THE MINISTRY AND THE TRACE: SUBVERTING END-TO-END ENCRYPTION

Gurshabad Grover, Tanaya Rajwade & Divyank Katira[*]

End-to-end encrypted messaging allows individuals to hold confidential conversations free from the interference of states and private corporations. To aid surveillance and prosecution of crimes, the Indian Government has mandated online messaging providers to enable identification of originators of messages that traverse their platforms. This paper establishes how the different ways in which this 'traceability' mandate can be implemented (dropping end-to-end encryption, hashing messages, and attaching originator information to messages) come with serious costs to usability, security and privacy. Through a legal and constitutional analysis, we contend that traceability exceeds the scope of delegated legislation under the Information Technology Act, and is at odds with the fundamental right to privacy.

TABLE OF CONTENTS

[*]Gurshabad Grover <gurshabad@cis-india.org> is a technologist and legal researcher at the Centre for Internet and Society (CIS). Tanaya Rajwade is a graduate of the National Law University Delhi and is currently a legal advisor at a London-based law firm; she was formerly Policy Officer at CIS. Divyank Katira is a technology researcher at CIS. The authors are grateful to Elonnai Hickok and the anonymous reviewers for their constructive comments and suggestions, and to Shubhika Saluja, Kanav Khanna, Abhay Bhandari and Raghav Ahooja for their assistance. Opinions and inaccuracies in this document remain the authors' alone. Disclosure: This work was supported by a research grant to CIS from Facebook India, and the John D. and Catherine T. MacArthur Foundation.

I. INTRODUCTION

Since the beginning of the crypto wars in the 1990s, many jurisdictions have been concerned with citizens' use of strong encryption for private communications and the consequent impediments for information collection by law enforcement agencies. In recent years, particular attention has been paid to end-to-end encrypted ('E2EE') messaging.[1] This form of cryptography allows messages only to be read by senders and their intended recipients. Content shared by users over E2EE channels is inaccessible to even the service providers.

Thus, E2EE can provide individuals with a "zone of privacy" where they can hold opinions and exercise freedom of expression without interference from states or private corporations.[2] This can be particularly important in authoritarian states, where it is critical for journalists, researchers, lawyers, those from gender and sexual minorities, and civil society to have an avenue for communication that is free of surveillance and harassment.[3] With private communications increasingly moving online, the absence of such protections would grant states unprecedented surveillance capabilities, a threat only accentuated in authoritarian states and even ones with weak procedural safeguards.

On the other end of the spectrum are claims of law enforcement and intelligence agencies. Such agencies often rely on gathering personal data stored by online services to investigate or prosecute crime.[4] They claim that E2EE systems preclude them from accessing electronic evidence that may be necessary to investigate and prosecute serious crimes.[5]

In a bid to remove barriers to accessing user data, some governments have attempted to prohibit E2EE.[6] Governments have also tried, apart from legal impositions, to advocate against E2EE. In the past few years, the Five Eyes have demanded law enforcement access to encrypted information,[7] and the US, UK and Australian governments have been

---

[1] HOOVER INSTITUTION, *The International Legal Dynamics Of Encryption* (October 2016), available at https://www.hoover.org/research/international-legal-dynamics-encryption (Last visited on June 21, 2021).

[2] Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Report on encryption, anonymity, and the human rights framework*, ¶12, A/HRC/29/32, (May 22, 2015).

[3] *Id*.

[4] Rishab Bailey, et al., , *Use of personal data by intelligence agencies and law enforcement agencies*, August 7, 2019, DATA GOVERNANCE NETWORK, available at https://www.datagovernance.org/files/research/BBPR2018-Use-of-personal-data.pdf (Last visited on April 6, 2021).

[5] Federal Bureau of Investigation, *The Lawful Access Challenge*, available at https://www.fbi.gov/about/leadership-and-structure/science-and-technology-branch/lawful-access (Last visited on April 6, 2021).

[6] E.g., China has effectively banned end-to-end encryption by restricting foreign companies that offer such services; and Chinese companies do not offer E2EE either. The Prime Minister of the United Kingdom pledged in 2015 to seek a ban on E2EE. *See* Lorand Laskai & Adam Segal, *The Encryption Debate in China*, May 30, 2019, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE, available at https://carnegieendowment.org/2019/05/30/encryption-debate-in-china-pub-79216 (Last visited on April 6, 2021); INDEPENDENT (Andrew Griffin), *WhatsApp and iMessage could be banned under new surveillance plans*, January 12, 2015, available at https://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-and-snapchat-could-be-banned-under-new-surveillance-plans-9973035.html (Last visited on April 6, 2021).

[7] Susan Landau, *The Five Eyes Statement on Encryption: Things Are Seldom What They Seem*, September 26, 2018, LAWFARE, available at https://www.lawfareblog.com/five-eyes-statement-encryption-things-are-seldom-what-they-seem (Last visited on April 6, 2021).

advocating against the deployment of E2EE on Facebook's platforms.[8] India is no exception: the Government released a draft National Encryption Policy in 2015 that placed stringent obligations on services offering encrypted communications, and required them to store unencrypted information to be shared with the Government on request.[9] While the draft Policy was later withdrawn, the Government's efforts to curtail strong encryption in India have continued.[10] In October 2020, India joined the Five Eyes (Australia, Canada, New Zealand, the United Kingdom, and the United States) in issuing a statement on the challenges posed by E2EE to law enforcement functions, and urged industry to collaborate with governments to reach "mutually agreeable solutions."[11]

The most recent move by the Indian government that threatens the use of E2EE comes in the form of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ('2021 Rules').[12] The 2021 Rules have received criticism for placing extensive obligations on intermediaries that threaten freedom of expression,[13] and creating a regulatory framework for online curated-content platforms and digital news publishers without such legal powers in the IT Act.[14] This paper specifically focuses on Rule 4(2), which mandates popular messaging services to facilitate the identification of the 'first originator' of any message that is sent through their platforms in response to a lawful court or government order,[15] a rule commonly referred to as 'traceability'. While the language of the rule suggests that the Government does not want to ban or 'break' end-to-end encryption,[16] commentators have

[8] THE GUARDIAN (Julia Carrie Wong), *US, UK and Australia urge Facebook to create backdoor access to encrypted messages*, October 4, 2019, available at https://www.theguardian.com/technology/2019/oct/03/facebook-surveillance-us-uk-australia-backdoor-encryption (Last visited on April 6, 2021).

[9] Bhairav Acharya, *The Short-lived Adventure of India's Encryption Policy*, November 27, 2015, CENTRE FOR INTERNET AND SOCIETY, available at https://cis-india.org/internet-governance/blog/the-short-lived-adventure-of-india2019s-encryption-policy (Last visited on June 21, 2021).

[10] Bedavyasa Mohanty, *The Encryption Debate in India*, May 30, 2019, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE available at https://carnegieendowment.org/2019/05/30/encryption-debate-in-india-pub-79213 (Last visited on June 21, 2021).

[11] Office of Public Affairs, *'International Statement: End-To-End Encryption and Public Safety'*, THE UNITED STATES DEPARTMENT OF JUSTICE, October 11, 2020, available at https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety (Last visited on June 21, 2021).

[12] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

[13] SOFTWARE FREEDOM LAW CENTRE INDIA, *Analysis Of The Information Technology (Intermediary Guidelines And Digital Media Ethics Code) Rules, 2021*, February 27, 2021, available at https://sflc.in/analysis-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021 (Last visited on June 21, 2021).

[14] INTERNET FREEDOM FOUNDATION, *Deep dive : How the intermediaries rules are anti-democratic and unconstitutional.*, February 27, 2021, available at https://internetfreedom.in/intermediaries-rules-2021/ (Last visited on June 21, 2021).

[15] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 4(2).

[16] *Id*. (Provided also that in complying with an order for identification of the first originator, no significant social media intermediary shall be required to disclose the contents of any electronic message [...]).

suggested that traceability will end up doing so anyway.[17] At the very least, there are clear privacy-related implications of the requirement that demand closer scrutiny.[18]

This paper examines the traceability requirement, its legality and constitutionality, and its implications for the privacy and security inherent in E2EE. Part II of this paper covers the background of how traceability has been discussed across the executive, judiciary and the legislature. We briefly cover the legislative history of the traceability mandate and summarise the rule as it appears in the 2021 Rules. We also discuss the developments in a public interest litigation case, originally filed in the Madras High Court, that led to technical deliberations on how messages can be traced to their origin. We additionally look at traceability as it appears in the report of the Rajya Sabha Ad-hoc Committee that was set up in 2019 to look into issues surrounding child sexual abuse material online.

In Part III, we list and discuss the different possible ways in which messaging platforms could implement the traceability requirement. We examine the effects of each proposal, focusing on the implications for the security and privacy guarantees expected from E2EE.

Given this understanding of the effects and implications of the rule, we critically examine the legality and constitutionality of the rule in Part IV. We argue that introducing the requirement through executive notification exceeds the scope of what is permitted under delegated legislation. We also contend that the rule may not stand up to constitutional scrutiny, given the Supreme Court's 2017 decision in Justice *K. S. Puttaswamy (Retd.) and Anr.* v. *Union of India And Ors.* ('Puttaswamy'), which affirmed the fundamental right to privacy guaranteed to all Indian citizens. We conclude, in Part V, by suggesting alternative legal and policy reforms that can be pursued to help resolve some of the issues that law enforcement agencies face.

