sampling to seek primary inputs from a diverse set of stakeholders impacted by the IT Rules, 2021 by utilising three mechanisms to seek inputs from a total of 82 stakeholders, out of which 70 inputs were received on Part II of the IT Rules, 2021. The stakeholder distribution on Part II includes:

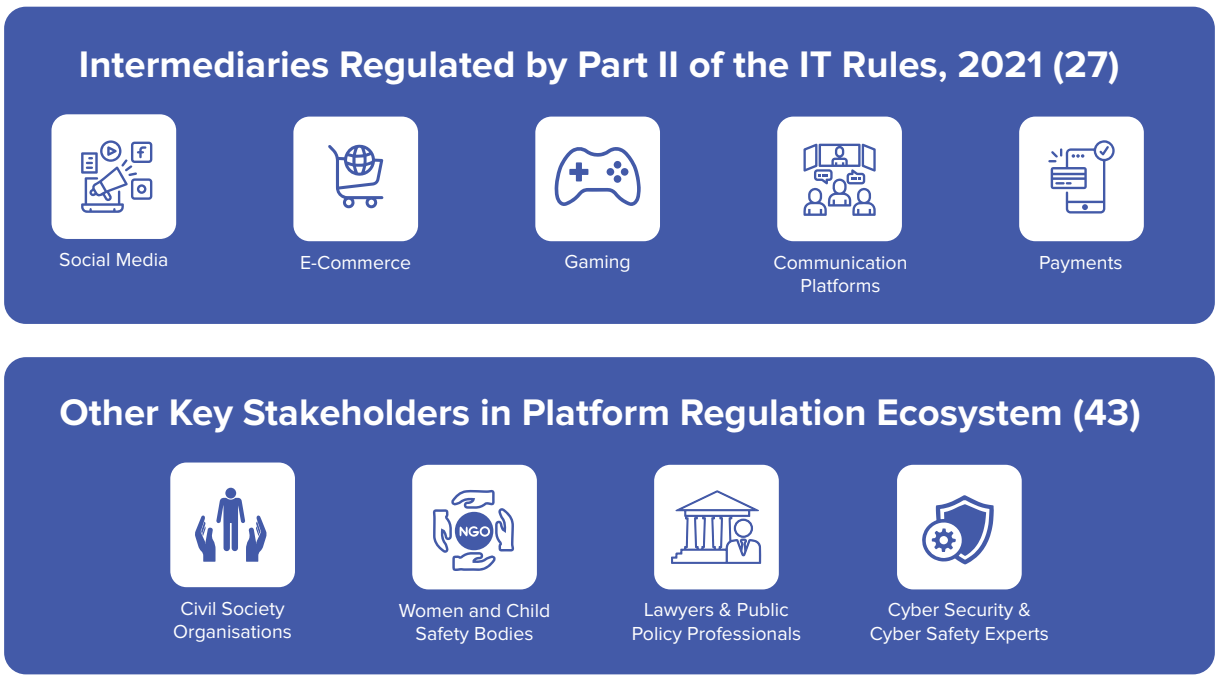


FIGURE 2: STAKEHOLDER DESIGN

Questionnaire

Detailed stakeholder-group specific questionnaires were shared over emails. 7% of the stakeholders responded to the questionnaire.

Semi-structured interviews

The stakeholder specific questionnaires were utilised to conduct in-depth semi-structured interviews. 83% of the stakeholders were interviewed virtually.

Focus Group Discussions

Four FGDs were conducted as part of this research which included 2 FGDs on Part II of the IT Rules, 2021. These include one each with Intermediaries and Civil Society Organisations. In all, 10% of the stakeholders gave their inputs

FIGURE 3: DATA COLLECTION METHODS

This report is based on the findings of The Dialogue's research by analysing the inputs received from stakeholders on Part II of the IT Rules, 2021.

INTRODUCTION

The internet ecosystem has been a major driver of human development, and India has been a key contributor towards the growth of the global digital economy. As established by a number of significant metrics, from internet connections[1] to mobile application downloads,[2] both the volume and the growth of India's digital economy now exceeds that of most other countries. According to The Internet Adoption in India-ICUBE 2020 report by the IAMAI and Kantar, India will have more than 900 million active internet users by 2025.[3]

The rising demand for remote working and infotainment is driving a rapid uptake of digital services, be it on social media platforms, communication platforms, services platforms, over the top entertainment platforms or online news platforms. In the new post-pandemic normal, the needs of the user base (examples include video conferencing and group voice calling) have transitioned rapidly from being a convenience enabling service to a daily necessity. This evolving landscape of the digital economy provides opportunities for growth and development, and also becomes a potential site of reorientation of traditional regulatory mechanisms, to ensure policy relevance while also promoting innovation.

While on one hand, digital transition has made it easier for citizens from marginalised communities to voice their concerns publicly, on the other hand, it has made it possible for malicious elements to suppress user voice and proliferate a range of online safety threats. According to the data released by National Crime Records Bureau (NCRB), India witnessed 50,035 cases of cybercrime in 2021, recording an 11.8% surge in such offences over the previous year.[4] Rapidly increasing threats to different aspects of user safety, including their physical, emotional as well as financial wellbeing, have emerged as a major challenge for Law Enforcement Agencies (LEA). Accordingly, proposals for more effective technological and legal solutions for combating these emerging online challenges have begun gaining traction. After all, with personal and professional aspirations being pursued by leveraging online applications, effective regulation is paramount to combat the threats to online safety and preserve consumer trust. In a bid to address some of these concerns and regulate more effectively, the MeitY introduced the IT Rules, 2021.

This report analyses the impact of the regulation on all kinds of digital intermediaries operating in India including social media platforms, gaming platforms, e-commerce platforms and fintech platforms as well as civil society organisations, women and child safety bodies, lawyers and public policy experts. The report iterates the fundamental issues highlighted by the stakeholders pertaining to Part II of the Rules followed by a dedicated section on key insights. The report closes with the expectations of the stakeholders from the proposed amendment of the IT Act and key policy recommendations for a progressive platform regulation regime.

