INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 3 AND ISSUE 1 OF 2023

INSTITUTE OF LEGAL EDUCATION

Indian Journal of Legal Review [ISSN - 2583-2344]

(Free and Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 3 and Issue 1 of 2022 (Access Full Issue on - https://ijlr.iledu.in/volume-3-and-issue-1-of-2023/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education (Established by I.L.E. Educational Trust)

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR]

Volume 3 and Issue 1 of 2023

ISSN - 2583-2344 *(and)* ISBN - 978-81-961120-2-8

Published by

Institute of Legal Education

https://iledu.in

IT (Intermediary Guidelines and Digital Media Ethics) Rules, 2021: Constitutionally Justified Or Not?

Authors: Abhishek Charan, Student of Alliance School of Law, Alliance University, Bangalore

Best Citation - Abhishek Charan, IT (Intermediary Guidelines and Digital Media Ethics) Rules, 2021: Constitutionally Justified Or Not?, Indian Journal of Legal Review (IJLR), 3 (1) of 2023, Pg. 459-465, ISSN - 2583-2344.

Abstract

On 25th February, 2021, the Ministry of Electronics and Information Technology and the Ministry of Information and Broadcasting notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021(herein after referred to as "IT Rules, 2021"). These rules triggered a discourse from all the stakeholders who are directly and indirectly affected by these guidelines. This comes after couple incidents of violence which are believed to have been caused through messages over platforms like WhatsApp, Facebook, Twitter, etc. and also on few films or shows which are released over platforms like Netflix, Amazon Prime, etc. 2021 has introduced significant due diligence requirements which need to be followed by any intermediary be it a significant social media intermediary, a news and current affairs content intermediary or an OTT platform. These rules relate to compelling interception, monitoring, and decryption of communications. These rules seem to violate Article 19(1) (a) by seeking to impermissibly deprive intermediaries of their safe-harbour protection under Section 79 of the IT Act, and violates the K.S Puttaswamy judgment- Article 21's guarantee of privacy by requiring traceability by design. This paper focuses on whether the IT Rules of 2021 complies the law set by the Hon'ble Supreme Court in K.S Puttaswamy v Union of India (2017) 10 SCC 1 and also whether the traceability mandate of the IT Rules would be helpful or not.

Keywords: IT Rules 2021, Traceability, Puttaswamy judgment and Right to Privacy

1.1. Introduction

The role of social media and online speech in civil society has come under heightened scrutiny. On 25th February, 2021, the Ministry of Electronics and Information Technology and the Ministry of Information and Broadcasting notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021(herein after referred to as "IT Rules, 2021"). These rules triggered a discourse from all the stakeholders who are directly and indirectly affected by these guidelines. As always, one set of scholars found solace after a long wait for the much-needed legislation to regulate the over-the-top (commonly referred to as "OTT") platforms like Netflix, Amazon Prime, AltBalaji etc. The other set of scholars looked at these rules as camouflage for government surveillance and strategic censoring, which violated the fundamental right to freedom of thought and expression.

In December 2018, the Ministry released the draft Information Technology (Intermediary Guideline) Rules, 2018 and asked for review through public consultation. They also evaluated and weighed it against the existing Information Technology (Intermediary Rules), 2011. But Ministry did not seek any consultation before notifying the IT Rules, 2021. They flouted the pre-legislative consultative policy set by the Ministry of Law and Justice back in 2014, by avoiding to consider any scrutiny from the various stakeholder by steering clear of the minimum 30-day period in this complex matter.

Back in December 2018, the MIB commission a ten-member board to *"frame and suggest a regulatory framework for online media/news portals including digital broadcasting and entertainment/ infotainment sites & news/ media aggregators"* but later in the same year, they were dissolved and the responsibility was turned to Ministry of Electronics and Information Technology. Initially, Ministry of Electronics and Information Technology identified this division

INDIAN JOURNAL OF LEGAL REVIEW [IJLR]

Volume 3 and Issue 1 of 2023

ISSN - 2583-2344 *(and)* ISBN - 978-81-961120-2-8

Published by

Institute of Legal Education

https://iledu.in

of legislative jurisdiction between regulation over OTT platforms and social media platforms by Ministry of Electronics and Information Technology and the Ministry of Information Broadcasting respectively. In 2020, the Government of India (Allocation of Business) Rules, 1961 were amended to give the jurisdictional power to MIB on the regulation of OTT platforms and online news media.[1306] The Government in its official press release statement regarding the IT Guidelines said that *"Amidst growing concerns around lack of transparency, accountability and rights of users related to digital media and after elaborate consultation with the public and stakeholders, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 has been framed in exercise of powers under section 87 (2) of the Information Technology Act, 2000 and in supersession of the earlier Information Technology (Intermediary Guidelines) Rules 2011."*[1307]