II. BACKGROUND

A. LEGISLATIVE HISTORY AND THE RULE

The growth of the internet industry has been facilitated by legal frameworks that allow online platforms to carry out their functions without attracting liability for third-party content.[19] In India, the Information Technology Act, 2000 ('IT Act') creates such a framework for online intermediaries. An intermediary is defined as a "person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record."[20] Providers of such internet services are exempted from liability for third-party content that they

[17] Aditi Agrawal, *Traceability and end-to-end encryption cannot co-exist on digital messaging platforms: Experts*, March 15, 2021, FORBES INDIA, available at https://www.forbesindia.com/article/take-one-big-story-of-the-day/traceability-and-endtoend-encryption-cannot-coexist-on-digital-messaging-platforms-experts/66969/1 (Last visited on April 6, 2021); WHATSAPP, *What is traceability and why does WhatsApp oppose it?*, available at https://faq.whatsapp.com/general/security-and-privacy/what-is-traceability-and-why-does-whatsapp-oppose-it/?lang=en (Last visited on June 21, 2021).

[18] Yashovardhan Azad, *'Will the new IT rules imperil data privacy?'*, March 11, 2021, THE HINDU BUSINESSLINE, available at https://www.thehindubusinessline.com/opinion/will-the-new-it-rules-imperil-data-privacy/article34046165.ece (Last visited on June 21, 2021).

[19] Anupam Chander, *How Law Made Silicon Valley*, Vol. 63(3) EMORY LAW J. 639 (2014).

[20] Information Technology Act, 2000, § 2(w).

process, provided they do not modify or initiate transmissions and comply with content blocking orders and the due diligence guidelines notified under §79 of the IT Act.[21]

In July 2018, the Minister of Electronics and Information Technology proposed amending the guidelines to address the "misuse of social media platforms to spread rumours and fake news" in response to a rise in violent incidents and lynchings.[22] Subsequently, in December 2018, the Ministry of Electronics and Information Technology ('MeitY') circulated the draft Intermediary Guidelines (Amendment) Rules ('Draft Rules'),[23] and invited comments from stakeholders.[24] The Draft Rules included a traceability requirement, under which intermediaries would have to enable "tracing out" of content creators on their platform in response to governmental information requests.[25] After the draft rule faced criticism for its vagueness and potential harms to privacy and freedom of expression,[26] it was changed significantly and specified in more detail when formally notified in the 2021 Rules.[27]

The traceability requirement as it appears in the 2021 Rules is applicable to popular social media intermediaries that primarily provide messaging services.[28] These services are

[21] Information Technology Act, 2000, § 79.

[22] RAJYA SABHA DEBATE, *Calling Attention To Matter Of Urgent Public Importance: The misuse of social media platforms to spread rumours and fake news leading to rising incidents of violence and lynching in the country*, 171, July 26, 2018, available at https://rsdebate.nic.in/bitstream/123456789/684107/2/PD_246_26072018_p455_p485_32.pdf (Last visited on April 6, 2020).

[23] The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 (Draft Rules).

[24] MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, *Comments Invited on Draft of Intermediary Guideline*s, *2018*, December 27, 2018, available at https://meity.gov.in/comments-invited-draft-intermediary-rules (Last visited on April 6, 2020).

[25] The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018, Rule 3(5).

[26] MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, *Public Comments on Draft Intermediary Guidelines Rules, 2018*, ¶41-42 (Asia Internet Coalition), ¶101 (Amnesty International), ¶115 (CCAOI), ¶114 (Asia Cloud Computing Association), ¶189 (IAMAI), ¶195 (CII), ¶200 (Article 19), ¶221 (Internet Freedom Foundation), ¶257 (Centre for Internet and Society), ¶290 (NIPFP), ¶318 (SFLC.in), ¶374 (Free Software Movement of India), ¶384 (Mozilla), ¶487-488 (CCG, NLUD), available at https://meity.gov.in/writereaddata/files/public_comments_draft_intermediary_guidelines_rules_2018.pdf (Last visited on June 21, 2021); *Addendum to comments*, ¶25 (The Dialogue), ¶45-46 (ASSOCHAM), ¶68 (Global Network Initiative), ¶82 (Medianama), available at https://meity.gov.in/writereaddata/files/Addendum1_Public_comments_on_draft_intermediary_guidelines.pdf (Last visited on June 21, 2021); Mishi Choudhary & Eben Moglen, *Protect right to privacy: Petition to make social media traceable strips the privacy right of all meaning*, January 24, 2021, TIMES OF INDIA, available at https://timesofindia.indiatimes.com/blogs/toi-edit-page/protect-right-to-privacy-petition-to-make-social-media-traceable-strips-the-privacy-right-of-all-meaning/ (Last visited on April 6, 2020); Vrinda Bhandari, *Opinion | Draft IT rules will have a serious impact on the privacy of citizens*, November 27, 2019, LIVEMINT available at https://www.livemint.com/opinion/online-views/opinion-draft-it-rules-will-have-a-serious-impact-on-the-privacy-of-citizens-11574814696619.html (Last visited on April 6, 2020); Rahul Mathhan, *Opinion | End-to-end encryption must be retained at all cost*, August 27, 2019, LIVEMINT, available at https://www.livemint.com/opinion/online-views/opinion-end-to-end-encryption-must-be-retained-at-all-cost-1566926664869.html (Last visited on April 6, 2020).

[27] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 4(2).

[28] It is applicable to social media intermediaries providing messaging services, with more than 50 lakh users in India, where social media intermediaries are defined as "an intermediary which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services." *See* Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 2(w); MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, Notification No. 869, February 26, 2021, available at http://egazette.nic.in/WriteReadData/2021/225497.pdf (Last visited on April 6, 2020).

obligated to "enable the identification of the first originator" of information when required by a judicial order or an order under §69 of the IT Act, which empowers certain agencies to send interception and decryption requests to intermediaries.[29]

Such orders must be for investigation or prevention of crimes related to: (1) national security and sovereignty, public order or friendly relations with foreign states; or (2) rape, sexually explicit material or child sexual abuse material if they have an associated jail sentence of more than five years. The rules state that an order of traceability will only be passed if there are no less intrusive alternatives available to the Government. The rule clarifies that intermediaries will not be compelled to reveal the contents of the message. Additionally, intermediaries are required to identify the first originator 'in Indian territory'.

B. OTHER DEVELOPMENTS

Aside these, it is also crucial to discuss two other developments that informed the Ministry's decision on traceability.

The first relates to a petition filed in the Madras High Court in 2019. The original plea in the public interest litigation sought the linking of social media accounts with "government-authorised identity proof."[30] The court ruled this possibility out on account of such a decision being inconsistent with earlier apex court decisions.[31] However, in the course of discussions around legal tools to combat cybercrime, the State of Tamil Nadu brought the Court's attention to the Draft Rules, which diverted the proceedings to the feasibility of implementing traceability on E2EE messaging services.[32]

The Court sought inputs from experts into the technological viability of tracing the originators of messages (or traceability) on WhatsApp.[33] Prof. V. Kamakoti submitted a proposal claiming that traceability was possible without breaking encryption, which then rebutted by WhatsApp[34] and commentators.[35] The Madras High Court petition, along with petitions before

[29] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 4(2).

[30] J Pathiban v. The Superintendent of Police and Ors W.P. No. 20774/2018 and 20214/2018 Madras High Court; Ezhilarasi v. State, H.C.P.(MD) No. 905 of 2018 Madras High Court.

[31] *See* K S Puttaswamy and Ors. v Union of India (2019) 1 SCC 1, ¶219(e), which circumscribed the use of Aadhaar.

[32] Anthony Clement Rubin v. Union of India, WP 20774 of 2018; Janani Krishnamurthy v. Union of India, WP 20214 of 2018.; MEDIANAMA (Aditi Agrawal), *WhatsApp to Madras HC: Impossible to track the sender of a message because of encryption*, June 10, 2019, available at https://www.medianama.com/2019/06/223-whatsapp-to-madras-hc-impossible-to-track-the-sender-of-a-message-because-of-encryption/ (Last visited on June 21, 2021)

[33] MEDIANAMA (Aditi Agrawal), *Tell us if traceability is technically possible: Madras HC to WhatsApp and IIT Madras professor*, August 1, 2019, available at https://www.medianama.com/2019/08/223-tell-us-if-traceability-is-technically-possible-madras-hc-to-whatsapp-and-iit-madras-professor/ (Last visited on April 10, 2020).

[34] MEDIANAMA (Aditi Agrawal), *Exclusive: WhatsApp's response to Dr Kamakoti's submission*, August 21, 2019, available at https://www.medianama.com/2019/08/223-exclusive-whatsapps-response-kamakotis-submission/ (Last visited on April 6, 2020).

[35] Anand Venkatnarayanan, *Dr Kamakoti's solution for WhatsApp traceability without breaking encryption is erroneous and not feasible*, August 13, 2019, MEDIANAMA, available at https://www.medianama.com/2019/08/223-kamakoti-solution-for-traceability-whatsapp-encryption-madras-anand-venkatanarayanan/ (Last visited on April 6, 2020); ECONOMIC TIMES (Megha Mandavia), *Digital rights body IFF files IIT-B Prof submission saying traceability on whatsapp vulnerable to falsification*, August 25, 2019, available at https://economictimes.indiatimes.com/tech/internet/digital-rights-body-iff-files-iit-b-prof-submission-saying-traceability-on-whatsapp-vulnerable-to-falsification/articleshow/70826842.cms?from=mdr (Last visited on April 6, 2020).

other courts that asked for linking of government identification with social media accounts,[36] is pending before the Supreme Court.[37]

The proposal by Prof. Kamakoti on how to achieve traceability on end-to-end encrypted messaging platforms is discussed in detail in part III of this article.