---

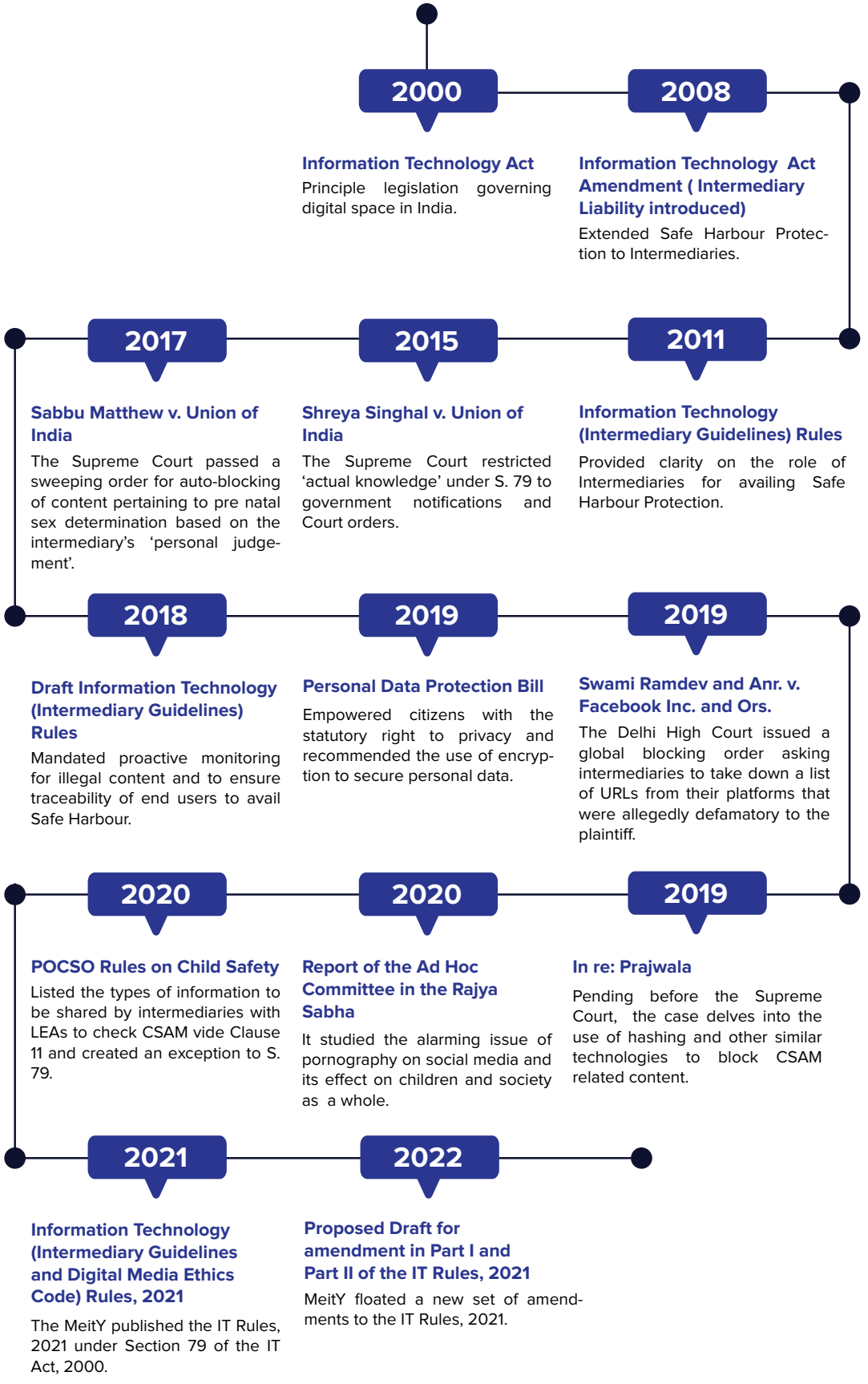
[1] Kaur, D. (2020, November 27). *India's internet connectivity doubled in just 4 years*. TechWire Asia. Retrieved from https://techwireasia.com/2020/11/indias-internet-connectivity-doubled-in-just-4-years/

[2] Keelery, S. (2020, July 15). *Mobile app usage in India - statistics & facts. Statista*. Retrieved from https://www.statista.com/topics/5600/mobile-app-usage-in-india/

[3] The Internet and Mobile Association of India and Nielsen Holdings. (2019). *Digital in India*. Retrieved from https://reverieinc.com/wp-content/uploads/2020/09/IAMAI-Digital-in-India-2019-Round-2-Report.pdf

[4] Sunny, S. (2020, December 25). *Cyber crime cases went up during lockdown, shows Delhi police data*. Hindustan Times. Retrieved from https://www.hindustantimes.com/cities/cyber-crime-cases-went-up-during-lockdown-shows-delhi-police-data/story-syScqUXmhZFBS13Bks51TJ.html

Figure 4: Timeline | Intermediary Liability in India



1. CONTEXT SETTING-ANALYSING CHALLENGES THAT THE RULES SEEK TO RESOLVE

It is important to scrutinise any regulatory or policy development from multiple lenses owing to their capacity of impacting not just the subjects of regulation (which are the intermediaries in this case) but also the other stakeholders involved (for instance, the users). Moreover, the 'test of proportionality' is crucial to determine if a legal or policy measure is commensurate with the harm they seek to tackle. The section below details the nature of harms and the challenges that the IT Rules, 2021 seek to address.

1.1. FAKE NEWS AND DISINFORMATION

Though fake news is not defined under any law in India, the 267th Report of the Law Commission of India on Hate Speech[5] discusses the provisions under the Indian Penal Code[6] and the Code of Criminal Procedure[7] that alludes to the criminality around proliferation of '*select forms of speech that are an exception to the freedom of speech*'. In general parlance, fake news refers to false statements of fact reported in online media that readers would reasonably believe are true,[8] including both intentional lies (disinformation) and inadvertent falsehoods (misinformation).[9] There also exists a third category of 'information disorder' referred to as malinformation which is based on reality but is spread to inflict harm on a person, organisation or country (eg: revenge pornography).[10]

It is critical to explore appropriate technological and regulatory solutions to tackle fake news. However, given the unavoidable ramifications of such solutions towards propagating pre-censorship, it is important to scrutinise their reasonableness to ensure that they do not impinge upon the free speech of the users.[11] In this context, it is especially important to critically analyse the feasibility of using technological tools that are incapable of understanding the context behind any piece of content as they may not only impact online free speech, but also render platforms as 'arbiters of truth and justice'.[12] This is a role that the *Shreya Singhal* judgement explicitly prohibits the intermediaries from playing, considering its implication of empowering these private platforms with the ability to restrict the fundamental rights of the citizens, a role which lies in the exclusive domain of the State under the Indian Constitution.[13]

---

[5] Law Commission of India. (2017). *Hate Speech*. Retrieved from https://lawcommissionofindia.nic.in/reports/Report267.pdf
[6] Sections 124A, 153B, 295A, 298 and 505 (1) & (2), IPC, 1860.
[7] Sections 95, 107 and 144, CrPC, 1973.
[8] Allcott, H., & Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election. *Journal Of Economic Perspectives, 31(2)*, 211-236. https://doi.org/10.1257/jep.31.2.211
[9] *Library Guides: News: Fake News, Misinformation & Disinformation*. Campus Library, University of Washington Bothell & Cascadia College. (2022). Retrieved from https://guides.lib.uw.edu/c.php?g=345925&p=7772376
[10] Ireton, C., & Posetti, J. (2018). Journalism, fake news & disinformation: handbook for journalism education and training. UNESCO. Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000265552
[11] Rizvi, K., (2019, December 14). Over Regulating Intermediaries: Threat To Free Speech?. Inc42 Media. Retrieved from https://inc42.com/resources/over-regulating-intermediaries-threat-to-free-speech/
[12] Rizvi, K., & Tiwari, P. (2021, February 17). Towards a more free and equal internet. The Pioneer. Retrieved from https://www.dailypioneer.com/2021/columnists/towards-a-more-free-and-equal-internet.html
[13] *Shreya Singhal v. Union of India*, AIR 2015 SC 1523.