Part II of the IT Act ,2021 has introduced significant due diligence requirements which need to be followed by any intermediary be it a significant social media intermediary, a news and current affairs content intermediary or an OTT platform. These rules relate to compelling interception, monitoring, and decryption of communications. These rules seem to violate Article 19(1)(a) by seeking to impermissibly deprive intermediaries of their safe-harbour protection under Section 79 of the IT Act, and violates the K.S Puttaswamy judgment- Article 21's guarantee of privacy by requiring traceability by design. This is the main focus of this paper.

1.2. Literature Review:

(Maheshwari & Nojeim, 2021) in their article argue that the traceability mandate imposed in India by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 undermines encryption and negatively impacts cybersecurity as well as the fundamental right to privacy.

Similarly, in their working paper, Moksha Sharma and Keerti Pendyal (**Sharma & Pendtal, 2021**) have made an attempt to analyze the impact of Rule 3 of the IT Guidelines and have compared this to copyright legislations in India. Rule 3 requires intermediaries to perform due diligence by publishing on their platform (website and/or mobile application) the terms & conditions for accessing the services provided by the intermediary. They also have to inform the users to not "host, display, upload, modify, publish, transmit, store, update or share any information that" would violate the various provisions mentioned in Rule 3 (1) (b). The authors argue that several of these obligations appear to be reasonable expectations, the intermediary companies have a big role to play in our online interactions. The authors also argue that the language with respect to some of these rules is very vague and the vague nature of the terms used in the rules leaves them open to subjective interpretation of authorities.

The implications of Puttaswamy judgment have been lucidly explained by **(Bhandari & Sane, 2018)**. The authors seek to conceptualise the right to privacy and its implications from the State and private actors, post the Puttaswamy judgment. The authors also examine the draft Personal Data Protection Bill, 2018 submitted by the Justice Srikrishna Committe and evaluate how it has fared in regulating the actions of the State relative to the private sector, with a broad focus on consent, surveillance, and the interaction between the State and private sector including the ability of the latter to deny data requests of the former. The main argument of the authors is that that considering the privacy concerns against State action, the

[1306] Outlook (ed), "Govt Brings OTT Operators under Ambit of I&B Ministry" , available at: (*https://www.outlookindia.com/*November 11, 2020) < https://www.outlookindia.com/newsscroll/govt-brings-ott-operators-under-ambit-of-ib-ministry/1974311 > accessed 1st December, 2022

[1307] Ministry of Electronics and Information Technology through Press Information Bureau, Government notifies Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, (25th Feb,2021) available at < https://pib.gov.in/PressReleseDetailm.aspx?PRID=1700749 > accessed 25th November, 2022.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR]

Volume 3 and Issue 1 of 2023

ISSN - 2583-2344 *(and)* ISBN - 978-81-961120-2-8

Published by

Institute of Legal Education

https://iledu.in

challenge to implementation in the area of personal data may only get exacerbated.

In **(Siripurapu & Merrow, 2021)** authors argue that social media has been blamed for spreading disinformation and contributing to violence around the world. In this article, the authors first analyze how the social media platforms regulate the content and also include data on the content blocked by the media platforms. Then, they proceed to a comparative analysis of the regulating mechanisms employed by various governments around the world.

(Karnik, 2021) in their paper has attempted to critically analyze the IT Guidelines. The paper divides the analysis according to different verticals that will be affected by the Rules, namely, i) social media intermediaries like Facebook, Instagram, Twitter, ii) OTT platforms like Netflix, Amazon Prime and lastly iii) news and current affairs content providers like The Wire, LiveLaw. The author also looks into the intermediary rules of different countries, thereby providing a global perspective. The author concludes by arguing that these rules are lopsided and establish excessive delegation of power to the executive.

1.3. Research Statement:

The guidelines notified by the government poses a threat to the regulation of the intermediaries and the privacy of the public at large since the government can ask the intermediaries to take down any content and to trace a particular message. This violates the necessity and proportionality tests by the Supreme Court. Further, these guidelines are not product of any parliamentary process. The main focus of this paper is not against the complete absence of regulation but to determine whether the present guidelines are based on principles of constitutional morality.