The second development came from the legislature. In December 2019, the Rajya Sabha created an *ad hoc* committee to tackle the growing problem of child sexual abuse material (CSAM) on social media.[38] Its final report recommended amending the Intermediary Guidelines "to include the ability to trace the originator or sender of the message shared on end-to-end encryption platforms in cases where [CSAM] has come to the attention of law enforcement agencies."[39] The report recommended permitting the "breaking of end-to-end encryption to trace distributors of child pornography."[40]

While both developments speak to traceability, it is important to carve out a distinction. The technical proposals presented before the Madras High Court explicitly stopped short of requiring intermediaries to break E2EE,[41] whereas the Rajya Sabha *ad hoc* Committee had no such qualms. The Committee also made no comment on whether it was technically feasible at all to break the security guarantees in certain circumstances. The report was cited as a reason for the traceability requirement appearing in the 2021 Rules.[42]

III. WAYS TO IMPLEMENT TRACEABILITY AND THEIR IMPLICATIONS

Secure online messaging solutions have evolved over time to provide a number of security and privacy guarantees to their users, the culmination of which is a mechanism known as end-to-end encrypted messaging.[43] In addition to providing encryption in transit, which keeps messages secure as they travel over the publicly shared Internet, end-to-end encrypted messaging also precludes messaging service providers — who mediate the exchange of messages — from reading the contents of these private communications.[44] This mechanism of making communications readable only at the ends of the conversation, and not storing them en masse on a centralised server, significantly increases the difficulty of mass surveillance. Communication

[36] MEDIANAMA (Aditi Agrawal), *Facebook transfer petition: Whatsapp, Facebook submit list of related cases to SC*, November 5, 2019, available at https://www.medianama.com/2019/11/223-facebook-whatsapp-related-cases/ (Last visited on April 6, 2020).
[37] Facebook Inc v. Union of India, (2019) SCC OnLine SC 1717.
[38] Adhoc Committee of the Rajya Sabha, *Report of the Adhoc Committee of the Rajya Sabha to Study the Alarming Issue of Pornography on Social Media and its Effect on Children and Society as a Whole* (January 25, 2020).
[39] *Id*., at ¶2.2.
[40] *Id*.
[41] MEDIANAMA (Aditi Agrawal & Nikhil Pahwa), *IIT Madras's Kamakoti tells MediaNama how WhatsApp traceability is possible without undermining end-to-end encryption*, August 8, 2019, available at https://www.medianama.com/2019/08/223-kamakoti-medianama-whatsapp-traceability-interview/ (Last visited on April 10, 2020).
[42] Press Release, MINISTRY OF ELECTRONICS & IT, *Government notifies Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021*, February 25, 2021, available at https://pib.gov.in/Pressreleaseshare.aspx?PRID=1700749 (Last visited on April 10, 2020).
[43] Kseniia Ermoshina et al., *End-to-end encrypted messaging protocols: An overview.* INTERNATIONAL CONFERENCE ON INTERNET SCIENCE (January 5, 2017).
[44] Id.; Katriel Cohn-Gordon et al., A formal security analysis of the signal messaging protocol, Vol. 33(4) J. Cryptol. 1914-1983 (2020).

security and privacy are maintained even in the face of compromise of the server infrastructure of the messaging service provider.

Put formally, secure messaging solutions offer the following security and privacy properties:[45]

- *Confidentiality*: No entity other than the sender and recipient can read the contents of a message.
- *Integrity*: No entity can modify the contents of a message in transit.
- *Authentication*: A message recipient can verify that the message came from the 'claimed' source. However, since messaging services adopt weak identification mechanisms, such as phone numbers, to identify their users, the claimed source may not correspond to the real author of a message. This limitation is detailed below.
- *Deniability, Forward and Future Secrecy*: Deniability ensures that anyone with a record of the transcript, including message recipients, cannot 'cryptographically' prove to others that a particular participant of a communication authored the message.[46] Forward and Future Secrecy relate to protecting the confidentiality of messages sent before and after the compromise of an end-user device. A detailed explanation of these properties is omitted here as we do not make use of them in our analysis.

The wording of Rule 4(2) of the 2021 Rules, which introduces the traceability mandate, suggests that it applies in cases where the Government already has access to the contents of a message and only wants the ability to find its 'first originator'. For end-to-end encrypted messages, the contents can only be found by either gaining access to one of the end-user devices participating in a communication or through a recipient of a message disclosing it to law enforcement. In the absence of a definition of first originator, we presume it is the very first individual to introduce a particular message to a platform — we call this the "absolute originator". However, there is also the possibility of multiple originators i.e., people who independently sent the same message, leading to multiple, disparate chains of forwarded messages, each leading back to a different originator — which we refer to as 'relative originators'.[47]

The traceability requirement mandates identification of the first originator without specifying how this may be technically implemented. This leaves room for messaging service providers to pick a method of their choice. In this section, we describe the various methods being proposed to allow traceability in messaging services, including hashing each message and tagging each message with the originator's information. We explore their utility and drawbacks, and discuss the tradeoffs of each choice on the privacy and security of users of these services.

[45] Nik Unger et al., *SoK: secure messaging*, 2015 IEEE Symposium on Security and Privacy (2015) ¶10.
[46] Mallory Knodel et al., *Definition of End-to-end Encryption* ¶3.1.2 (Internet Engineering Task Force, Internet-Draft Working Document 2021) available at https://datatracker.ietf.org/doc/draft-knodel-e2ee-definition/ (Last visited on June 21, 2021).
[47] This terminology was used by a participant in a discussion on the 2021 Rules organised by the Center for Democracy and Technology (CDT). The discussion was held on March 3, 2021 under the Chatham House Rule.

A. DO NOTHING, OR NOT IMPLEMENT E2EE

There exists a plethora of messaging services that do not use E2EE.[48] If the intermediaries operating such services store and have access to the plaintext of all communications sent over their channels, then it is straightforward for them to identify the absolute originator of content. These organisations can simply perform a search for the content in their message data store, and find all the instances of the content on their platform. All relative originators as well as the absolute originator can also be similarly identified.

This design and ability thus present an easy solution for companies that, on the other hand, have deployed E2EE. Technically, the simplest way for them to comply with the traceability mandate would be to change their product and remove E2EE entirely. While this is not mandated by the rule, it is important to note the indirect regulatory consequences of the traceability rule. Current free and open-source implementations of E2EE messaging,[49] and even ongoing efforts to devise open standards[50] for the same do not support traceability of any form out of the box. Thus, overall, the traceability rule can greatly disincentivise companies from deploying secure E2EE.

This method would have a deleterious effect on both security and privacy of communications. Breaking the confidentiality guarantee and making the contents of all messages of all users visible to messaging providers opens up the possibility of employees and contractors of the service provider gaining unauthorised access to private communications of individuals, and creates a large central cache of extremely sensitive information which would be a lucrative target for bad actors.[51]

B. STORE 'HASHES' OF ALL MESSAGES

Hashing is a mathematical operation that converts any piece of information, such as the contents of this paper or a movie, into a short, unique string of characters that is hard to guess. It is a one-way operation, i.e., it is generally considered computationally infeasible to retrieve the original piece of information from its hash.[52]

Following the notification of the 2021 Rules, government officials have suggested that service providers may comply with the traceability mandate by having their applications compute hashes of all the messages sent on their platforms prior to encryption on the end-user

[48] Two such popular services are direct messages on Facebook and Twitter. *See* Gennnie Gebhart & Kurt Opsahl, *After This Week's Hack, It Is Past Time for Twitter to End-to-End. Electronic Frontier Foundation*, ELECTRONIC FRONTIER FOUNDATION, July 17, 2020, available at https://www.eff.org/deeplinks/2020/07/after-weeks-hack-it-past-time-twitter-end-end-encrypt-direct-messages (Last visited on June 21, 2021); Andy Greenberg, *Facebook Says Encrypting Messenger by Default Will Take Years.*, WIRED, January 10, 2020, available at https://www.wired.com/story/facebook-messenger-end-to-end-encryption-default/ (Last visited on June 21, 2021).

[49] SIGNAL, *Technical information: Specifications and software libraries for developers*, available at https://signal.org/docs/ (Last visited on March 24, 2021).

[50] Datatracker, *Messaging Layer Security (mls)*, INTERNET ENGINEERING TASK FORCE, available at https://datatracker.ietf.org/wg/mls/about/ (Last visited on March 24, 2021).

[51] GEBHART, *supra* note 48.

[52] Bart Preneel, *Cryptographic hash functions.*, Vol. 5(4) EUR. TRANS. TELECOMMUN. 431 (1994).

device.[53] Service providers will retain the hash of each transmitted message on their servers. In case of a lawful request to find the originator of a particular message, service providers can compute the hash of that message and compare it to all previously recorded hashes. This will allow them to identify all relative originators of the message, as well as the absolute originator and everyone else who sent or forwarded a particular message.

However, this method has two flaws. Firstly, it trusts the end-user device to truthfully calculate the hash of the message prior to encryption. Since this device is under the control of the individual, the messaging application running on it can be easily modified by a motivated individual to attach an incorrect hash.[54] Because the service provider only sees the encrypted version and not the contents of the message, it has no way of verifying the hash. This makes this mechanism easy to circumvent for the motivated bad actors it is intended to catch.

Secondly, storing hashes of all messages on the service provider's infrastructure seriously undermines the expected confidentiality of messages. Hashing is not equivalent to encryption, and it is possible for a resourceful actor to guess the contents of a message from its hash. A simple example of this is a message that reads "Good Morning", which is a commonly used phrase. Anyone could calculate the hash of this message, and if they had access to the large database of hashes of all messages this method requires service providers to store, they could identify everyone who has sent that exact message.