1.2. CHILD SEXUAL ABUSE MATERIAL

Online sexual exploitation of minors including grooming, live streaming, consuming child sexual abuse material (CSAM), and coercing and blackmailing children for sexual purposes has become one of the most significant challenges threatening child safety on the internet. Reports by prominent news agencies suggest that 11.7% of all CSAM images are being uploaded from India.[14]

There is unanimous agreement on the need to protect children in digital spaces along with the need to mitigate the proliferation of CSAM online on a global scale. In India, Section 67A and 67B of the Information Technology Act, 2000, deal with punishment for publishing or transmitting material containing sexually explicit acts, etc, in electronic form and punishment for publishing or transmitting material depicting children in sexually explicit acts, etc., in electronic form. Additionally, The Protection of Children from Sexual Offences (POCSO) Rules of 2020[15] make everything related to CSAM, right from its manufacturing to its storage, and transfer, a criminal offence.[16]

Despite the existence of these regulatory frameworks the focus remains on exploring more avenues of regulation rather than concentrating on the effective implementation of these existing mechanisms. What is even more important is that in most of these solutions being explored, security and privacy are considered antithetical to each other while in reality both are two sides of the same coin.[17] Additionally, there exists the concern that the narrative around the right to privacy primarily focuses on adults, while minors' right to privacy is taken for granted. There is a need to scrutinise the legitimacy of such an approach given that the privacy of each individual is an essential non-derogable limb of national security.[18] Further, the fundamental rights of children similar to those of adults are "interdependent, non-hierarchical and indivisible."[19]

1.3. SEDITIOUS AND TERRORISM RELATED CONTENT

Section 69 of the IT Act, authorises the central and state governments to intercept and decrypt any information necessary for protecting national security, preserving public order, or investigating crime.[20] It also requires users and service providers to assist law enforcement and

---

[14] Kanna, R. (2020, April 18). *Most online content on child sexual abuse from India*. The Hindu. Retrieved from https://www.thehindu.com/news/national/most-online-content-on-child-sexual-abuse-from-india/article31377784.ece
[15] Rule 11, The Protection of Children from Sexual Offences Rules, 2020.
[16] Shreya, S., & Tiwari, P. (2022, December 26). *Analysing the American Safe Harbour Regime: Takeaways for India*, (p. 2). The Dialogue. Retrieved from https://thedialogue.co/wp-content/uploads/2020/12/Analysing-the-American-Safe-Harbour-Regime_Takeaways-for-India_The-Dialogue.pdf
[17] Rizvi, K., & Vaidyanathan, M. (2019, December 17). Why Privacy And Security Should Go Hand-In-Hand: The Balancing Act. Inc42 Media. Retrieved 2 July 2022, from https://inc42.com/resources/why-privacy-and-security-should-go-hand-in-hand-the-balancing-act/
[18] Shreya, S., & Tiwari, P. (2022, December 26). *Analysing the American Safe Harbour Regime: Takeaways for India*, (p. 20). The Dialogue. Retrieved from https://thedialogue.co/wp-content/uploads/2020/12/Analysing-the-American-Safe-Harbour-Regime_Takeaways-for-India_The-Dialogue.pdf
[19] Kardefelt-Winther, D., Day, E., Berman, G., Witting, S., & Bose, A. (2020, October). *Encryption, Privacy and Children's Right to Protection from Harm*. UNESCO. Retrieved from https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%e2%80%99s_right_to_protection_from_harm.pdf
[20] Section 69, IT Act, 2000.

government agencies with accessing this information. Soon after passing these amendments, the government developed Information Technology Rules (The Decryption Rules).[21] The Decryption Rules clarify the parameters of decryption and the required protocol.[22] While recommendations have been made regarding the need for making these provisions more robust by incorporating adequate checks and balances in the exercise of these powers, the government has argued to explore improved technological solutions to tackle the rising national security and public order threats. The mandate of originator traceability as provided under the new IT Rules is an apt evidence in this regard.

While ensuring national security is a critical aim of the state, it is equally important to ensure technical feasibility and competence of the proposed solutions to attain the desired goals. Proportionality, transparency and balance between privacy and national security goals provides the legitimacy needed for democratic governance. The Indian regulatory framework is already extremely nuanced with robust legislations to prosecute cybercriminals and protect child and women safety. The need is to focus on effective implementation of the laws and capacity building of the LEAs.[23] The American Invest in Child Safety Act aimed at enhancing the capacity of the state machinery is a crucial legislation in this regard that India can take inspiration from.[24]

[21] Decryption Rules, 2009. Retrieved from https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Procedure%20and%20Safeguards%20for%20Interception%2C%20Monitoring%20and%20Decryption%20of%20Information%29%20Rules%2C%202009.pdf

[22] Mohanty, B. (2019, May 30) *The Encryption Debate in India*, Carnegie Endowment for International Peace. Retrieved from https://carnegieendowment.org/2019/05/30/encryption-debate-in-india-pub-79213

[23] Shreya, S., & Mehta, S. (2021, February, 25). Time to tackle online gender violence. The Pioneer. Retrieved from https://www.dailypioneer.com/2021/columnists/time-to-tackle-online-gender-violence.html

[24] Section 4, Invest in Child Safety Bill, 2021. Retrieved from https://www.congress.gov/bill/117th-congress/senate-bill/223/text

2. ANALYSING EXPERIENCES FROM THE GROUND- PART II OF THE IT RULES, 2021

The IT Act accords safe harbour protection to the intermediaries, wherein they are protected from all forms of liability in respect of third party user generated content, provided they meet the conditions as laid down under Section 79 of the IT Act, and also the additional due diligence requirements prescribed under the Rules made under this provision.[25] This protection is a critical shield from legal consequences in cases wherein the platforms have no 'actual knowledge' of the illegality of the content. The immunity ensures protection from unwarranted legal repercussions and ensures an enabling environment for businesses to expand and innovate. It also serves as the cornerstone of digital rights by protecting user generated speech from unwarranted censorship by the intermediaries.[26] It allows the creation of a free, open and inclusive digital space that empowers people with their constitutionally guaranteed fundamental human rights.

This chapter analyses the compliance experience of the intermediaries regulated by Part II of the Rules. Inputs received from the intermediaries are analysed alongside the inputs from legal, technical and public policy experts, and The Dialogue's research to determine the overall impact of the mandates in the digital ecosystem, it's effectiveness in curbing online harms and it's interaction with goals of innovation and ease of doing business.

2.1. CREATION OF DIFFERENTIAL OBLIGATIONS BASED ON PLATFORM SIZE

Differential classes of intermediaries are created by the Rules, with Rule 2(w) classifying social media intermediaries while Rules 2 (v) going a step ahead and creating a sub-classification of 'significant social media intermediaries'.[27] The threshold for being considered a significant social media intermediary has been notified as 50 lakh (5 million) registered users in India.[28]

Majority of the respondents, including the intermediaries, as well as subject matter experts noted that in a country like India with a population of 1.3 billion people, setting a threshold of 5 million is quite low. The stakeholders mentioned that early stage companies and startups would easily fall under this category, and face heavy compliance burden which may impact their ease of doing business. Several respondents compared this with the limits in other foreign jurisdictions, especially the NetzDG legislation in Germany that fixed a threshold of

---

[25] Section 79, IT Act, 2000.
[26] Shreya, S., & Tiwari, P. (2022, December 26). *Analysing the American Safe Harbour Regime*: Takeaways for India, (p. 20). The Dialogue. Retrieved from https://thedialogue.co/wp-content/uploads/2020/12/Analysing-the-American-Safe-Harbour-Regime_Takeaways-for-India_The-Dialogue.pdf
[27] Rule 2(v), IT Rules, 2021.
[28] Ministry of Electronics and Information Technology. (2021). Notification. Retrieved from https://www.meity.gov.in/writereaddata/files/Gazette%20Significant%20social%20media%20threshold.pdf

2 million in the country, where just 73 million people are estimated to be using the internet.[29] This means that the limit prescribed under the German law is 2.7% of the digital users, whereas in India with almost 776 million internet users,[30] the threshold is 5 million which is merely 0.64% of the country's digital population. The primary inputs as well as our analysis shows that re-evaluation of this threshold in consonance with the population size is critical to ensure targeted regulation without impinging upon the business interests of emerging startups.

Additionally, as per Rule 6, the government can order any intermediary to comply with obligations imposed on a significant social media intermediary under Rule 4, provided it satisfies the threshold of '*a material risk of harm to the sovereignty and integrity of India, security of the state, friendly relations with foreign states or public order*'.[31] Most of the intermediaries across the technology ecosystem, as well as many lawyers and public policy experts, noted that in the absence of a clear definition of what constitutes '*material risk of harm*,' this provision is rendered vague.

