Indian Journal of Law and Technology

Volume 17 | Issue 1 Article 2

2021

Encryption in India: Preserving the Online Engine of Privacy, Free Expression, Security, and Economic Growth

Encryption in India: Preserving the Online Engine of Privacy, Free Expression, Security, and Economic Growth

Greg Nojeim & Namrata Maheshwari***

Abstract *This article argues that the traceability mandate imposed in India by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 undermines encryption and negatively impacts cybersecurity as well as the fundamental right to privacy. In doing so, it explains how the traceability requirement fails the necessity and proportionality test laid down by the Indian Supreme Court in the Puttaswamy judgment, wherein it held that the right to privacy is a fundamental right under the Constitution of India. Further, the article makes a case for why encryption is important for protecting privacy, free expression, and other human rights, and also for bulwarking the economy, preserving democracy, and ensuring national security.*

* Greg Nojeim is a Senior Counsel and Co-Director of the Security and Surveillance Project at the Center for Democracy & Technology, an NGO with offices in Washington, D.C. and Brussels.

** Namrata Maheshwari is Asia Pacific Policy Counsel at Access Now, an international non-profit organisation, and former Consultant with the Center for Democracy and Technology. She is an India qualified lawyer.

The authors would like to thank Ankit Kapoor, BA.LLB (Hons.) student at NLSIU, for his assistance with the preliminary research for this article.

Part I of the article provides a background on how encryption works and the purpose it serves in the digital era. Part II analyzes the trajectory of encryption policy in India and the relevant legal frameworks. Thereafter, Part III explains the traceability mandate under the New Intermediary Guidelines and its effect on encryption, and consequently, the impact on cybersecurity and the right to privacy. It assesses whether it meets the requirement of necessity and proportionality as set out by the Supreme Court. Finally, Part IV explains that encryption should be protected and encouraged because it guards against unwarranted surveillance and preserves privacy and expression, is a crucial tool to protect human rights in the digital age, strengthens national security, and benefits the economy.

Introduction

One of the strongest statements in favour of privacy against government intrusion was made by the former Prime Minister of the United Kingdom, William Pitt, in 1763: 'The poorest man may in his cottage, bid defiance to all the forces of the Crown. It may be frail, its roof may shake; the wind may blow through it; the storm may enter; the rain may enter, but the King of England may not enter; all his force dares not cross the threshold of the ruined tenement.'[1] Centuries later, while the protection of privacy against government surveillance remains a work in progress, encryption serves as a veritable gatekeeper of the online sphere that houses the most sensitive and private information of individuals, communities, corporations, and the state alike.

Despite the positive impact of encryption on privacy, security, and the economy, the Indian government proposes to weaken encryption and imperil users' rights while jeopardising the security of data online.[2] This article aims to contribute to the encryption debate in India, and globally, by showing that proposals that have the effect of weakening encryption and communications security should be rejected because they will not achieve the desired objectives and would instead severely hamper privacy, free expression, and cybersecurity, and cause significant damage to the economy.

Section I of this article provides background information about encryption. Section II elucidates the trajectory of encryption policy in India by providing

---

1 William Pitt, Speech on the Excise Bill (1763) (quoted in *Miller v United States* 1958 SCC OnLine US SC 131 : 2 L Ed 2d 1332 : 357 US 301, 307 (1958)).

2 Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

an overview of the important developments pertaining to encryption over the last three decades. Section III analyses changes to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which impose a requirement that communications carried on certain messaging services be traceable to their source. It shows that a traceability mandate would weaken encryption, fail to accomplish the goal of stopping the spread of fake news, and would not meet the requirements of the proportionality test the Supreme Court recently established when it held that the right to privacy is a fundamental right under the Indian Constitution. Finally, Section IV preceding the conclusion makes a case for protecting and encouraging encryption because of its importance for privacy in the face of rampant surveillance, the necessity for upholding human rights, and a positive correlation with national security and economic growth.

I. Background on Encryption

In the digital era, the amount of sensitive data stored electronically grows, and will continue to grow exponentially.[3] Medical and biometric records, bank account details, private communications, and location information are only a few of the many examples of such data that is now more easily accessible than ever before.[4] The concomitant effects of this trajectory are serious concerns pertaining to privacy[5] and online security.[6] The COVID-19 pandemic has created new demands for digital data, both by forcing many schools and workplaces into remote settings and by fostering technologies to fight the disease. This in turn has aggravated associated privacy concerns[7]

---

[3] Thomas Alsop, 'Data Storage - Statistics & Facts' (*Statista*, 23 June 2020) <https://www.statista.com/topics/3150/data-storage/#dossierSummary__chapter1> accessed 12 November 2020.