This can create new avenues for mass surveillance, profiling and censorship. Since a hash is essentially a unique fingerprint of a message, a database of hashes of all messages can be used to identify everyone who has shared particular content. By identifying relative and absolute originators, and everyone else who sent or forwarded a particular message with a single search, messaging service providers (and consequently law enforcement agencies) will be capable of listing down all identities who have shared a particular popular message, which, say, invites recipients to a particular protest or is otherwise critical of the state. Messages can also be automatically filtered based on their hash. A service provider could create a predefined blocklist of hashes and prevent the delivery of messages that are on this list.[55]

Additionally, a powerful adversary, capable of calculating trillions of hashes per second, could also perform a dictionary attack, i.e., they could calculate hashes of combinations of commonly used words and phrases to guess the contents of some messages from just their hashes. This weakness can be exploited by service providers as well as anyone who accesses or

---

[53] Deeksha Bhardwaj, *Hash constant: Govt's solution to tracing originator of viral messages*, HINDUSTAN TIMES, March 2, 2021, available at https://www.hindustantimes.com/india-news/hash-constant-govt-s-solution-to-tracing-originator-of-viral-messages-101614667706841.html (Last visited on March 31, 2021).

[54] Modified messaging applications which provide added functionality are already being unofficially circulated today. *See* Ivan Mehta, *Africa is using WhatsApp 'mods' with extra features we all want*, THE NEXT WEB, March 10, 2020, available at https://thenextweb.com/africa/2020/03/10/africa-is-using-whatsapp-mods-with-extra-features-we-all-want (Last visited on March 31, 2021).

[55] This proposal is similar to 'client-side scanning' mechanisms that have been proposed elsewhere in the world, except that in this case the hashes are stored by the server — making it even less secure than performing filtering on the client side. *See* Erica Portnoy, *Why Adding Client-Side Scanning Breaks End-To-End Encryption*, ELECTRONIC FRONTIER FOUNDATION DEEPLINKS BLOG, November 1, 2019, available at https://www.eff.org/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption (Last visited on March 31, 2021).

compromises the service provider's infrastructure — a feat that is well within the capabilities of some intelligence agencies.[56]

Overall, this method can easily be circumvented by motivated individuals. More importantly, for the general public, it seriously weakens message confidentiality guarantees offered by E2EE.

C. ATTACH ORIGINATOR INFORMATION TO MESSAGES

While secure messaging applications in use today can guarantee the confidentiality of messages, they are not metadata resistant. Metadata refers to the data that describes a piece of information.[57] This means that while messaging service providers cannot see the contents of messages sent through their platforms, they do see metadata relating to them. This includes information showcasing who is participating in a conversation, when messages are sent, where the participants are located, and what the size of a message is.[58] The intelligence value of metadata to law enforcement is well-established as it can reveal important contextual information about confidential messages.[59] To protect the privacy of their users, some messaging service providers attempt to minimise the amount of metadata visible to them.[60]

A submission by Dr. Kamakoti to the Madras High Court described a proposal to implement traceability without compromising the confidentiality guarantees that the secure messaging services provide. It suggested that service providers could modify their applications to attach an additional piece of metadata to messages in the form of information about the originator of a message.[61] Originator information refers to any identifier that is linked to or can help track down an individual, such as a phone number or username, or device identifiers such as the IMEI numbers assigned to cellular phones. This information will travel along with the message as it is forwarded and can subsequently be used to identify the originator of the message. Since this originator information only points to the originator of the forward chain in question, the methods proposed here can only identify relative originators and not the absolute originator.

The submission proposed two ways of attaching originator information to messages, either by making it visible to all message recipients, or encrypting it in a way that only the service provider can see it:

1. Attach originator information to all messages

[56] Ralph Langner, *Stuxnet: Dissecting a cyberwarfare weapon.*, Vol.9(3) IEEE SECUR. PRIV. 49 (2011).
[57] ELECTRONIC FRONTIER FOUNDATION, *Surveillance and Self Defense: Metadata*, available at https://ssd.eff.org/en/glossary/metadata (Last visited on June 21, 2021).
[58] Thomas Brewster, *Forget About Backdoors, This Is The Data WhatsApp Actually Hands To Cops*, FORBES, January 22, 2017, available at https://www.forbes.com/sites/thomasbrewster/2017/01/22/whatsapp-facebook-backdoor-government-data-request/?sh=1c0024531030 (Last visited on June 21, 2021).
[59] David Cole, *We Kill People Based on Metadata*, THE NEW YORK REVIEW OF BOOKS. July 23, 2020, available at https://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/ (Last visited on June 21, 2021).
[60] Joshua Lund, *Technology preview: Sealed sender for Signal*, SIGNAL BLOG, October 29, 2019, available at https://signal.org/blog/sealed-sender (Last visited on March 31, 2021).
[61] Aditi Agrawal & Nikhil Pahwa, *IIT Madras's Kamakoti tells MediaNama how WhatsApp traceability is possible without undermining end-to-end encryption*, MEDIANAMA, August 8, 2019, available at https://www.medianama.com/2019/08/223-kamakoti-medianama-whatsapp-traceability-interview/ (Last visited on June 21, 2021).

This suggestion entails having the originator information attached to the contents of the message. This information would travel along with the message as it is forwarded, making the relative originator of the message visible to each recipient of the message.[62]

A consequence of this method would be that personal identifying information about the relative originator would be made available to unrelated third-parties without their consent when any recipient decides to forward a message. This chips away at users' privacy, and also opens up avenues for actors to harass individuals with whom they do not agree.[63] Dr. Kamakoti has suggested that service providers build a "Message Not Forwardable" setting into their applications to allow individuals to opt-out of this.[64] Such an option would prevent message recipients from using the forward functionality in messaging applications, stopping unintentional dissemination of the relative originator's identity.

It should be noted that this implementation makes the use of government/court orders for traceability redundant. As stated earlier, the traceability requirement assumes that the law enforcement agencies have access to a copy of the message. If the originator information is available to each recipient, law enforcement agencies would presumably have the accompanying originator information as well.

2. Attach encrypted originator information to all messages

The second proposal is similar in that it involves including the originator information in every message, but encrypting in a way that it is only made visible to the service provider. In this method, the service provider would hold a key that would allow it to decrypt the originator information attached to messages. The encrypted originator information would travel with the message as it is forwarded and upon receiving a lawful order, the service provider could reveal the relative originator of the message.

This proposal requires the creation and management of a key that allows decryption of the originator information that is attached to a message.[65] However, the secure management of such keys is still a challenge. Such keys would be a valuable target for malicious actors.[66]

Both of Dr. Kamakoti's proposed methods are susceptible to a common flaw, which was pointed out in Dr. Prabhakaran's submission to the Madras High Court.[67] In these methods, the originator information is not authenticated. This means that it is not cryptographically tied to the identity of the originator. Without this, the originator information can be maliciously modified by any of the senders or recipients of the message (to point to an incorrect or invalid originator). Dr. Prabhakaran suggests that this limitation can be addressed by having the originator attach a

[62] *Id*.
[63] Aditi Agrawal, *Exclusive: WhatsApp's response to Dr Kamakoti's recommendation for traceability in WhatsApp*, MEDIANAMA, August 21, 2019, available at https://www.medianama.com/2019/08/223-exclusive-whatsapps-response-kamakotis-submission/ (Last visited on April 10, 2020).
[64] AGRAWAL & PAHWA, *supra* note 61.
[65] *Id*.
[66] *Id*.
[67] Aditi Agrawal, *Kamakoti's proposals will erode user privacy, says IIT Bombay expert in IFF submission*, MEDIANAMA, August 27, 2019, available at https://www.medianama.com/2019/08/223-iff-response-kamakoti-submission-traceability-2/, (Last visited on April 10, 2020).

digital signature (proof that the message was authored on their registered device, which would be verified by the service provider), to the message.

The methods proposed by Dr. Kamakoti do not break confidentiality of messages, i.e., service providers would still not be able to read the contents of a message. They only propose the addition of an additional piece of metadata in the form of originator information. This approach is similar to an academic study that also devised a way to implement traceability.[68] However, at a time when secure messaging services are trying to minimise the amount of identifying information they collect about their users, this proposal to modify their design to collect more metadata than is required for their operation weakens privacy guarantees.[69]

It should also be noted that both the proposals are only capable of tracing relative originators of content, and cannot identify the absolute originator. Depending on how the rule is interpreted and enforced by the government, there is a possibility that Dr. Kamakoti's proposals do not meet legal requirements imposed by the rule.

We have described three methods by which messaging service providers can comply with the traceability mandate. The first two — not using end-to-end encryption or storing a hash of all messages — both allow for the tracing of both relative and absolute originators, but compromise message confidentiality. The third method, proposed by Dr. Kamakoti, only weakens the privacy properties of messaging applications, but does not allow for the identification of the absolute originator. At this juncture, it becomes pertinent to delve into some limitations that may arise from the real-world implementation of these designs.

D. COMMON LIMITATIONS

There are a number of limitations that are common to all of the methods to implement traceability described above. These are: weak identification, weak attribution, and the difficulty in limiting the geographical effects of traceability. These limitations relate to the operability of these designs in the real-world and how they may fall short of their intended goal of finding the originator of a message:

1. Weak identification mechanisms

Messaging service providers use weak identification mechanisms to identify their users, such as a phone number or email address, which can be registered anonymously or stolen.[70] This means that an originator, as identified by any of the traceability mechanisms described above, may not correspond to the individual who actually sent the message. The proposals also ignore the wide availability of unofficial clients (of say WhatsApp), which may be used to forge sender

[68] Niryan Tyagi et al., *Traceback for End-to-End Encrypted Messaging.*, 2019 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY (November 11, 2019).
[69] LUND, *supra* note 60.
[70] Brian Krebs, *Why Phone Numbers Stink As Identity Proof*, KREBS ON SECURITY, March 17, 2019, available at https://krebsonsecurity.com/2019/03/why-phone-numbers-stink-as-identity-proof (Last visited on March 31, 2021); Joseph Cox, *A Hacker Got All My Texts for $16*, VICE, March 15 2021, available at https://www.vice.com/en/article/y3g8wb/hacker-got-my-texts-16-dollars-sakari-netnumber (Last visited on March 31, 2021).

information that is proposed to be added to each message.[71] This makes traceability mechanisms easy to circumvent for the motivated bad actors that it is intended to catch.