They added that this poses the risk of discriminatory compliance requirements owing to the absence of adequate checks and balances on the exercise of the power conferred under this provision. Many respondents highlighted that though the government has not used this provision in the last one year, the nature of the power is quite overwhelming, where the executive is provided a statutory blank cheque to pursue any intermediary. Lack of safeguards on the exercise of this power can be a case of excessive delegation to the executive, leading to an arbitrary impact on intermediaries, who may be forced to comply with the additional due diligence mandates.

[29] United Nations Population Division (2019) World Population Prospects: 2019. The World Bank. Retrieved from https://data.worldbank.org/indicator/SP.POP.TOTL?locations=DE
[30] TRAI (2021, January 21) *The Indian Telecom Services Performance Indicators July – September, 2020*, Telecom Regulatory Authority of India. Retrieved from https://www.trai.gov.in/sites/default/files/QPIR_21012021_0.pdf
[31] Rule 6, IT Rules, 2021.

TABLE 1: KEY INSIGHTS ON CREATION OF DIFFERENTIAL OBLIGATIONS BASED ON PLATFORM SIZE

KEY INSIGHTS

- **Onerous Threshold:** Majority of the intermediaries noted that in a country like India with a population of over 1.3 billion setting a threshold of 5 million is quite onerous from an ease of doing business standpoint.
- **Global Context:** Several lawyers and public policy professionals compared the threshold with those in the foreign jurisdictions and mentioned that the prescribed limit is significantly lower than international standards.
- **Checks and Balances:** Majority of the intermediaries, lawyers and public policy professionals noted that lack of safeguard on the exercise of the power under Rules 6, can be a case of excessive delegation to the executive, leading to an arbitrary impact on intermediaries of all sizes across the technology ecosystem.
- **SOPs on calculation of threshold and exercise of executive power:** A detailed Standard Operating Procedure must be published explaining the criteria for calculation of the threshold and guiding the exercise of power by the executive under Rule 6.

2.2. DUE DILIGENCE & GRIEVANCE REDRESSAL BY DIGITAL INTERMEDIARIES

2.2.1. Timeline for content takedown and assisting the LEAs

Under the IT Rules, intermediaries must complete the takedown process under Section 79(3) of the IT Act, within 36 hours [Rule 3(1) (d)]. Further, the Rules have provided intermediaries with a 72-hour limit for providing information assistance to LEAs [Rule 3(1)(j)]. The Rules also add additional takedown requirements, wherein under specific scenarios, such as nudity, depiction of sexual conduct or impersonation, the intermediary is required to take down such content, upon request of the concerned user, within 24 hours [Rule 3(2)(b)].

Majority of the intermediaries highlighted that the singular takedown and information assistance timelines across all grades of harmful content have been a cause of concern for them. Intermediatries dealing with larger amounts of user based contents opined that such a '*one size fits all*' approach can be overwhelming, and impact innovation and investment in the ecosystem. Another issue highlighted by a larger number of intermediaries and lawyers was that the process by which LEAs can request takedown which is beyond the scope of Section 69A

IT Act, is also not defined in the Rules. This may lead to excessive delegation of power in the hands of the executive where any officer can request for any information without a clearly defined procedure. The inputs from the interview and The Dialogue's research explicates that there is a legitimate need for detailed SOPs to clarify the scope and nature of LEAs who are authorised to request information assistance under the IT Rules.

The number of such LEAs should be kept to the minimum so as to effectuate efficient monitoring of the implementation and compliance from all intermediaries. Many intermediaries, lawyers as well as public policy experts also discussed the form in which legal requests were received from LEAs. They emphasised that the SOPs on the IT Rules should provide for vital legitimacy to the far more efficient, safe and compliant means of raising legal requests by LEAs through the dedicated legal channels provided by all intermediaries. This ensures that the teams which are appropriately trained for responding to legal requests for content removal, information and preservation are directly looped in and are able to review and accordingly respond.

Another important concern highlighted by lawyers and civil society organisations was the digital rights implications of singular takedown and assistance norm without appropriate content gradation. Many respondents from these groups felt that due to the time crunch, it is possible that the intermediaries may end up censoring too much when the posts are taken down for obscenity or nudity because they are taken out of context. The time constraint is also harmful for posts and content related to minority hate crime, morphed media and cases of revenge porn.[33]

Research demonstrates that approximately 50% of takedown requests are targeted at potentially legitimate or protected speech.[32] Thus, given the severe implications of such takedowns on free speech and privacy of the users, it is crucial that a graded approach is taken where an extended timeline of four to five days is provided for takedown of content posing lesser serious grade of harm like defamation or contempt, while a shorter timeline of 24 hours is given for the takedown of content posing grave safety implications, such as proliferation of child pornography.

The Dialogue's assessment suggests that if every packet is construed an emergency packet then no packet will remain an emergency packet. The SOPs should provide gradation of the requests depending upon the degree of emergency and accordingly provide different timelines for each 'grade' of information. Additionally, takedown requests citing vague terms such as decency, public order, morality, etc. should be followed with appropriate court orders. This measure shall not only help the intermediaries assist the government more efficaciously by prioritising the grave and critical requests, but will also help the law enforcement agencies that face challenges owing to delay in information sharing in time-sensitive scenarios. Content gradation allows intermediaries to streamline their internal processes, which in turn helps them act more effectively on requests.

---

[32] Bar-Ziv, S., & Elkin-Koren, N. (2018). Behind the Scenes of Online Copyright Enforcement: Empirical Evidence on Notice & Takedown. Connecticut Law Review, 50. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3214214

[33] Ministry of Electronics & IT. (2019). *Public Comments On Draft Intermediary Guidelines, 2018*. Retrieved from https://www.meity.gov.in/writereaddata/files/Addendum1_Public_comments_on_draft_intermediary_guidelines.pdf

2.2.2. Timeline for Grievance Redressal

Under the Information Technology (Intermediaries Guidelines), 2011, grievance officer was responsible for receiving complaints from users concerning the Rules and redressing them within a month. In the IT Rules, 2021 the Grievance Officer is responsible for acknowledging complaints within 24 hours and resolving them within a timeline of 15 days.[34] The official has also been made responsible for the receipt and acknowledgement of any order, notice or direction issued by the appropriate government, any competent authority or a court of competent jurisdiction.

A large number of civil society organisations, especially women and child safety experts, noted that these timelines have been useful to ensure better responsiveness from the intermediaries. Respondents from these groups highlighted that a fast track mechanism for complaint redressal is in the users' best interest, especially in matters posing grave online safety threats, and the Rules have been successful in ensuring the same. The intermediaries had a mixed response to this issue. Most of the smaller companies informed us that they receive five to ten complaints per month and they have not faced any major challenge in resolving them. The larger intermediaries also said that they have been successful in instituting an effective grievance redressal process and have ensured compliance with the mandate. However, considering the deluge of grievances received by them, they noted that it becomes difficult to ensure a fair application of mind to every complaint and resolve it judiciously within such a limited time.[35]

The Dialogue's research coupled with the opinion of legal and policy experts explicates that a gradation of user complaints based on the severity of the risk is a more sustainable way forward. While a limited time for acknowledging the grievances is reasonable to ensure accountability from the intermediaries, timeline for redressal should vary depending on the nature of the grievance. In grievances related to women and child safety, a shorter timeline should be prescribed, however for lesser serious harms like contempt and trademark infringement an extended timeline should be given for redressal.