1.4. Research question:

Based on the backdrop of the above research statement, the author proposes the following question-Whether the guidelines framed is an overuse of restrictions under Art. 19(2)?

1.5. Hypothesis:

The guidelines framed by the government infringe the golden triangle of articles 14,19 and 21 by violating the necessity and proportionality tests and are arbitrary and vague. They also attempt to overrule the judgment of the Supreme Court in Shreya Singhal's case.

1.6. Scope and objective:

The scope of this paper is limited to analyzing how the rules affect social media intermediaries such as WhatsApp, Twitter, Facebook, etc. and the content regulation of OTT platforms. The paper also studies the legality of these guidelines imposed and to check whether they are beyond the scope of reasonableness under Art. 19(2).

1.7. Methodology:

The paper is entirely based on doctrinal research method and secondary data resources. The primary source used is the IT guidelines of 2021 and the secondary sources used in the paper are articles, journals and scholarly websites.

2. How Encryption Systems Work And Traceability Mandate Is Not Helpful

In today's digital world, where almost everyone we come across have a smartphone and a social media account or use WhatsApp, the data stored in servers or any other electronic medium has grown exponentially. It will continue to do so. This phenomenon as triggered a lot of political discourse on privacy concerns and aspects. Encryption is the most common and perhaps the only way which protects data privacy. To simply put, it is the method by which an information is sort of coded and locked in a box and the key is rendered unintelligible to an unauthorized recipient but an authorized recipient of a message has the key to access the box and to decode the message into plain text.[1308] This protects the information or data from

[1308] Gulshan Rai, RK Dubash, & AK Chakravarty, 'Cryptography Technology and Policy Directions in the Context of NII' (1997) Information Technology Group, Department of Electronics Cyber law Series 3, Version 1 https://web.archive.org/web/19990506205823/http:/www.allindia.com:80/gov/doe/cryplaw.htm accessed on 13th December 2022

INDIAN JOURNAL OF LEGAL REVIEW [IJLR]
Volume 3 and Issue 1 of 2023
ISSN - 2583-2344 *(and)* ISBN - 978-81-961120-2-8
Published by
Institute of Legal Education
https://iledu.in

unauthorized access and preserves the authenticity of the data of the users. This method of encryption is used to protect both stored and transmitted data.[1309] The most common form of encryption which is used is the end-to-end encryption in short E2EE. This form makes sure that apart from the sender and the recipient, nobody else including the intermediary platform and the communication service provider can access the information.[1310] Under Indian laws, encryption is defined as - '[t]he process of transforming plaintext data into an unintelligible form (cypher text) such that the original data either cannot be recovered (one-way encryption) or cannot be recovered without using an inverse decryption process (two-way encryption).'[1311] However, there is no legislation for encryption alone. It is governed by the Rules made by the government under the IT Act of 2000. Presently, the New Intermediary Guidelines supersede the Information Technology (Intermediaries guidelines) Rules, 2011. These Guidelines are to be followed by the intermediaries and non-compliance of such would render them ineligible for protection under the IT Act's S. 79 which gives these platforms a safe harbor and exempts them from any liability for third party as long as the provisions of the section are fulfilled. Since, there is zero chance of interference of social media intermediaries under the E2EE system, they cannot interfere with the message and enjoy the power of S. 79. This is essential for users to express themselves freely and exercise the right guaranteed under Art. 19(1)(a). The traceability mandate provided by the 2021 guidelines under Rule 4(2) is applicable to any significant social media intermediary which the ethics code defines as SSMI[1312]. However, the guidelines are applicable even to those intermediaries which are not significant intermediaries[1313].

The main justification for bringing these codes are to curb anti-national elements[1314] and preventing fake news.[1315] However, undermining encryption is not a perfect or rational solution. the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has said, governments 'have not demonstrated that criminal or terrorist use of encryption serves as an insuperable barrier to law enforcement objectives'[1316]

2.1. Working of Encryption

Every alphabet and every message has a particular mathematical value or number.[1317] This in computer science language is called hashing. It is the same method used for password verification systems. The E2EE system also works on a similar mechanism but much more advanced and rigid. This example will be easy to understand this system: If A types and sends "Good Morning" to B, the message "Good Morning" will first be codified on the hash value. This message will be put in a locker and the key is available only to B. When B receives the message on the phone, the software automatically uses the key and unlocks the message which can be read only by the