2. Weak attribution

A message's originator, as identified by a traceability mechanism, does not necessarily correspond to the true author of a piece of information. The user may simply copy content from elsewhere and paste it into the messaging application and the information may be shared in the form of a screenshot, which is a common practice on messaging applications.[72]

Experts have also suggested that a traceability mandate may spawn commercial services located offshore to aid the spread of messages. A well-resourced actor could contract foreign services to forward messages to Indians, completely depleting any benefits of the traceability mandate.[73]

3. Geofencing limitations

The 2021 Rules state that if the first originator of a message is located outside India, the first originator within India shall be deemed to be the first originator of a particular message.[74] Experts have noted concerns about how such exceptions in determining the originator of a message would be implemented in online communications occurring across territorial boundaries, given the global nature of the internet.[75] Based on the limited personally-identifying information messaging service providers collect about their users, they would have to guess a user's nationality from the phone number associated with their account or rely on a self-declared location. This can be inaccurate or out-of-date, leading to misidentification of the originator. Service providers have expressed that they would likely face legal challenges globally if they were to comply with the traceability mandate in the face of this limitation,[76] as the privacy-reducing effects of this mandate may spill over to other geographies.

[71] Submission of Intervenor in Antony Clement Rubin & Anr. v Union of India, WP No. 20744 & 20214 of 2019 Madras High Court.
[72] AGRAWAL, *supra* note 63.
[73] Submission of Intervenor in Antony Clement Rubin & Anr. v Union of India, WP No. 20744 & 20214 of 2019 Madras High Court.
[74] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 4(2).
[75] Aditi Agrawal, *Traceability and end-to-end encryption cannot co-exist on digital messaging platforms: Experts*, FORBES INDIA, March 15, 2021, available at https://www.forbesindia.com/article/take-one-big-story-of-the-day/traceability-and-endtoend-encryption-cannot-coexist-on-digital-messaging-platforms-experts/66969/1 (Last visited on June 21, 2021).
[76] AGRAWAL, *supra* note 63.

Method	**Who can be traced**	**Effects on security and privacy**	**Ease of circumvention**
Remove end-to-end encryption	Can trace all relative originators, the absolute originator, and all individuals who sent a message.	*Breaks message confidentiality:* Storing a copy of all messages of all users on the service provider's server makes them accessible to insiders (employees, contractors) and creates a very lucrative target to breach.	*Weak identification:* Relies on phone numbers or other device identifiers to identify individuals.
Store hashes of all messages	Can trace all relative originators, the absolute originator, and all individuals who sent a message.	*Seriously undermines message confidentiality:* Storing hashes of all messages of all users on the service provider's server weakens confidentiality guarantees. A powerful adversary can pre-compute hashes of common phrases and messages (dictionary attack) and match them with stored hashes to find the contents of many messages.	*End-user can supply incorrect hash:* Relies on end-user device to truthfully compute and attach the correct hash of the message, and the server has no way of verifying it. *Weak identification:* Relies on phone numbers or other device identifiers to identify individuals.
Attach originator information	Can only trace a single relative originator of messages.	*Weakens privacy guarantees:* Originator's identity is made accessible to third parties such as: recipients of forwarded messages (in case of unencrypted originator information); employees and contractors of the service provider; and actors capable of breaching the service provider's infrastructure.	*Weak identification:* Relies on phone numbers or other device identifiers to identify individuals.

Table I: A summary of the properties of technical methods to implement traceability.

IV. LEGAL ANALYSIS OF TRACEABILITY

From the above descriptions of the technical methods to implement traceability (summarised in Table I), it is evident that there are a number of tradeoffs to the security and privacy of online messaging. With that information, in this part, we evaluate the legal implications of the rule, focusing on the actual impact on the rights of the users. We argue that the rule is unconstitutional because it creates a disproportionate harm to citizens' privacy to meet the state's need for surveillance. We also contend that the rule exceeds the scope of delegated legislation authorised by the parent Act.

A. INFRINGEMENT OF PRIVACY

Like any ostensible infringement of the right to privacy, the traceability requirement has to be evaluated in the light of the ruling in Puttaswamy which declared privacy to be an inalienable natural right.[77] It is important to note that the precise elements and application of the tests have been the subject of some debate.[78] For our analysis, we adopt the framework by Bhandari, et al, which condenses the Supreme Court's judgment in Puttaswamy, and in the more recent *Puttaswamy* v. *Union of India (*'Aadhaar'*)*.[79] Any restraint on privacy must satisfy the following criteria: legality; legitimacy, suitability and necessity; balancing (the right and need to interfere thereinto), and procedural safeguards.[80]

1. LEGALITY

Legality has been interpreted as the existence of a law in line with the requirements of Article 21 of the Constitution.[81] Per Aadhaar, "[a]n executive notification does not satisfy the requirement of a valid law contemplated under Puttaswamy. A valid law, in this case, would mean a law passed by Parliament [...]"[82] The introduction of the traceability requirement through the 2021 Rules is an exercise in delegated legislation, taking the form of an executive notification. Therefore, we need to examine whether §69A and §79, the provisions that the Government has drawn power to issue these rules from, contemplate such an invasion into privacy.

§69A of the IT Act only empowers the government to send content takedown notices to intermediaries, and does not envision any rulemaking power for authorising any infringement of privacy. §79 is much broader: as mentioned earlier, it creates an intermediary liability framework that exempts intermediaries from liability for third-party content, provided that such intermediaries satisfy certain conditions and follow due diligence guidelines. §79(3)(b) is one of those conditions, and requires intermediaries to take down content when they receive a lawful

[77] Puttaswamy v. Union of India, (2017) 10 SCC 1 ('Puttaswamy').
[78] Aparna Chandra, *Proportionality in India: A Bridge to Nowhere?* ,Vol. 3(2), OxHRHJ, 55, (2020);Vrinda Bhandari & Karan Lahiri, *The Surveillance State, Privacy and Criminal Investigation in India: Possible Futures in a Post-Puttaswamy World*, Vol. 3(2), OxHRHJ, 55, (2020); Malavika Prasad, *Aadhaar verdict: SC's majority judgment lacks consistency in logic and reasoning, turns constitutional analysis on its head*, FIRSTPOST , September 29, 2018, available at https://www.firstpost.com/india/aadhaar-verdict-scs-majority-judgment-lacks-consistency-in-logic-and-reasoning-turns-constitutional-analysis-on-its-head-5284941.html (Last visisted on April 10, 2020).
[79] Bhandari & Lahiri, *supra* note 78.
[80] *Id*.
[81] *Id.*; Puttaswamy, *supra* note 77.
[82] Puttaswamy, *supra* note 77, at ¶304.

content takedown order.[83] Therefore, one can note that both the provisions clearly permit restrictions on the right to freedom of expression. In contrast, authorisation for curbs on privacy is markedly absent in §69A and §79 of the Act.

As the parent provisions do not explicitly authorise any power that will infringe upon citizens' privacy, the introduction of the traceability requirement through delegated legislation does not adequately fulfill the test of legality.

A caveat is necessary here: this fault can be considered administrative in nature. There are other provisions in the IT Act, like §69, which provide for surveillance powers. Therefore, one could argue that the traceability requirement would satisfy the test of legality if the government notifies the rules again, albeit explicitly drawing its rulemaking power from such parent provisions. Note also that the IT Act reserves a general rule-making power for the Central Government.[84] Thus, a comprehensive analysis of legality requires us to investigate whether the rules (including traceability) exceed the general scope of rule-making and whether the rule is *ultra vires* the parent Act. Thus, although the rule in its current form does not strictly pass the 'legality' test in Puttaswamy, we explore these two questions in more detail in the next sub-part.

2. LEGITIMATE STATE AIM

For now, we can move on to assessing whether the policy is backed by a legitimate state aim, i.e. whether 'the goal is of sufficient importance justifying overriding a constitutional right.'[85] The press note accompanying the notification of the rule outlines the Government's rationale: proceedings in the Supreme Court that asked the Government to frame guidelines to eliminate online child sexual abuse and rape related content; a Calling Attention Motion in the Rajya Sabha on disinformation leading to violent lynchings, to which the Ministry had promised amending the rules to include traceability; and the Report of the Ad-hoc Committee of the Rajya Sabha that recommended breaking end-to-end encryption so that originators of child sexual abuse material could be traced.[86]

However, the rule states that an order to trace the first originator can be passed for the "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

[83] The section requires them to take content down when they receive 'actual knowledge', a term interpreted by the Supreme Court in *Shreya Singhal v. Union of India* to mean only government or court orders, *see* Shreya Singhal v. Union of India, (2013) 12 S.C.C. 73.

[84] Information Technology Act, 2000, § 87; Supreme Court in a number of decisions has held that where power is conferred to make subordinate legislation in general terms, the subsequent particularisation of the matters/topics has to be construed as merely illustrative and not limiting the scope of the general power, *see* Academy Of Nutrition Improvement v.Union Of India, 2011 8 SCC 274.

[85] Puttaswamy, *supra* note 77, at ¶268.