2.2.3. Timeline for Mandatory Data Retention

Rule 3(1)(h) has doubled the mandatory period of data retention. Any data which has been the subject of a removal order, and user account data of a deleted account-both need to be preserved for 180 days as opposed to the earlier 90 days.

Majority of the intermediaries noted that the data retention mandates are difficult considering that in order to comply with the global data minimisation norms, companies generally preserve user data for only 90 days. Data minimisation is one of the fundamental principles for safeguarding informational privacy followed by all the privacy respecting regimes across the

---

[34] Rule 3(2)(a)(i), IT Rules, 2021.
[35] Dash, Z. (2018, February 10). Do Our Wiretapping Laws Adequately Protect the Right to Privacy?. Economic and Political Weekly Enagage, 53(6). Retrieved from https://www.epw.in/engage/article/can-government-continue-unhindered-wiretapping-without-flouting-right-privacy

world. This principle means that only relevant and limited personal data must be collected that is sufficient to fulfil the designated purpose. The statement of objects and reasons along with Clauses 6 and 7 of India's Personal Data Protection Bill, 2019, also reinforces the values of data minimisation.

The intermediaries and technical experts emphasised that new technical solutions needed to be developed and a re-calibration of the existing infrastructure was required to comply with this mandate. Given the technicalities involved, respondents across the board felt that the three months period that was given for complying with the Rules was insufficient. Such a major overhaul in data storage and processing capabilities requires building capacity in the form of upskilling, technical upgradation and integration of these changes in the existing workflows.

In light of these complexities, many legal and technical experts advised adopting a 90 + 90 days approach in the SOPs. The intermediaries may store the data for the original 90 days period to begin with, and then depending upon the relevance of any particular data for an ongoing investigation etc., the same may be retained further, while the rest of the data may be deleted. This mechanism will reduce the compliance costs for the intermediaries and also ensure adherence with the privacy and data minimisation norms.

TABLE 2: KEY INSIGHTS ON DUE DILIGENCE AND GRIEVANCE REDRESSAL MANDATES FOR INTERMEDIARIES UNDER RULE 3

KEY INSIGHTS

- **Content gradation:** Majority of intermediaries dealing with large amounts of user generated content noted that singular timelines for information assistance and content takedown across all grades of user generated content is overwhelming and impacts investment.
- **SOPs on information assistance requests by LEAs:** Majority of respondents from all stakeholder groups mentioned the need for clear Standard Operating Procedures to delineate the process and format of information requests by the LEAs.
- **SOPs for checks and balances on LEA access:** It is important that the SOPs provide legitimacy to the far more efficient, safe and compliant means of raising legal requests through dedicated legal channels provided by all intermediaries.
- **Greater platform accountability:** Many civil society organisations and safety bodies noted that delineation of specific timelines for acknowledgement and redressal of user grievance has been very helpful in ensuring better responsiveness from the intermediaries.

- **Preserving data minimisation principles in the SOPs:** Many legal and technical experts highlighted the inconsistency of the data retention mandate with principles of data minimisation and suggested the adoption of a 90 + 90 days approach through the SOPs instead of 180 days.

2.3. ADDITIONAL DUE DILIGENCE REQUIREMENTS OF SIGNIFICANT SOCIAL MEDIA INTERMEDIARIES

2.3.1. Appointment of Additional Personnels & Their Personal Liability

In addition to the obligations for all digital intermediaries, SSMIs have additional requirement of appointing three officers: a Chief Compliance Officer (responsible for ensuring compliance with the IT Act and the rules made therein), a nodal officer (to coordinate with the LEAs) and a resident grievance officer (having functions similar to those of the CCO). The Chief Compliance Officer is supposed to be a key managerial personnel from the company, who can be held personally liable for any company failure to meet the due diligence requirements prescribed by the law. Based upon penalties outlined in Sections 69 and 69A of the IT Act, this could include prison terms up to seven years, as well as significant fines.

The majority of the respondents agreed that the creation of these portfolios such as a Nodal Officer and a Grievance Officer is a welcome step that shall ensure better accountability on part of the platforms leading to better protection of user interests in the digital space. The Resident Grievance Officer is also supposed to give a prior notice to the user whose content has been removed while explaining the action being taken and the grounds or reasons for such action.

Many subject matter experts including lawyers and digital rights experts noted that these mandates reinforce the ideals of the Santa Clara Principles,[36] which is the global framework on platform regulation and also the fundamental ethos of natural justice.[37] It will go a long way towards ensuring transparency and accountability in the actions of platforms that impact human rights.

However, personal liability of the Chief Compliance Officer was strongly opposed by majority of the intermediaries interviewed. Majority of the lawyers noted that despite the need for effective reporting lines between the intermediaries and the government, subjecting individual employees to criminal liability is both unnecessary and disproportional. This is especially true in light of the fact that criminal liability demands a much higher burden of wrongdoing. However, given the huge volume of third party content that might be violative of the rules, CCOs may not always have the malicious intent that is essentially associated with criminal liability. Section 79 of the IT Act under which the IT Rules have been notified, empower the government to

prescribe due diligence mandates for intermediaries. Accordingly, any *breach of duty* under the Rules should be the sole liability of the intermediaries and not its employees. Personal liability for employees may lead to increased censorship, where the threat to employee safety would compel the platforms to always err on the side of caution, thus potentially over censoring content.

Intermediaries noted that overwhelming costs of regulatory compliance pose substantial economic burden when taken in combination with expectations to prohibit and aggressively police vaguely defined forms of content, engineer access to data, and fulfil difficult due diligence requirements. Many lawyers and tech policy experts observed that in today's era of decriminalisation of multiple legislations, including the Companies Act, 2013, criminal liability of employees for company's failures is restrictive for the goals of ease of doing business and innovation. It might also impact India's image as a propitious business destination and create barriers where foreign investors may deter from investing in India to avoid the additional challenge of recruiting and then ensuring the protection of their employees from such potential criminal sanctions.[38]

2.3.2. Originator Traceability

The growing challenge of fake news and child sexual abuse material on messaging platforms has been a cause of concern for the state machinery since a long time now, and in order to tackle the same, Rule 4 (2) of the Rules mandates enabling technical measures to identify the first originator of the information on its computer resource (the identity of the person who generated a message) on significant social media messaging platforms.[39]

Despite the good intent, this provision has been critiqued widely by not just the intermediaries, but also a majority of the technical[40] and legal[41] experts who have noted its unavoidable implication of putting an end to end-to-end encryption.

---

[36] The Santa Clara Principles: On Transparency and Accountability in Content Moderation. Retrieved from https://santaclaraprinciples.org
[37] Ombudsman for Banking Services and Investments. *Natural justice and procedural fairness at OBSI*. Retrieved from https://www.obsi.ca/en/how-we-work/resources/Documents/Principles-of-Natural-Justice-in-Ombudsmanship.pdf
[38] Shreya, S. (2021, July 6). What Twitter Case Tells Us About Issues with India's IT Regime. The Quint. Retrieved from https://www.thequint.com/voices/opinion/what-twitter-case-tells-us-about-issues-with-indias-it-regime-it-rules-2021-chief-compliance-officer
[39] Rule 4 (2), IT Rules, 2021.
[40] The Dialogue, *Analysing the Technical Workarounds to End-to-end encryption*. (2022). Retrieved from https://www.ijlt.in/post/analysing-the-technical-workarounds-to-end-to-end-encryption
See also: Nojeim, G. & Maheshwari, N. (2021). Encryption in India: Preserving the Online Engine of Privacy, Free Expression, Security, and Economic Growth. Indian Journal Of Law And Technology, 17(1). Retrieved from https://www.ijlt.in/journal/encryption-in-india%3A-preserving-the-online-engine-of-privacy%2C-free-expression%2C-security%2C-and-economic-growth
[41] Rizvi, K., & Singh, S. (2021, March 15). *Does The Traceability Requirement Meet The Puttaswamy Test?*. Live Law. Retrieved from https://www.livelaw.in/columns/the-puttaswamy-test-right-to-privacy-article-21-171181
See also : Grover, G., Rajwade, T., & Katira, D. (2022). The Ministry And The Trace: Subverting End-To-End Encryption. NUJS Law Review, 14(2). Retrieved from http://nujslawreview.org/2021/07/09/the-ministry-and-the-trace-subverting-end-to-end-encryption/