[1309] Nate Lord, 'Data Protection: Data In Transit vs. Data At Rest' (*Digital Guardian*, 15 July 2019) https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest accessed on 13th December 2022

[1310] Saurabh Sharma, 'End-to-end Encryption: The Heart of Data Security in Today's DigitalWorld' (*Live Mint*, 5 December 2019) https://www.livemint.com/opinion/columns/endto-end-encryption-the-heart-of-data-security-in-today-s-digital-world-11575560730299.html

[1311] Information Technology (Certifying Authorities) Rules, 2000, sch V. Also see Neha Alawadhi, 'RS Panel Suggests Breaking Encryption to Curb Child Pornography Distribution' (*Business Standard,* 27 January 2020) https://www.business-standard.com/article/technology/rs-panel-suggests-breaking-encryption-to-curb-child-pornograhy-distribution-120012600705_1.html accessed 15th December 2022

[1312] New Intermediary Guidelines, rule 2(v).

[1313] New Intermediary Guidelines, rule 6

[1314] The term 'anti-national elements' mentioned in the press release accompanying the Draft IT rules has no legal definition. 'Draft IT rules issued for public consultation' (Ministry of Electronics & Information Technology, 24 December 2018) https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1557159

[1315] 'Government notifies Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021' (*Ministry of Information & Broadcasting*, 25 February 2021) https://www.pib.gov.in/PressReleseDetail.aspx?PRID=1700766 accessed on 4th December 2022

[1316] UNHRC 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (22 May 2015) A/HRC/29/32; Soumyarendra Barik, 'Encryption and Issues Related to Misinformation' (*Medianama*, 15 June 2020) https://www.medianama.com/2020/06/223-encryption-misinformation/> also see, 'Fact Sheet: Intermediaries and Encryption' (*Internet Society*, 2 June 2020) https://www.internetsociety.org/resources/doc/2020/fact-sheet-intermediaries-and-encryption/ accessed 13th December 2022.

[1317] Mehab Quresi, 'What is hashing & why does Indian govt want WhatsApp to use it?' (*The Quint*, 25 March 2021) https://www.thequint.com/tech-and-auto/what-are-hashes-and-why-does-india-wants-whatsapp-to-implement-them#:~:text=Hashing%20is%20a%20process%20where,be%20easily%20traced%20when%20needed.&text=The%20Indian%20government%20wants%20WhatsApp%20to%20implement%20traceability%20in%20its%20services accessed on 13 December 2022

INDIAN JOURNAL OF LEGAL REVIEW [IJLR]

Volume 3 and Issue 1 of 2023

ISSN - 2583-2344 *(and)* ISBN - 978-81-961120-2-8

Published by

Institute of Legal Education

https://iledu.in

recipient i.e. B. Under the end to end encryption, the intermediary has no access to the message. It only uses the key to unlock the message. The government's requirement is that the intermediaries must assigning an alpha-numeric hash value to every message sent and the intermediary must keep a library of such values, thereby making it easy for tracing a particular message.[1318] However, this is practically not possible as it is on the assumption that the message and its alphabets, spacing, etc. are the same and does not change. Even a small change like adding an extra dot or writing everything in small letters will make a different value from the first message. So it is difficult to identify the originator which the government intends to.

3. Violation of arts. 14, 19 and 21

'The poorest man may in his cottage, bid defiance to all the forces of the Crown. It may be frail, its roof may shake; the wind may blow through it; the storm may enter; the rain may enter, but the King of England may not enter; all his force dares not cross the threshold of the ruined tenement.' ~ William Pitt, (Prime Minister of UK in 1763), quoted by the US Supreme Court in *Miller v United States* 1958 SCC OnLine US SC 131

These IT Rules 2021 do not comply with the Puttaswamy judgment of the Supreme Court and other previous judgments on fundamental rights. The Rules appear to overuse the provisions of reasonable restrictions under Art. 19(2). This will have a direct chilling effect on free speech and expression. Due to its negative aspect on the right to privacy (which is established as a fundamental right), the traceability mandate of the IT Rules 2021, must satisfy the tests of proportionality and necessity as laid down by the Supreme Court in K.S. Puttaswamy v Union of India[1319]. Nine judges of the Court unanimously held that "right to privacy is protected as an intrinsic part of right to life and personal liberty under Art. 21 and as a part of freedoms guaranteed by Part III". The proportionality and necessity tests requires four things[1320]:

1. The said action should have a statutory backing or must be backed up by a law.
2. The proposed action should be necessary for a 'legitimate' aim.
3. The extent of interference must be proportionate to the need of such interference.
4. There should be procedural safeguards against abuse.