[86] Ministry of Electronics and Information Technology, *Government notifies Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021*, Press Information Bureau, February 25, 2021, available at https://pib.gov.in/PressReleseDetailm.aspx?PRID=1700749 (Last visited on March 25, 2021).

of not less than five years."[87] While these grounds in the actual rule are expansive compared to the press release, they are still legitimate grounds for surveillance.[88]

3. SUITABILITY AND NECESSITY

The suitability test evaluates whether the measures are capable of realising the goals pursued.[89] Ostensibly, tracing originators of content can aid law enforcement agencies in finding and prosecuting actors responsible for producing content that qualifies as an unlawful act, or incites crime. However, as established in the previous part, all traceability implementations suffer from critical limitations that prevent it from achieving this goal, and also pose operational difficulties for messaging services.

Even if traceability could be operationalised as envisioned by the government, its potential use cases are very limited. For instance, groups circulating child sexual abuse or extremist material are likely to be restricted to a narrow set of individuals. In such cases, manual tracing of originators through a physical investigation or the use of metadata is viable. The requirement is possibly only useful for messages that are designed to be viral and spread to a larger community which can make existing surveillance methods time-consuming.

For those circumstances, the traceability requirement signals a state interest in prosecuting creators and ignoring distributors. It is important to consider a recent observation by the Madras High Court in this context: the act of forwarding a message amounts to accepting and endorsing a message.[90] However, the traceability requirement seemingly ignores the culpability of forwarding parties. Thus, the traceability mandate can contribute to a culture of impunity in message recipients, who may share/forward content without critically assessing it, resting in an assurance that law enforcement agencies will not take any action against them. In this regard, consider that frameworks to counter the spread of misinformation focus on encouraging skepticism in individuals,[91] given the critical role information recipients can play in combating the spread of misinformation.[92]

Given the relative ease with which all traceability proposals can be circumvented by motivated individuals, how poorly they identify the actual creators of content, and the limited scenarios in which it may be potentially useful, serious doubt is cast on the suitability of this mandate in achieving the goals pursued.

The next prong, necessity, requires an assessment of whether the specific measure is critical and whether there are alternatives with a "lesser degree of limitation which can achieve the same purpose."[93] From the previous part of the paper, it is clear that the traceability mandate requires platforms to incorporate a feature and/or retain more data just for the purposes of state

[87] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 4(2).
[88] Vrinda Bhandari and Karan Lahiri, supra note 78 citing *Puttaswamy* ¶311 (Chandrachud J), ¶639 (Kaul J).
[89] Puttaswamy, *supra* note 77, at ¶267 (Per Sikri J)
[90] S.VE. Shekher v. The Inspector of Police , Criminal Appeal No. 12229 of 2018 (Madras HC), ¶46(Unreported).
[91] Stephan. Lewandowsky et al, *Misinformation and Its Correction: Continued Influence and Successful Debiasing*, Vol.13(3), PSYCHOL SCI PUBLIC INTEREST, 106–131(2012).
[92] M. Laeeq Khan & Ika Karlina Idris, *Recognise misinformation and verify before sharing: a reasoned action and information literacy perspective*, Vol. 38(12), BEHAVIOUR & INFORMATION TECHNOLOGY, 1194-1212 (2019).
[93] Note that rule 4(2) in its language also repeats this test as a procedural safeguard, *see* Puttaswamy, *supra* note 77, at ¶280.

surveillance. However, the government has not presented any evidence that the amount of data (and the current surveillance powers) are inadequate to counter the issues that traceability is meant to solve.

Generally, metadata collected by online services (in the normal course of their operation, or in response to surveillance requests) can aid the detection and investigation of crimes. Law enforcement agencies have openly acknowledged that metadata can provide comprehensive information about user activity and the networks they form part of.[94]

Moreover, platforms that have deployed E2EE themselves also use such data to combat harmful content: for instance, WhatsApp proactively scans all unencrypted data of users to detect and stop child sexual exploitation and other forms of abuse.[95] Another service, Matrix, has outlined how users and administrators deploying Matrix can moderate content and apply specific rules based on metadata.[96]

If the metadata is not enough, specific end-user devices can be targeted and broken into, based on the evidence already available to law enforcement agencies.[97] While these methods carry their own set of concerns that merit a discussion outside of the scope of this paper, they can be considered more proportionate because they target specific individuals, rather than undermining the communication security and privacy of all citizens.[98]

It is also important to keep in mind that different types of harmful content spread in different ways, and may require tailored solutions rather than a one-size-fits-all approach. For instance, a detailed study on online child sexual abuse material in India recommended that such content can be combated by advocating for changes in how user join groups, and better enforcement of rules by these platforms.[99] These would not affect platform architecture or E2EE. In fact, it brought to notice that a critical gap in addressing complaints of child sexual abuse

[94] A former NSA General Counsel has stated that "metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content." As unfortunate as it seems, former director of the NSA and CIA General Michael Hayden even admitted that these agencies "kill people based on metadata.", *See* Cole, *supra* note 59.

[95] WHATSAPP FAQ, *How WhatsApp Helps Fight Child Exploitation*, February, 2021, available at https://faq.whatsapp.com/general/how-whatsapp-helps-fight-child-exploitation/?lang=en (Last visited on June 21, 2021).

[96] MATRIX, *Combating abuse in Matrix - without backdoors,* November 9, 2020, available at https://matrix.org/blog/2020/10/19/combating-abuse-in-matrix-without-backdoors/ (Last visited on June 21, 2021).

[97] The Central Government and the Delhi Police are known to have such capabilities, *see* Aditi Agrawal, *Exclusive: Delhi Police Has the Tools to Extract Data from Smartphones, Including IPhones*. MediaNama, December 22, 2020, available at https://www.medianama.com/2020/12/223-exclusive-delhi-police-has-tools-extract-data-from-smartphones-iphones/ (Last visited on June 21, 2021); Gurshabad Grover & Tanaya Rajwade, *Pegasus Snoopgate, an Opportune Moment to Revisit Legal Framework Governing State Surveillance Framework*¸ THE INDIAN EXPRESS, December 25, 2019 available at https://indianexpress.com/article/opinion/columns/pegasus-whatsapp-surveillance-data-protection-6183355/(Last visited on June 21, 2021).

[98] Rishab Bailey et al., *Backdoors to Encryption: Analysing an intermediary's duty to provide "technical assistance"*, DATA GOVERNANCE NETWORK, March 15, 2021, available at https://datagovernance.org/report/backdoors-to-encryption-analysing-an-intermediarys-duty-to-provide-technical-assistance, (Last visited on June 21, 2021).

[99] CYBER PEACE FOUNDATION, *End (-to-End Encrypted) Child Sexual Abuse Material*(July, 2020) available at https://www.cyberpeace.org/CyberPeace/Repository/End-to-end-Encrypted-CSAM-2.pdf (Last visited on June 21, 2021).

material was the lack of adequate reporting and follow-up mechanisms on the part of the Government.[100]

Thus, in light of these surveillance mechanisms that are less intrusive to citizens' privacy, the Government has failed to demonstrate how traceability is necessary for them to carry out their functions.

4. BALANCING THE RIGHT AND INTERFERENCE THEREOF

This stage involves balancing the importance of achieving the proper purpose with the social importance of preventing limitations on constitutional rights.[101] All the proposed technical methods to implement traceability described in Part III have an effect on the security and privacy of online communications that a large proportion of citizens rely on. These effects range from the risk of compromise of communications to hostile foreign states to the reduction in the reasonable standard of privacy that we expect from our communications.

Here, it is pertinent to note a joint effort by scholars around the world to articulate how the tests of necessity and proportionality (as they appear comparably in international human rights law)[102] apply to communications surveillance. They clearly outline that governments "should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State Communications Surveillance purposes."[103] Traceability runs squarely opposite to this proposition.

In a similar vein, Puttaswamy recognised data protection as a critical component of informational privacy, which in turn is a part of the constitutional right to privacy. A cardinal principle in data protection is data minimisation, i.e. states should create laws that force companies to collect the least amount of user information that they need to operate and provide their service.[104] All traceability solutions require at least the collection of more personally identifiable information that is not critical for their operation. The traceability requirement runs contrary to this principle, thereby sanctions not just state surveillance, but encourages more private surveillance.

With the focus on bad actors, it should not be ignored that the traceability rule will affect a large population's security and privacy. In this regard, it's important to keep in mind how E2EE services are normally used by the larger public. WhatsApp, for instance, which is popular in India and has been the primary target for the traceability requirement, is mostly used for private

---

[100] *Id*.

[101] Puttaswamy, *supra* note 77, at ¶281.

[102] Apart from the general commitment to international law articulated in Article 51 of the Constitution, Justice Chandrachud's judgement in Puttaswamy clearly affirms that the judgment also seeks to align India's consideration of the right to privacy with international human rights law, *see* Puttaswamy, *supra* note 77, at ¶129

[103] ELECTRONIC FRONTIER FOUNDATION, *Necessary & Proportionate: On the Application of Human Rights to Communications Surveillance*, December 2014, available at https://necessaryandproportionate.org/files/en_principles_2014.pdf, (Last visited on March 25, 2020).

[104] JUSTICE B.N. SRIKRISHNA COMMITTEE, *A Free and Fair Digital Economy – Protecting Privacy, Empowering Indians*, ¶ 52 (July, 2018); ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, *OECD guidelines on the protection of privacy and transborder flows of personal data*, available at at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Last visited on June 21, 2021).

and personal communication: "90% of messages sent on WhatsApp are between two people, and the average group size is fewer than 10 people."[105] In fact, Indian users found that their exposure to problematic content was significantly higher on more public platforms (including social media and search engines), than it was on E2EE services.[106]

Thus, without reasonable justification, the traceability mandate infringes on the security and privacy of the many, in an ostensible attempt to catch a few bad actors, who can easily fool these systems and continue their behaviour.