FIGURE 5: RAMIFICATIONS OF BREAKING ENCRYPTION[42]

[42] Shreya, S., & Tiwari, P. (2022, December 26). *Analysing the American Safe Harbour Regime: Takeaways for India*, (p. 20). The Dialogue. Retrieved from https://thedialogue.co/wp-content/uploads/2020/12/Analysing-the-American-Safe-Harbour-Regime_Takeaways-for-India_The-Dialogue.pdf

In our conversation with subject matter experts on this issue, the lawyers observed that while the rules clarify that the provision is supposed to be used only in cases of serious offences, most of the categories of offences mentioned are open ended and can easily be subjected to abuse. The proviso noted that,

"Provided that an order shall only be passed for the purposes of prevention, detection, investigation, prosecution or punishment of an offence related to the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order, or of incitement to an offence relating to the above or in relation with rape, sexually explicit material or child sexual abuse material, punishable with imprisonment for a term of not less than five years:"[43]

The purposes outlined are overly broad and do not meet the proportionality test ruled in the *Puttaswamy* judgement. It was also noted by some of them that the rule mentions that in identifying the originator, the intermediary shall not be required to disclose the content of the message. However, when read alongside the Decryption Rules,[44] the State authorities have the power to demand not just the details of the originator but also that of all the recipients of the said message and the content of the message.[45]

The intermediaries and cybersecurity experts were unanimous in their opinion that it is technically impossible to introduce traceability on encrypted platforms without breaking the encryption technology itself. End-to-end encryption is a critical aspect of maintaining confidentiality in technologically driven communications.. It protects user privacy in the everyday conversations that we have with our friends and partners, and empowers women and other marginalised groups to fearlessly voice their views on public platforms using the veneer of encryption enabled anonymity.[46]

The cybersecurity experts also noted that traceability is in fact an ineffective tool for LEAs given that it can be easily spoofed leading to innocent citizens being falsely incriminated.[47] Similarly, majority of the lawyers tested it on the threshold of the Puttaswamy judgement and highlighted that the provision does not satisfy the four-fold test laid down by the Supreme Court to determine the validity of restrictions on privacy, which calls for the existence of a legitimate aim, suitability or rational nexus, necessity, and proportionality.[48]

The aim of preventing threat to national security is too broad and vague given that there does not exist any precise definition of national security, either under these rules or anywhere else. Intermediaries and policy experts, in addition to the lawyers, stressed that the solution is

---

[43] Rule 4(2), IT Rules, 2021.
[44] Rule 3, Decryption Rules, 2009.
[45] Rodriguez, K. (2021, June 2). *Why Indian Courts Should Reject Traceability Obligations*. Electronic Frontier Foundation. Retrieved from https://www.eff.org/deeplinks/2021/06/why-indian-courts-should-reject-traceability-obligations
[46] Tiwari, P., & Shreya, S. (2020, October 31). *In the Digital Age, Here's How Encryption is Protecting Your Privacy*. The Bastion. Retrieved from https://thebastion.co.in/politics-and/in-the-age-of-the-internet-heres-how-encryption-is-protecting-your-privacy/
[47] *WhatsApp drags Govt to court on new message tracing rules*. The Hindu Business Line. (2021, May 26). Retrieved from https://www.thehindubusinessline.com/companies/whatsapp-drags-govt-to-court-against-new-it-rule-on-tracing-message-originator/article34646461.ece
[48] Rizvi, K., & Singh, S. (2021, March 15). Does The Traceability Requirement Meet The Puttaswamy Test?. Live Law. Retrieved from https://www.livelaw.in/columns/the-puttaswamy-test-right-to-privacy-article-21-171181

not suitable given that the savvy cybercriminals can easily shift to unregulated encrypted platforms.

As per the SIRIUS EU Digital Evidence Report (2021), out of the 208 law enforcement agency officials interviewed, only 20% selected content data amongst the top three data sets required for investigation.[49] For the remaining 80%, metadata like phone number, registration details, IP address etc. was sufficient. Moreover, as per a revelation under the Freedom of Information Act, the FBI disclosed its ability to legally access secure messaging app content and metadata like subscriber data, message sender/receiver data, device backup, IP address, date/time of information, registration time data, user contacts among other data sets that do not require breaking encryption.[50] If encryption is compromised, then savvy criminals will simply shift to unregulated encrypted platforms.[51]

With criminals moving to unregulated encrypted platforms, it will put the government in a difficult position where access to metadata may not be possible.[52] Cybercriminals shall continue to use encryption while it is the privacy of innocent citizens that shall be at bay. The argument of necessity also fails to stand as cybersecurity experts and veterans from law enforcement highlighted that solutions like metadata analysis and development of traditional surveillance technologies are far less intrusive and more sustainable and effective.[53]According to The Dialogue's study on national security implications of weakening encryption, based on qualitative inputs from veterans in law enforcement and intelligence agencies, noted that weakening encryption[54] would lead to more security concerns than it seeks to resolve. The experts expressed their agreement on the importance of end-to-end encryption in ensuring informational privacy, safety and security of citizens and national security. The report recommends pausing legislation of encryption hostile laws, committing to surveillance reforms and conducting evidence-based research on encryption technology and more specifically on the modern technology requirements of the law enforcement agencies.

Another significant point that came to fore in the response of not just cybersecurity and legal experts but also the civil society organisations, was that undermining end-to-end encryption not just makes the platform even more vulnerable to attack by cybercriminals but also to foreign espionage. It opens doors to greater national security threats,[55] thereby defeating the argument of proportionality as well.

---

[49] SIRIUS EU. (2021). *SIRIUS EU Digital Evidence Situation Report*. Retrieved from https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS_DESR_12_2021.pdf

[50] Federal Bureau of Investigation. (2020). *Lawful Access*. Retrieved from https://s3.documentcloud.org/documents/21120480/fbi-doc.pdf

[51] Graham, R. (2016, June). How Terrorists Use Encryption. CTC Sentinel, 9(16), 20-25. Retrieved from https://www.ctc.usma.edu/how-terrorists-use-encryption/

[52] Graham, R. (2016, June). How Terrorists Use Encryption. CTC Sentinel, 9(16), 20-25. Retrieved from https://www.ctc.usma.edu/how-terrorists-use-encryption/

[53] Azad, Y., & Venkatnaryanan, A. (2021, July 6). *IT Rules 2021: Govt should not weaken fundamental right to privacy in the name of security*. The Economic Times. Retrievable from https://economictimes.indiatimes.com/opinion/et-commentary/privacyand-protection-possible/articleshow/84151895.cms?from=mdr

[54] Azad, Y., Venkatnarayanan, A., Tiwari, P., & Chatterjee, S. (2022, January 12). *Analysing the National Security Implications of Weakening Encryption*. The Dialogue. Retrieved from https://thedialogue.co/wp-content/uploads/2022/01/Report-_-National-Security-Encryption-_-The-Dialogue-DeepStrat-_-Jan-12-2022.pdf

2.3.3. Proactive Monitoring

Rule 4 (5) envisages the deployment of AI-enabled automated tools or other mechanisms to proactively identify information that depicts any act or simulation in any form depicting rape or CSAM whether explicit or implicit.[56]

This provision is a better version of the Draft Intermediary Liability Rules of 2018[57] as the use of the word 'endeavour' in the provision suggests that the intermediaries are required to do so only on a best effort basis. However, given the unpredictable ramifications[58] of using AI technology in content moderation, many digital rights organisations observed that there is a need to make the provision more robust. The organisations also highlighted that while these automated tools are presently proposed to be deployed in respect of only highly objectionable content, such as depictions of rape or CSAM, such a measure is nevertheless concerning, as once technical changes are implemented in the systems they tend to exhibit functional creep in the short to medium term. For example, the tools to check for CSAM may well be customised to censor those whose content may be politically inconvenient but ostensibly legal. Tampering of the training data used or the hash register relied upon could also lead to concerns like viewpoint discrimination.