[4] Eva-Maria Schomakersa, Chantal Lidyni
, Dirk Müllmannb & Martina Zieflea, 'Internet Users' Perceptions of Information Sensitivity – Insights from Germany' (2019) 46 Intl J Info Management 142, 143-148.

[5] ibid.

[6] Terrence Berg, 'The Changing Face of Cybercrime', (2007) 86 Michigan Bar J 18.

[7] Elizabeth Beattie, 'We're Watching You: COVID-19 Surveillance Raises Privacy Fears' (*Al Jazerra*, 3 April 2020) <https://www.aljazeera.com/news/2020/4/3/were-watching-you-covid-19-surveillance-raises-privacy-fears> accessed 2 November 2020; For updates on global responses to the covid-19 pandemic that raise privacy related concerns, *see*: 'Tracking the Global Response to COVID-19' (*Privacy International*) <https://privacyinternational.org/examples/tracking-global-response-covid-19> accessed 12 November 2020, and Andrej Zwitter & Oskar J. Gstrein, 'Big Data, Privacy and COVID-19 – Learning from Humanitarian Expertise in Data Protection' (2020) 5 J Intl Humanitarian Action <https://jhumanitarianaction.springeropen.com/articles/10.1186/s41018-020-00072-6> accessed 12 November 2020.

and enhanced the importance of tools such as encryption to secure data and protect individuals, governments, and the economy.

Encryption preserves data privacy and security. It is the method in cryptography[8] by which information is 'locked' and rendered unintelligible to an unauthorized recipient, and the authorized recipient possesses a 'key'[9] that decrypts the message and converts it into plain text.[10] In other words, encryption scrambles readable text or files in a way that only the sender and the intended recipient can comprehend the content. It protects data from unauthorized access and preserves the authenticity and privacy of information online, and protects users in a range of ways. As Philipp Rogaway puts it, 'cryptography rearranges power: it configures who can do what, from what.'[11] By ensuring that users retain autonomy over who accesses their data, encryption re-balances the power of users with the power of other parties that typically have more. Most banking applications and credit card payment terminals use encryption and it is broadly used across most communication platforms.[12]

Encryption protects both stored data and data in transit.[13] One of the most secure forms of encryption is end-to-end encryption ('**E2EE**'). E2EE

---

[8] *The American Heritage Dictionary of English Language* (4th edn, Houghton Mifflin Co. 2000) 439. Herein, cryptography is defined as '1. The process or skill of communicating in or deciphering secret writings or ciphers. 2. Secret writing.'

[9] An encryption key is a string of numbers. The longer the string, the stronger the encryption. Typically, when using encryption software, the user's password activates the key. There are two methods of employing such keys – symmetric encryption, also known as private key encryption; and asymmetric encryption, also known as public key encryption. Private key encryption entails the use of the same key to encrypt and decrypt content. Whereas public key encryption requires a public key, known to the public, to encrypt and a private key, known only to the individual using encryption, to decrypt. It is considered virtually impossible to break strong public key encryption without acquiring the private key. Branden M. Palfreyman, 'Lessons from the British and American Approaches to Compelled Decryption' (2007) 75(1) Brooklyn L Rev 345, 350-352; Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999) 36; 'A Deep Dive on End-to-End Encryption: How Do Public Key Encryption Systems Work?' (*Surveillance Self-Defense*, 29 November 2018) <https://ssd.eff.org/en/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work> accessed 12 November 2020.

[10] Gulshan Rai, RK Dubash, & AK Chakravarty, 'Cryptography Technology and Policy Directions in the Context of NII' (1997) Information Technology Group, Department of Electronics Cyberlaw Series 3, Version 1 <https://web.archive.org/web/19990506205823/http:/www.allindia.com:80/gov/doe/cryplaw.htm> accessed 12 November 2020.

[11] Philipp Rogaway. 'The Moral Character of Cryptographic Work' (Asiacrypt, Auckland, December 2015).

[12] James Titcomb, 'What is Encryption, How Does It Work and What Apps Use It?' (*The Telegraph*, 29 March 2017) <https://www.telegraph.co.uk/technology/0/encryption-should-using/> accessed 12 November 2020.