It is also essential that the chosen measure must be one that is effective and least intrusive. Furthermore, when the said action infringes fundamental rights, it is also mandatory to show that there is no other equally effective method available to tackle the problem. The traceability mandate is disproportionate in these above mentioned aspects as it threatens to infringe the right to privacy. This has a ripple effect on the freedom of speech and expression as one cannot utilize their right to propagate and exchange ideas. It is the duty of the Courts and not the executive to decide if any action taken by the government is right or wrong. In ***Mirzapur Moti Jamat case***[1321] *it was held* that to satisfy the test of reasonable restriction, while imposing a total prohibition on the slaughter of bull and bullocks, it must be proved that a lesser alternative would be inadequate. In the case of ***Akhil Bharatiya Soshit Karmachari Sangh* v. *Union of India***[1322], the Supreme Court held that the reasonableness of restrictions imposed by the Statute is required to be independently examined. Further in the case of ***Pathumma* v. *State of Kerala***[1323] it was held by Apex Court that the directives principles of the State policy ***per se*** can never negate the requirements of Part III. It is equally important for the State of Mahadpur to show the

[1318] Surabhi Agarwal, 'Govt Proposes Alpha-Numeric Hash to Track WhatsApp Chat' (*ET CIO*, 23 March 2021) available at: https://cio.economictimes.indiatimes.com/news/social-media/govt-proposes-alpha-numeric-hash-to-track-whatsapp-chat/81643144 accessed 3rd December 2022.

[1319] K.S. Puttaswamy v Union of India (2017) 10 SCC 1

[1320] K.S. Puttaswamy v Union of India (2017) 10 SCC 1 para 71, SK Kaul J.

[1321] State of Gujarat v. Mirzapur Moti Kureshi Kassab Jamat, (2005) 8 SCC 534

[1322] 1981 AIR 298

[1323] 1978 SCR (2) 537

INDIAN JOURNAL OF LEGAL REVIEW [IJLR]
Volume 3 and Issue 1 of 2023
ISSN - 2583-2344 *(and)* ISBN - 978-81-961120-2-8
Published by
Institute of Legal Education
https://iledu.in

proportionality test as well which the State has not. As held in ***Anuj Garg v. Hotel Association of India***[1324], if a law discriminates on any of the prohibited grounds, it needs to be tested not merely against "reasonableness" under Article 14 but be subject to "strict scrutiny".

In the absence of proportionality and any demonstration as to how the interference is 'relevant and sufficient,' the traceability proposal fails to fulfil the 'necessary in a democratic society' limb of the test laid down by the Supreme Court. Furthermore, there are no procedural safeguards against abuse of the traceability mandate. This is also violating the principles of natural justice. This also violates Art. 14. As mentioned earlier in the case of ***Anuj Garg v. Hotel Association of India***[1325], if a law discriminates on any of the prohibited grounds, it needs to be tested not merely against "reasonableness" under Article 14 but be subject to "strict scrutiny". In considering reasonableness from the point of view of Article 14, the Court has also to consider the objective for such classification. If the objective be illogical, unfair and unjust, necessarily the classification will have to be held as unreasonable.[1326] In the case of ***Akhil Bharatiya Soshit Karmachari Sangh*** **v.** ***Union of India***[1327], the Supreme Court held that the reasonableness of restrictions imposed by the Statute is required to be independently examined.

4. Conclusion

The provisions of the IT Rules, 2021 are not passed by any parliamentary process but rather plain executive orders under section 87(2) of the IT Act, 2000. The Rules are violative of the Puttaswamy judgment and other judgments of the Supreme Court and have a chilling effect on free speech. Although the reason for bringing in these is to make sure the intermediaries do not function as per the whims and fancies of their algorithms like how Trump was suspended from twitter and to tackle the problems of fake news, defamatory and seditious content. However, all of these have to be proved or at least demonstrated by the government as per the Puttaswamy judgment. Without which, all these reasons are nothing but strong a rhetoric. Also undermining encryption is not a feasible solution as the law enforcement agencies have not expressed or established that the encryption mechanism is being misused. Therefore, to sum it up, these IT Rules of 2021 are not constitutionally justified.