Multiple civil society organisations and lawyers noted that proactive monitoring poses challenges for both, the fundamental right to free speech and privacy of the users. This is because constant monitoring of user activity poses concern for their informational privacy and the filters are not nuanced enough to analyse content on a case by case basis, so the platforms are likely to overcompensate by censoring any speech that falls within the grey area.

There are no established thresholds and standards to gauge the dependability of automated tools. The Dialogue's research shows that letting the social algorithms do the content moderation task can be challenging at multiple levels, including the inability of global-data trained AI to appreciate the local context of speech or media content;[59] its limited capacity to proactively monitor content in regional languages, when there are so many languages in India and very limited training data, and finally, the high cost of building its algorithms.[60] The cost challenge is especially critical for startups and other small businesses with limited economic bandwidth and expertise. Compliance with this mandate requires extremely high investment owing to the costs involved in the required technological calibrations and the expense of the needed tools.

Majority of the intermediaries noted that given the large volumes of harmful content, proactive monitoring has certainly emerged as a critical tool to tackle the online safety challenges at a larger scale and in a timely manner. However, it is imperative that its use continues to be

---

[55] Prevelakis, V., & Spinellis, D. (2007, June 29). *The Athens Affair.* IEEE Spectrum. Retrieved from https://spectrum.ieee.org/telecom/security/the-athens-affair
[56] Rule 4(5), IT Rules, 2021.1.
[57] Draft Intermediary Liability Rules, 2018. Retrieved from https://www.meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf
[58] Heinrichs, B. (2021). Discrimination in the age of artificial intelligence. *AI & SOCIETY*, 37(1), 143-154. https://doi.org/10.1007/s00146-021-01192-2
[59] Vaidyanathan, M., & Rizvi, K. (2020, April 29). Social Media Platforms: A Theater for Exercising Free Speech. Rights View. Retrieved from https://blogs.cuit.columbia.edu/rightsviews/2020/04/29/social-media-platforms-a-theater-for-exercising-free-speech/
[60] Pande, T., & Shreya, S. (2021, January 25). *Make AI evolution inclusive in India*. The Pioneer. Retrieved from https://www.dailypioneer.com/2021/columnists/make-ai-evolution-inclusive-in-india.html

directed as a suggestive measure only and not as a mandatory precondition for availing safe harbour protection. This will preserve both free speech of the users and promote ease of doing business. It is crucial that the SOPs and the proposed amendment to the IT Act explore avenues for providing more regulatory flexibility to the intermediaries to innovate and take action against high risk content. Encouraging intermediaries to invest in technological innovation, the expansion and use of shared databases of hashes and URLs and more efficient notice and takedown procedures are some innovative policy measures that must be promoted for effective redressal of online harms.[61]

2.3.4. User Verification

Rule 4 (7) prescribes the requirement for SSMIs to allow their users to voluntarily verify their accounts, using any appropriate mechanism including their active Indian mobile number,[62] a feature popularly termed as 'blue ticking'. This mandate has received mixed responses from the stakeholders involved.

In our interviews, many safety organisations noted that the emerging online harms including fake news, CSAM and trolls take advantage of the anonymity provided by social media. However, digital rights experts noted that though the provision is envisaged to be operationalised on a voluntary basis, it can lead to the creation of two types of users and open avenues for discrimination and curtailment of rights for the people who opt out of the verification process. Civil society organisations and many lawyers also added that having KYC like norms for accessing social media can be challenging for anonymous users and whistleblowers given that there may be many legitimate reasons as well because of which someone would want to use a pseudonym online. For such individuals and the organisations that support them, securing anonymity can be critical. Anonymous communications have an important place in social and political discourse. In fact, the American Supreme Court in *McIntyre v. Ohio Elections Commission* recognised it as an essential component of the right to free speech protected under the First Amendment of their Constitution.[63]

Anonymity can be inconvenient from a regulatory standpoint. However, it serves to keep the free flow of information and opinions in a digital space - an aspect that may be lost permanently in a straitjacketed verification ecosystem. Accordingly, it is critical to find a balance wherein the platforms at all times must possess limited meta data on activity of all users. This will ensure that when the LEAs request metadata to catch criminals using platforms for illegal activities on the presentation of a legal warrant per procedure established by law then the platforms should be in a position to comply.

---

[61] *Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse*. WeProtect. (2020). Retrieved from https://www.weprotect.org/wp-content/uploads/11-Voluntary-principles-detailed.pdf
[62] Rule 4 (7), IT Rules, 2021.
[63] *McIntyre v. Ohio Elections Commission*, 514 U.S. 334.

TABLE 3: KEY INSIGHTS ON ADDITIONAL DUE DILIGENCE FOR SSMIs UNDER RULE 4 AND COMPLIANCE REQUIREMENTS UNDER PART II OF THE IT RULES , 2021

KEY INSIGHTS

- **Ramifications of personal liability:** Personal liability of the chief compliance officer was strongly opposed by majority of the stakeholders. They highlighted that it is inconsistent with established criminal law principles and has led to excessive economic burden for the intermediaries owing to the challenges of hiring for this position and the impending threat of legal action.

- **Infeasibility of originator traceability:** Intermediaries and cybersecurity experts mentioned that it is technically impossible to introduce traceability on encrypted platforms without breaking the encryption technology which is the biggest shield for cybersecurity and user privacy.

- **SOPs for deployment of proactive monitoring:** Majority of the intermediaries highlighted that proactive monitoring has emerged as a critical tool for tackling the deluge of harmful content. However, given the impending challenges around both free expression and ease of doing business, it is imperative that its deployment is directed on a best effort basis only.

- **Balancing anonymity and safety:** The mandate on user verification received mixed responses from the respondents. Accordingly, while preserving anonymity is important to protect the digital rights of vulnerable communities, intermediaries must collect limited meta data on activity of all users.

- **Response by intermediaries on ease of doing business and entry barriers:** 87.5% of the intermediaries responded that the compliance mandates in Part II of the IT Rules, 2021 may lead to creation of entry barriers and impact their ease of doing business in India.

- **Response by other stakeholders on ease of doing business and entry barriers:** 85% of the other stakeholders including lawyers, public policy professionals, civil society organisations and academics noted that the compliance mandates in Part II of the IT Rules, 2021 may lead to creation of entry barriers and impact ease of doing business in India.