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

ensures that no one other than the sender and the intended recipient, including intermediaries such as the communication service provider itself, can view the information exchanged.[14]

Indian law defines encryption as '[t]he process of transforming plaintext data into an unintelligible form (cypher text) such that the original data either cannot be recovered (one-way encryption) or cannot be recovered without using an inverse decryption process (two-way encryption).'[15]

India does not currently have legislation dedicated to encryption. It is governed largely by sectoral regulations and the Information Technology Act, 2000[16] ('**IT Act**'). The last few decades have witnessed the evolution of the Indian government's approach to encryption with some recent developments reflecting the government's perception of encryption as an obstacle for government agencies.[17]

II. The Trajectory of Encryption Policy in India

Technology policy on matters pertaining to encryption began taking shape in India in the 1990s.[18] The growth of digital banking, electronic commu-

---

accessed 12 November 2020.

[14] Saurabh Sharma, 'End-to-end Encryption: The Heart of Data Security in Today's Digital World' (*Live Mint*, 5 December 2019) <https://www.livemint.com/opinion/columns/end-to-end-encryption-the-heart-of-data-security-in-today-s-digital-world-11575560730299.html> accessed 12 November 2020.

[15] Information Technology (Certifying Authorities) Rules, 2000, sch V.

[16] Information Technology Act, 2000 ('IT Act').

[17] For instance, the traceability mandate under Rule 4(2) of the Information Technology (Intermediaries Guidelines and Digital Media Ethics Code) Rules, 2021; the report by the ad-hoc committee of the Rajya Sabha recommending that law enforcement agencies should be permitted to break end-to-end encryption to trace the distributor of child pornography on social media, *see*: Neha Alawadhi, 'RS Panel Suggests Breaking Encryption to Curb Child Pornography Distribution' (*Business Standard,* 27 January 2020) <https://www.business-standard.com/article/technology/rs-panel-suggests-breaking-encryption-to-curb-child-pornograhy-distribution-120012600705_1.html> accessed 20 July 2021; and statements by the former Minister of Electronics and Information Technology demanding that the origins of messages on end-to-end encrypted platforms should be traceable, *see*: 'Right to Privacy not for those Who Abuse Internet Platform: Ravi Shankar Prasad' (*The New Indian Express*, 14 October 2019) <https://www.newindianexpress.com/nation/2019/oct/14/right-to-privacy-not-for-those-who-abuse-internet-platform-ravi-shankar-prasad-2047531.html> accessed 17 July 2021.

[18] Bedavyasa Mohanty, 'The Encryption Debate in India' (2019) Carnegie Endowment for International Peace, 2 <https://carnegieendowment.org/files/WP_The_Encryption_Debate_in_India.pdf> accessed 12 November 2020. The Indian Telegraph Act, 1885, and the rules thereunder, on the governance of communications are applicable in the context of encryption, even though they were not specifically framed in that regard. For an overview of laws relating to encryption in India, *see*: 'The Road Ahead for Encryption in India' (2020) NASSCOM-DSCI, 29-36 <https://community.nasscom.in/communities/

nication, online intermediaries, and e-commerce led the Indian government to enact the IT Act. The IT Act established a regulatory framework governing the virtual marketplace[19] and introduced a range of e-commerce and internet-related criminal offences.[20] The Act endorsed the use of Public Key Infrastructure (PKI), a system of encryption used for cybersecurity, for secure exchange of data and money.[21] However, as recognized by the Reserve Bank of India (RBI) while issuing guidelines for internet banking,[22] PKI and other sophisticated encryption tools were not commonly available in India then.[23] As a result, the RBI recommended 128-bit Secure Socket Layer (SSL) encryption as an alternative to PKI and to ensure security in online banking, and the Securities Exchange Board of India recommended this standard as the default for e-commerce.[24]

However, subsequently, encryption policy took a turn that reflected governmental concern that encryption will preclude government access to data. The regulatory framework on encryption is now set out simultaneously in the IT Act, the Indian Telegraph Act, 1885[25] ('**Telegraph Act**') as well as sector-specific regulations.[26] These provisions are aimed at specifying the standard of encryption that may be used, permitting decryption by governmental

---

policy-advocacy/nasscom-dsci-discussion-paper-the-road-ahead-for-encryption-in-india.html> accessed 12 November 2020.