References

1. Bhandari, V., & Sane, R. (2018). Protecting Citizens From The State: Analysing the Impact post Puttaswamy and Implications of Justice Srikrishna Committee. Socio-Legal Review, 44.
2. Karnik, N. (2021). Analysis of Intermediary Guidelines and Digital Media Ethics Code, 2021. International Journal of Law Management & Humanities, 4(4), 1155-1168.
3. Maheshwari, N., & Nojeim, G. (2021). Encryption in India: Preserving The Online Engine of Privacy, Free Expression and Security. The Indian Journal Of Law And Technology, 17, 1-44.
4. Sharma, M., & Pendtal, K. (2021). IT Rules 2021: Protection From Malicious Content or Chilling Free Speech. Centre for Research in Finance, Technology, and Law. Retrieved from https://ssrn.com/abstract=3967857
5. Siripurapu, A., & Merrow, W. (2021). Social Media and Online Speech: How Should Countries Regulate Tech Giants? Council on Foreign Relations. Retrieved from https://www.jstor.org/stable/resrep31160
6. Gulshan Rai, RK Dubash, & AK Chakravarty, 'Cryptography Technology and Policy Directions in the Context of NII' (1997) Information Technology Group, Department of Electronics Cyber law Series 3, Version 1 https://web.archive.org/web/19990506205823/http:/www.allindia.com:80/gov/doe/cryplaw.htm accessed on 13th December 2022
7. Nate Lord, 'Data Protection: Data In Transit vs. Data At Rest' (Digital Guardian, 15 July 2019) https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest accessed on 13th December 2022

[1324] AIR 2008 SC 663.
[1325] AIR 2008 SC 663.
[1326] Ibid. Also held in *Deepak Sibal* v. *Punjab University*, AIR 1989 SC 903.
[1327] Refer to supra note 26.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR]

Volume 3 and Issue 1 of 2023

ISSN - 2583-2344 *(and)* ISBN - 978-81-961120-2-8

Published by

Institute of Legal Education

https://iledu.in

8. Saurabh Sharma, 'End-to-end Encryption: The Heart of Data Security in Today's DigitalWorld' (Live Mint, 5 December 2019) https://www.livemint.com/opinion/columns/end-to-end-encryption-the-heart-of-data-security-in-today-s-digital-world-11575560730299.html

9. Information Technology (Certifying Authorities) Rules, 2000, sch V. Also see Neha Alawadhi, 'RS Panel Suggests Breaking Encryption to Curb Child Pornography Distribution' (Business Standard, 27 January 2020)

10. https://www.business-standard.com/article/technology/rs-panel-suggests-breaking-encryption-to-curb-child-pornograhy-distribution-120012600705_1.html accessed 15th December 2022

11. 'Draft IT rules issued for public consultation' (Ministry of Electronics & Information Technology, 24 December 2018) https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1557159

12. 'Government notifies Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021' (Ministry of Information & Broadcasting, 25 February 2021) https://www.pib.gov.in/PressReleseDetail.aspx?PRID=1700766 accessed on 4th December 2022

13. UNHRC 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (22 May 2015) A/HRC/29/32; Soumyarendra Barik, 'Encryption and Issues Related to Misinformation' (Medianama, 15 June 2020)

14. https://www.medianama.com/2020/06/223-encryption-misinformation/> also see, 'Fact Sheet: Intermediaries and Encryption' (Internet Society, 2 June 2020) https://www.internetsociety.org/resources/doc/2020/fact-sheet-intermediaries-and-encryption/ accessed 13th December 2022.

15. Mehab Quresi, 'What is hashing & why does Indian govt want WhatsApp to use it?' (The Quint, 25 March 2021) https://www.thequint.com/tech-and-auto/what-are-hashes-and-why-does-india-wants-whatsapp-to-implement-them#:~:text=Hashing%20is%20a%20process%20where,be%20easily%20traced%20when%20needed.&text=The%20Indian%20government%20wants%20WhatsApp%20to%20implement%20traceability%20in%20its%20services. accessed 13 December 2022

16. Surabhi Agarwal, 'Govt Proposes Alpha-Numeric Hash to Track WhatsApp Chat' (ET CIO, 23 March 2021) available at: https://cio.economictimes.indiatimes.com/news/social-media/govt-proposes-alpha-numeric-hash-to-track-whatsapp-chat/81643144 accessed 3rd December 2022.