3. REVAMPING THE IT ACT: FEEDBACK FROM STAKEHOLDERS

The IT Act, 2000 was passed to give effect to the UNCITRAL framework of the 1990s. With drastic change in how society interacts in the digital realm, it is necessary to revisit the legislation. The proposed IT Act framework, whether through an amendment or a new legislation altogether, should cater to the key stakeholder concerns discussed below:

3.1. ENABLING A PROGRESSIVE INTERMEDIARY LIABILITY REGIME

The IT Rules, 2021 are a crucial initiative by the government to better regulate platforms in the digital space. The Rules entailed a major shift from the pre-existing regime in the IL Guidelines, 2011. The primary inputs from the stakeholders across the digital technology realm iterated in the previous chapters, highlight some of the key concerns with the IT Rules, 2021. The attempt to reimagine the IT Act must entail the alignment of the intermediary liability regime with the jurisprudence established by the hon'ble Supreme Court of India and global best practices. This entails that the standard of 'actual knowledge' prescribed in the *Shreya Singhal* case is adhered to, and that no criminal responsibility is imposed on employees of the intermediaries in adherence to the global best practices. It will be crucial that the new regime finds a balance between furthering fundamental rights in the digital realm, ensuring user safety and security, and holding intermediaries accountable. This balancing will aid the establishment of a stable, and predictable regime inspiring investor confidence and further ease of doing business in India.

3.2. INSTILLING PROCEDURAL SAFEGUARDS IN PROVISIONS FOR LAW ENFORCEMENT ASSISTANCE, SEARCH AND SEIZURE

It is crucial that the upcoming IT Act framework instils necessary procedural safeguards for affected parties when provisions for law enforcement assistance, and search and seizure are triggered. These include adequate notice, and written orders for document requests along with an opportunity to contest orders. Another reformative step required is to allow affected parties to mark certain documents as confidential or sensitive, requiring authorities to exercise a higher degree of safeguards when taking custody of such documents.

3.3. ENABLING A PROGRESSIVE ENCRYPTION REGIME

Encryption technology is a key enabler of human rights in the digital space. Advanced encryption is crucial to protect the data in the digital realm which is increasingly susceptible to cyber vulnerabilities. Moreover, any form of backdoor mandate for traceability or client-side scanning is replete with challenges rendering the entire citizenry vulnerable to cyberattacks. Research establishes that legitimate national security imperatives of the state can be fulfilled by asking platforms data sets which do not require breaking advanced encryption like end-to-end encryption. The proposed IT Act framework must ensure that principles of necessity, proportionality and data minimisation as envisaged in the *Puttaswamy judgement* are appropriately imbibed.

3.4. FURTHERING A UNIFORM AND TRANSPARENT CONTENT BLOCKING REGIME

Given content blocking is a necessary check on the operations of digital platforms, it is crucial to ensure that the overlapping regimes under Section 69A and the Rules 3(1)(d) of IT Rules, 2021 read with Section 79 IT Act are harmonised. Revisiting the overarching executive powers under Rules 15 and 16 of the IT Rules for content blocking for both, the platforms governed by Part II and Part III of the Rules is imperative. It is crucial that the procedural safeguards envisioned in the Parent act (Section 69A) are adhered to in all subordinate legislations.

Further, Section 69A defines that scope of exercising the blocking powers by the executive. The IT Act amendment should ensure that any blocking order beyond the scope defined in Section 69A, is accompanied by a court order. This is important because the blocking order entails determination of legal rights of the publisher of the content in question. Thus, it would be important that the committee is headed by a judicial officer or a retired justice of a constitutional court. Lastly, the proposed IT Act amendment should aspire to ensure that the review mechanism is transparent and that the affected party gets the opportunity of hearing.

3.5. NO CORPORATE CRIMINAL LIABILITY

The IT regime should not entail criminal responsibility of the employees of the platforms regulated. This will not just be in line with the global best practices, but also with the Indian efforts, such as decriminalising provisions of the Companies Act, 2013 and the Legal Metrology Act, 2009. Civil penalties are not only effective but also further ease of doing business. Accordingly, the scope of the existing Section 85 should not be expanded in any subsequent iteration and be adhered to by subordinate legislation as well.

3.6. ENHANCING CYBERSECURITY

The information seeking powers of Indian Computer Emergency Response Team (CERT-In) are broad. It is imperative that the safeguards envisioned in Section 69 of the IT Act are also built into Section 70B of the IT Act along with purpose limitation on information seeking powers of CERT-In. For instance, the recent CERT-In Direction mandating data retention for 5 years and mandatory reporting of all cybercrimes within a restrictive period of 6 hours, irrespective of the degree of harm, is inconsistent with the principles of data minimisation and may pose operational challenges for the platforms. While wider stakeholder consultation is imperative to determine the feasibility of these mandates, ensuring adequate checks and balances on the powers of nodal institutions under the Parent Act is equally paramount.

3.7. EXTENSIVE MULTI STAKEHOLDER CONSULTATION

A key concern raised post the introduction of the IT Rules, 2021 was lack of effective stakeholder consultation. It will be crucial that the proposed IT Act framework is only passed after extensive consultation with subject matter experts including technical experts, legal and policy professionals, civil society, child and women safety bodies, academics, digital platforms, law enforcement, and other sectoral regulators.

3.8. CAPACITY BUILDING

The digital space is an ever-growing ecosystem. It would be beneficial to designate a statutory authority to empower the various wings of the state and the citizenry on aspects of information technology. The American Invest in Child Safety Act creates a mandatory funding of 5 billion dollars along with 100 FBI agents and 65 more positions to tackle online sexual abuse. It will be beneficial to create a similar funding for law enforcement aiding them with more personnel and technology to tackle cybercrimes.

4. POLICY RECOMMENDATIONS

With globalisation in this information age, updating regulatory and technological prowess is crucial to ensure national interest both in security and economic terms. However, with several experts flagging certain concerns, it is important to engage in meaningful dialogue and ensure adequate responsiveness on part of all the stakeholders to create a robust platform regulation regime that harmonises the quest for economic growth empowerment while ensuring national security and preservation of digital rights.

I. **Sustained consultation with civil society and technical experts is encouraged to drive the global best practices for platform accountability in the Indian regime.**

II. **Revisit the threshold prescribed under the IT Rules, 2021 for classification of SSMIs in light of international practices, and India's economic interests.**

III. **Adopt a risk based content gradation mechanism guiding response timelines for takedowns and information assistance.**

IV. **Revisit the data retention mandate in light of privacy harms and compliance costs.**

V. **Remove the personal liability provision considering its legal infeasibility and economic repercussions and replace it with corporate financial penalties as the norm.**

VI. **Do not implement the originator traceability mandate given its potential to undermine users safety and national security.**

VII. **Do not make safe harbour protection contingent on proactive monitoring given the inherent biases that are likely to creep into such technologies.**

VIII. **Uphold the broad immunity protection for intermediaries in accordance with the Shreya Singhal mandate to preserve the free, open and secure nature of the internet.**

IX. **Publish implementable Standard Operating Procedures in consultation with experts to cater to the operational challenges within the IT Rules, 2021.**

X. **Institutionalise multi stakeholder approach for policy making and adopt a collaborative Rule making approach for the revamp of the IT Act, 2000.**

Imprint

Recommended Citation: Shruti Shreya and Pranav Tiwari. (2022, July 4). *IT Rules, 2021: A Regulatory Impact Assessment Study*. (Vol. 1). New Delhi. The Dialogue and Internet & Mobile Association of India.

The Dialogue™ is a public-policy think- tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue™ has been ranked as the world's Top 10 think- tanks to watch out for, by the Think-Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

www.thedialogue.co

The Internet & Mobile Association of India (IAMAI) is not-for-profit industry body registered under the Societies Act, 1896. Its mandate is to expand and enhance the online and mobile value added services sectors. It is dedicated to presenting a unified voice of the businesses it represents to the government, investors, consumers and other stakeholders.

www.iamai.in