19 Khaitan & Co., 'Digital Business in India: Overview' (*Thomson Reuters Practical Law*, 1 February 2017) <https://content.next.westlaw.com/Document/I910e2c5a3b8d11e598dc8b09b4f043e0/View/FullText.html?transitionType=Default&contextData=(sc.Default)&firstPage=true> accessed 12 November 2020.

20 Subhajit Basu and Richard Jones, 'Indian Information and Technology Act 2000: Review of the Regulatory Powers under the Act' (2005) 19(2) Intl Rev L Comp & Tech, 209, 219.

21 IT Act 2000, s 3.

22 'Internet Banking Guidelines' (*Reserve Bank of India*, 14 June 2001) <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=414&Mode=0> accessed 12 November 2020.

23 The lack of domestic capacity in respect of cryptographic software in India in the 1990s could largely be attributed to export controls, *see*: Arun Mohan Sukumar, Wassenaar's Web: A Ahreat to Technology Transfer' (*The Hindu*, 29 March 2016) <https://www.thehindu.com/opinion/columns/wassenaars-web-a-threat-to-technology-transfer/article7499748.ece> accessed 12 November 2020.

24 Committee on Internet based Securities Trading and Services, *First Report* (SEBI 2000) 6-7.

25 The Indian Telegraph Act, 1885 is the primary legislation governing communication in India. It gives the Central Government the exclusive privilege of 'establishing, maintaining and working telegraphs'. Under s 3(1-AA), 'telegraph' is defined as 'any appliance, instrument, material or apparatus used or capable of use for transmission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, visual or other electro-magnetic emissions, Radio waves or Hertzian waves, galvanic, electric or magnetic means'.

26 For instance, the Department of Telecommunications prohibits the use of bulk encryption, *see*: License Agreement for Unified License Agreement, para 37.1.

agencies, and compelling assistance with decryption so the government can gain access.[27]

The IT Act was amended with effect from 2009 to allow the central government to prescribe the modes or methods for encryption for e-governance and e-commerce.[28] Another amendment authorized the central and state governments to intercept, monitor, or decrypt communications in the interest of national security, sovereignty, defence and for the preservation of public order or investigation of an offence.[29] Service providers and subscribers are obligated to assist government agencies with accessing data in this manner.[30]

In the same year, the government enacted the Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules ('**Decryption Rules**').[31] The Decryption Rules set out the parameters and procedures for decryption. End-to-end encrypted platforms are arguably outside the scope of these rules since 'decryption assistance' is defined as assistance to 'allow access, *to the extent possible*, to encrypted information.'[32] The Decryption Rules empower the government[33] to issue an order for decryption for 'any informationas is sent to or from any person or

---

[27] [1] Pranesh Prakash & Japreet Grewal, 'How India Regulates Encryption' (*Center for Internet & Society*, 30 October 2015) <https://cis-india.org/internet-governance/blog/how-india-regulates-encryption> accessed 12 November 2020.

[28] Information Technology Act, 2000, s 84-A.

[29] Information Technology Act, 2000, s 69. A petition challenging the validity of this section is currently pending before the Supreme Court of India, *see*: *Internet Freedom Foundation v Union of India* (WP(C) No 44 of 2019)(pending). Herein, the petitioners approached the Supreme Court invoking its writ jurisdiction, under Article 32 of the Constitution of India, challenging the constitutionality of s 69 of IT Act and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 ('The Decryption Rules') on the grounds that they violate the Right to Equality (art 14), the Right to Freedom of Expression (art 19(1)(a)), and the Right to Privacy (art 21).

[30] Information Technology Act, 2000, s 69.

[31] The Decryption Rules. However, A petition challenging the validity of these Rules is currently pending before the Supreme Court of India, *see: Internet Freedom Foundation v Union of India* (WP(C) No 44 of 2019) (pending). Herein, the petitioners approached the Supreme Court through its writ jurisdiction, under art 32 of the Constitution, challenging the constitutionality of s 69 of IT Act and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 ('The Decryption Rules') on the grounds that they violate the Right to Equality (art 14), the Right to Freedom of Expression (art 19(1)(a)), and the Right to Privacy (art 21).

[32] The Decryption Rules, rule 2(g)(i) (emphasis added).