5. PROCEDURAL SAFEGUARDS

Lastly, we come to procedural safeguards. An order to intermediaries to identify the first originator of content can be passed either by courts, or by governmental agencies under §69 of the IT Act. While procedural safeguards can be considered inherent in orders passed by a court, the same cannot be said for executive surveillance orders issued under §69. The provision empowers authorised agencies to "intercept, monitor or decrypt" information in any computer resource, and order intermediaries to provide technical assistance for the same purposes.[107] The IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 ('Interception Rules') create a legal framework for the exercise of powers under the provision.

This framework has little accountability built in. For instance, issuance of a surveillance order under the Interception Rules does not require any judicial sanction.[108] The only mechanism for accountability under the Interception Rules is a review committee that assesses each order. The review committee entirely consists of ministerial secretaries, thus lacking oversight from independent authorities.[109] There is also no judicial or parliamentary oversight of the macro-level operations of this or any other surveillance mechanism.[110] This opaque and inscrutable framework has meant that there is little room for affected parties to find out if at all they are under surveillance. One can see how this effectively rules out challenges to illegal surveillance orders.[111]

It should be noted that the Supreme Court has not taken a critical view of such minimal procedural safeguards yet. In *People's Union Of Civil Liberties* v. *Union of India* ('PUCL'), for instance, the Supreme Court specifically laid down guidelines to act as procedural

[105] *Supra* note 95.
[106] CUTS INTERNATIONAL, *Understanding Consumers Perspective on Encryption in India*, available at https://cuts-ccier.org/pdf/survey-finding-understanding-consumers-perspective-on-encryption.pdf, (Last visited on June 21, 2021).
[107] Information Technology Act, 2000, § 69.
[108] The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 3.
[109] The Review Committee is constituted under rule 419A of Indian Telegraph Rules, 1951, *see* Rule 16, Indian Telegraph (Amendment) Rules, 2007.
[110] Chinmayi Arun, *Paper-Thin Safeguards and Mass Surveillance in India*, January 3, 2015, Vol. 26, NLSIR, 105 (2014).
[111] Internet Freedom Foundation v. Union of India, *Plaint filed by petitioner*, (2017) 10 SCC 1.

safeguards against an arbitrary exercise of surveillance powers under §5(2) of the Indian Telegraph Act — these guidelines did not mandate judicial sanction of each order.[112]

A caveat here is that the constitutionality of §5(2) of the Telegraph Act was not directly and seriously challenged in the case.[113] More importantly, PUCL was pronounced in 1996, much before Puttaswamy and Aadhaar. While legal scholars have argued that there existed a constitutional case for including judicial oversight even before these cases,[114] such oversight can be considered a 'constitutional imperative' after the tests on proportionality and procedural safeguards laid out in Puttaswamy and Aadhaar.[115] For instance, a surveillance provision in the Aadhaar Act was struck down by the Supreme Court in Aadhaar because it only required executive application of mind (and did not have judicial oversight).[116]

The lack of these safeguards is also incompatible with international human rights standards. A global pool of experts on communications privacy noted in the International Principles on the Application of Human Rights to Communication Surveillance, for instance, that all surveillance orders must be sanctioned by an independent judicial authority.[117] Additionally, they also require that users be afforded an opportunity to challenge the surveillance orders.[118]

Thus, it is critical to relook at whether the safeguards in the Interception Rules will pass constitutional scrutiny. Note that the constitutionality of §69 of the IT Act is currently under challenge in *Internet Freedom Foundation vs. Union of India*, where the petitioners have raised many of the issues mentioned here.[119]

Overall, the traceability rule is constitutionally suspect on account of not having a legal basis, disproportionately infringing on privacy when less intrusive alternatives are already available with the Government, and using a surveillance framework with minimal safeguards.

B. COMPARISON WITH THE PARENT ACT

The introduction of the traceability requirement through the 2021 Rules is an exercise in delegated legislation, referring to the rule-making power under §69A and §79 of the IT Act. It is an established principle that such delegated legislation cannot exceed the scope of the enabling provision of the parent statute.[120] In *Maharashtra State Board v Paritosh Kumar*, the apex court laid down a three-step test to assess the constitutionality of delegated legislation, namely: "(1) whether the provisions of such regulations fall within the scope and ambit of the power conferred by the statute on the delegate; (2) whether the rules/regulations framed by the delegate are to any extent inconsistent with the provisions of the parents enactment and; lastly (3)

[112] Arun, *supra* note 1110; People's Union Of Civil Liberties vs Union Of India, AIR 1997 SC 568.
[113] Bhandari & Lahiri, *supra* note 78.
[114] Arun, *supra* note 110.
[115] *Id*.
[116] Bhandari & Lahiri, *supra* note 78.
[117] *Supra* note 110.
[118] *Id*.
[119] *Supra* note 118.
[120] State of Tamil Nadu v. P Krishnamurthy, (2006) SCC 517.

whether they infringe any of the fundamental rights or other restrictions or limitations imposed by the Constitution."[121]

Pertinently, for the first and third prongs, we have already noted in the previous sub-part that §69A and §79 do not foresee or authorize invasion into citizens' privacy. It is also important in this regard to note that the 2021 Rules have been criticised for greatly exceeding the scope of delegated legislation.[122] The intermediary guidelines envisioned under the provision are meant to provide basic due diligence checks.[123] Even the creation of a separate category of 'significant social media intermediaries' or messaging services, definitions which do not appear in the parent Act, can be considered excessive delegation in rule-making.[124] Making a privacy obligation on this category is thus even more suspect.

As noted earlier, there are surveillance provisions in the IT Act, which also bestows a general rule-making power on the executive to carry out the functions of the Act. An analysis of traceability with respect to the second prong of the test then requires an examination of the relevant provisions in the Act.

The most pertinent provision relating to surveillance of communications is §69 of the Act and the associated Interception Rules, under which traceability orders will be issued. Rule 13(3) of the Interception Rules limits the ambit of information and decryption requests to the extent of the degree of the intermediary's control over the tools for decryption and information.[125] Therefore, the provision, read with the rules, does not fasten liability on intermediaries for information that they cannot access in the first place. This interpretation is supported by rule 2(g) of the Interception Rules, which defines 'decryption assistance' as allowing access "to the extent possible, to encrypted information." Therefore, the intermediary's obligations with respect to decryption requests are qualified by the same condition. This proviso is particularly significant in the case of end-to-end encrypted messaging service providers, where intermediaries neither have access to messages, nor to their decryption keys.[126] A plain reading of the phrase makes it clear that intermediaries, under the Interception Rules, cannot be compelled to fundamentally alter the nature of their platform and service. Thus, the current law confines the obligations of the intermediary to the assistance they can *reasonably* provide, given the existing architecture of the

[121] Maharashtra State Board of Secondary and Higher Education v. Paritosh Bhupesh Kumar Sheth, AIR 1984 SC 1543, ¶21.

[122] Raman Jit Singh Chima, *More about Big Government than Big Tech,* THE HINDU, March 1, 2021, available at https://www.thehindu.com/opinion/lead/more-about-big-government-than-big-tech/article33956682.ece(Last visited on June 21, 2021) ; Prashant Reddy, *New IT Rules: The Great Stretching of 'Due Diligence' Requirements Under Section 79,* THE WIRE, February 27, 2021 available at https://thewire.in/tech/new-it-rules-the-great-stretching-of-due-diligence-requirements-under-section-79(Last visited on June 21, 2021); Gurshabad Grover & Anna Liz Thomas, *Intermediary Liability and Safe Harbour: On Due Diligence and Automated Filtering,* LAW AND OTHER THINGS, November 25, 2020, available at https://lawandotherthings.com/2020/11/intermediary-liability-and-safe-harbour-on-due-diligence-and-automated-filtering/(Last visited on June 21, 2021)(Addressing the debate on the relationship between 'due diligence' and the guidelines).

[123] *Id*.

[124] Chima, *supra* note 122.

[125] Any direction of decryption of information issued under rule 3 to intermediary shall be limited to the extent the information is encrypted by the intermediary or the intermediary has control over the decryption key.

[126] WHATSAPP FAQ, *End-to-end encryption*, February, 2021, available at https://faq.whatsapp.com/en/android/28030015/ (Last visited on April 6, 2020); SIGNAL SUPPORT FAQ, *How do I know if my communication is private*? available at https://support.signal.org/hc/en-us/articles/360007318911-How-do-I-know-my-communication-is-private- (Last visited on April 6, 2020).

platform. This repeated emphasis on the interception and decryption *abilities* of the intermediaries indicates a broader policy decision that §69 and the Interception Rules do not provide for mandating changes to platform design and encryption, and cannot be grounds for compelling messaging services to collect specific types of information.

The traceability requirement forces messaging services to collect information about users that they were not previously recording. In this context, it is relevant to consider §67C of the Act, which empowers the government to prescribe (through secondary legislation) certain types of information that needs to be preserved and retained by an intermediary.[127] Currently, no regulations under the provision apply to intermediaries generally, or to communication services or social media companies specifically.[128] Significantly, the provision does not explicitly allow the government to mandate intermediaries to collect additional information. In other words, a plain reading of the section implies that the Government may require intermediaries to preserve information they are *already collecting* in the first place.[129]

§84A of the IT Act may also be relevant in this discussion. The provision allows the Central Government to prescribe "modes or methods" of encryption for the "secure use of the electronic medium and for the promotion of e-governance."[130] No such rules have been notified till date.[131] While there exists considerable literature criticising the Draft National Policy issued under the provision in 2015,[132] there has been very little debate on the nature and scope of powers granted to the government through this provision. From a purposive interpretation of the provision, the term 'secure use of the medium' indicates the prescription of *minimum* standards for encryption. Even if read broadly, the Government is only empowered to prescribe standards of encryption, say in terms of strength, rather than outright proscriptions on designs of encryption protocols or radical changes in services offered.

Seen together, these provisions make the broader policy decision in the IT Act clear: nothing empowers the Government to compel intermediaries to change the core technical architecture of their product or collect more personal information. As discussed in the previous section, achieving traceability is impossible without such changes. Once we note this, it is easy to appreciate how the traceability requirement conflicts with the current legal framework.

In *National Stock Exchange Member v Union of India*, the Delhi High Court clarified the hierarchy of legal norms. It held that generally, the lower norm (delegated legislation in this case) would be declared ultra vires the higher norm (the law passed by the Parliament) in case of conflict between

[127] Information Technology Act, 2000, §67C.

[128] In July 2016, it was reported that a committee was set up by the MeitY to formulate rules under the section that would be applicable to communication services, but no such rules have been notified yet. See Surabhi Agarwal, 'Indian govt to ask tech intermediaries like Gmail, Whatsapp to store user info', *see* Surabhi Agarwal, *Indian government to ask tech intermediaries like Google and Whatsapp to store user info*, ET TECH, October 14, 2016, available at https://tech.economictimes.indiatimes.com/news/internet/indian-govt-to-ask-tech-intermediaries-like-gmail-whatsapp-to-store-user-info/54842635 (Last visited on April 6, 2021).

[129] For instance, WhatsApp makes a policy decision to not retain most metadata related to a message sent through its service. The Government has the power through the provision to mandate them to retain this metadata for a specified duration. However, the Government would not be able to mandate WhatsApp to record certain types of information.

[130] Information Technology Act, 2000, §84A read with § 87(2)(zh).

[131] Vinay Kesari, *India's upcoming encryption wars*, FACTORDAILY, August 30, 2018, available at https://factordaily.com/indias-upcoming-encryption-wars (Last visited on April 6, 2021).

[132] *Supra* note 8.

the two.[133] Thus, the traceability requirement in 2021 rules can be seen as *ultra vires* of the parent Act.

C. ORIGINATORS AND EVIDENCE

The demand for traceability of information ostensibly seeks to enable the identification of individuals who may have committed criminal offences. Hence, it becomes important to consider how the requirement will interact with the legal framework on digital evidence.

The term 'originator' is defined in the IT Act as a "person who sends, generates, stores or transmits any electronic message; or causes any electronic message to be sent, generated, stored or transmitted to any other person."[134] Here, an incongruence in the usage of 'originator' is apparent: technological interventions to implement traceability can only identify a pseudonymous identifier relatable to a device, email address, or phone number (and not an actual person).

In this regard, §88A of the Indian Evidence Act clarifies the treatment to be given to electronic messages.[135] It states that the court may presume that an electronic message sent by a person through a service corresponds with the message fed into their computer for transmission. However, the provision specifically prohibits the court from making any presumptions as to the person who sent the message.[136] Thus, it acknowledges that people may use others' devices or identifiers (with or without authorisation), and the identity of the originator remains a question for determination based on facts.

This understanding of the 'originator' under the Indian Evidence Act,1872 appears to be at loggerheads with its treatment under the 2021 Rules. The Evidence Act envisages the 'originator' as an identity that is to be duly determined by a court of law in light of the evidence at hand, while the 2021 Rules view the 'originator' as an indisputable fact about the content creator's identity that can be discerned by technological means. This gulf in the interpretation of the law may appear minor; however, it does speak to the fact that there is only limited evidentiary value in the information messaging services can share in response to a traceability request. The information gleaned through a traceability request can form only part of the investigation, and by itself is not conclusive proof of the identity of the content creator or actor.

V. CONCLUSION

The traceability requirement is now being challenged in various High Courts in the country.[137] It is also significant against the backdrop of increasing advocacy by governments across the world to weaken E2EE requirements. In the recent past, we have seen the Lawful Access

[133] National Stock Exchange Member vs Union of India Ors., 2006 70 SCL 151, ¶ 14.
[134] Information Technology Act, 2000, §2(1)(za).
[135] Indian Evidence Act,1872, § 88A.
[136] *Id*.
[137] Note that this paper could not analyse the petitions because they emerged only as this paper was being finalised for publication, *see* SOFTWARE FREEDOM LAW CENTER, *Legal Challenges to the Traceability Provision - What Is Happening in India?* May 28, 2021, available at https://sflc.in/legal-challenges-traceability-provision-what-happening-india(Last visited on June 21, 2021).

to Encrypted Data Bill being tabled before the US Congress,[138] the FBI Director's testimony before the US Senate Judiciary Committee attributing the US Capitol attacks to the use of encrypted communication,[139] the call on Facebook to desist from deploying E2EE on its platforms and the Five Eyes demanding law enforcement access to encrypted information.

In addition to advocacy against E2EE, a recent trend in policy discussions is of proposals that insidiously undermine E2EE's security and privacy guarantees without 'breaking' E2EE. Experts have repeatedly highlighted the dangers of weakening encryption standards in these debates.[140]

The traceability requirement comes as a bold move by India in the global race to the bottom for minimum standards of information security. While the issues sought to be tackled by the government, such as mob lynchings and child pornography, are legitimate concerns, mandating messaging platforms to implement a mechanism for purely surveillance purposes does not align with our constitutional framework on the right to privacy. The state failed to demonstrate the necessity and proportionality of the traceability requirement, in the face of the availability of less intrusive means. The rule also suffers from a lack of procedural safeguards, further dragging it into unconstitutionality. Given the broad surveillance and draconian surveillance framework in India, traceability will only serve as a tool in the government's arsenal that can be deployed to justify disproportionate information requests.

It is also apparent here that the debate on 'traceability' is better contextualised within surveillance and lawful interception rather than intermediary liability. As we have seen, the 'traceability' proposal far exceeds the scope of what is envisioned by §69A and §79 of the IT Act, provisions that cannot and should not form the basis of any surveillance from the state. Even overall, the IT Act signals a broader policy framework, wherein the state is currently not empowered to mandate technical changes to platforms or coerce them to collect more personal information of users. Rather than enacting data protection legislation that abides by the principle of data minimisation, the government has, through traceability, created more opportunities for private surveillance.

That said, law enforcement access to information is impeded in other ways, which we believe should be priorities for reform for the government. Since popular online services are based in foreign jurisdictions, law enforcement agencies have to often go through procedures under the various mutual legal assistance treaties (MLATs) to which India is a party, and courts may

[138] United States Congress, Senate, *Lawful Access to Encrypted Data Act*, 23 Jun 2020. https://www.congress.gov/bill/116th-congress/senate-bill/4051?r=1&s=1, (Last visited on June 21, 2021).
[139] Tonya Riley, *The Cybersecurity 202: FBI Renews Attack on Encryption Ahead of Another Possible Attack on the Capitol,* THE WASHINGTON POST, March 4, 2021, available at https://www.washingtonpost.com/politics/2021/03/04/cybersecurity-202-fbi-renews-attack-encryption-ahead-another-possible-attack-capitol/ (Last visited on June 21, 2021).
[140] GLOBAL ENCRYPTION COALITION, *Breaking encryption myths: What the European Commission's leaked report got wrong about online security*, November 19, 2020, available at https://www.globalencryption.org/2020/11/breaking-encryption-myths/ (Last visited on June 21, 2021)**;** Knodel, *supra* note 40.

have to rely on letters rogatory.[141] These procedures can be cumbersome and time-consuming.[142] Renegotiating MLATs and opening channels for effective collaboration with foreign law enforcement agencies could be a starting point, extending to an overhaul of the MLAT regime.[143] Another avenue for capacity development in the state agencies would be targeted end-device hacking, which when authorised by a robust and lawful regime, can be a proportionate alternative to *en masse* traceability.

On encryption policy broadly, it is imperative that the government realise the importance of E2EE in facilitating the exercise of human rights, and how it enables security rather than undermines it. In the triad of users, governments and private corporations, the user is the weakest. E2EE affords users a zone of privacy from government and corporate surveillance, thereby protecting speech on the internet. The deleterious effect of undermining E2EE in India are not just theoretical: in a survey of more than 2000 participants, 27% stated that they were more likely to stop sharing certain kinds of information with contacts if E2EE was removed.[144] A rights-respecting approach to regulation necessitates that the Government of India move away from undermining E2EE, and instead pave the way for more private and secure communication on the internet.

[141] OBSERVER RESEARCH FOUNDATION, *Hitting Refresh: Making India-US data sharing work* (*Observer Research Foundation*, (August 2017) available at https://www.orfonline.org/wp-content/uploads/2017/08/MLAT-Book.pdf(last visited accessed April 6, 2020).

[142] Amber Sinha et al., *Cross-border Data Sharing and India: A Study in Processes, Content and Capacity*, CENTRE FOR INTERNET AND SOCIETY, September 27, 2018, available at https://cis-india.org/internet-governance/blog/cross-border-data-sharing-and-india-a-study-in-processes-content-and-capacity (Last visited on June 21, 2021).

[143] MLAT regimes commonly suffer from a host of problems, and researchers have sought reforms in various jurisdictions, *see* Jonah Force Hill, *Problematic Alternatives: MLAT Reform for the Digital Age,* HARVARD NATIONAL SECURITY JOURNAL, May 31, 2019, available at https://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/(Last visited on June 21, 2021).

[144] *Supra* note 106.