[33] In December 2018, the Ministry of Home Affairs authorized ten security and intelligence agencies to intercept, monitor and decrypt any information in any computer resource in accordance with the IT Act. *see*: Ministry of Home Affairs, Order dated 20 December 2018 <http://egazette.nic.in/WriteReadData/2018/194066.pdf> accessed 18 November 2020, *see*: The Wire Staff, 'Home Ministry Allows 10 Central Agencies to Engage in Electronic Snooping' (*The Wire*, 21 December 2018) <https://thewire.in/government/home-ministry-allows-10-central-agencies-to-engage-in-electronic-interception> accessed 12 November 2020.

class of persons or relating to any particular subject.'[34] The provision, therefore, covers a wide breadth of information and paves the way for non-targeted or indiscriminate decryption orders. Further, the Decryption Rules require that records pertaining to decryption orders be destroyed within a prescribed period of six months[35] which significantly diminishes the scope for review of the government's exercise of such unilateral power. The government often invokes national security to justify decryption orders.[36]

The first time encryption was openly portrayed as antithetical to national security in India was against the backdrop of the 2008 terror attacks in Mumbai. The government had previously threatened to block Research In Motion (RIM) from the Indian market[37] since the government could not monitor content shared on RIM's BlackBerry devices.[38] The news that those involved in the terror attacks had used BlackBerry devices[39] further intensified the government's antagonistic stance against encryption.[40] After protracted negotiations, RIM agreed to locate BlackBerry servers in India and enabled the government to intercept data of individual users sent over its messaging service, but not corporate customers' data sent over the BlackBerry Enterprise Server systems.[41] The outcome reduced users' privacy resulting from the concern that encryption poses a threat to national security. It is worth noting that intelligence officials were of the view that existing surveillance mechanisms had in fact gleaned sufficient information regarding the

---

[34] The Decryption Rules, rule 9.

[35] The Decryption Rules, rule 23. This provision is often invoked to reject applications under the Right to Information, 2005, regarding the number of decryption orders issued by the government.

[36] The Decryption Rules were framed under s 69, IT Act, which authorizes the central and state governments to intercept, monitor or decrypt communication in the interest of national security, sovereignty, defense and for preservation of public order or investigation of an offence.

[37] 'India Threatens to Shut Down BlackBerry Services' (*Voice of America News*, 11 August 2010) <https://www.voanews.com/east-asia/india-threatens-shut-down-blackberry-services> accessed 12 November 2020.

[38] Because RIM was a device manufacturer, restrictions on encryption standards applicable to telecommunication companies under license agreements were not applicable to RIM.

[39] Damien McElroy, 'Mumbai attacks: Terrorists Monitored British Websites using BlackBerry Phones' (*The Telegraph*, 28 November 2008) <https://www.telegraph.co.uk/news/worldnews/asia/india/3534599/Mumbai-attacks-Terrorists-monitored-coverage-on-UK-websites-using-BlackBerry-phones-bombay-india.html> accessed 12 November 2020.

[40] Sahil Makkar & Shauvik Ghosh, 'India Renews Threat to ban BlackBerry Services' (*LiveMint*, 29 July 2010) <https://www.livemint.com/Home-Page/H0ZmePNYWQk7Tv6NkNAefK/India-renews-threat-to-ban-BlackBerry-services.html>accessed 12 November 2020.

[41] Apurva Chaudhary, 'BlackBerry's Tussle with Indian Govt Finally Ends; BB Provides Interception System' (*Medianama*, 10 July 2013) <https://www.medianama.com/2013/07/223-blackberrys-tussle-with-indian-govt-finally-ends-bb-provides-interception-system/> accessed 12 November 2020.

preparation for the attack; agencies merely failed to put the pieces together.[42] Therefore, the need for creating backdoors to amplify surveillance capabilities and its value to investigations is questionable.

Seven years later, the central government made its first attempt to create a comprehensive policy on encryption. It released a draft National Encryption Policy in 2015[43] and withdrew it within two days in response to severe criticism from a range of stakeholders regarding concerns of privacy and state overreach. The draft had several problematic provisions.[44] For instance, it required users and businesses to retain plain text copies of encrypted communications for 90 days, triggering grave cybersecurity concerns. Further, the government could specify the key length and algorithm to be used in encryption technologies for all users and businesses, leaving no room for users to choose stronger standards, or for businesses to innovate and adopt security measures. An addendum was issued[45] with the aim of mitigating some of the damage. However, a revised draft of the encryption policy has not yet been released.

Most recently, and arguably most problematically, encryption has been in the spotlight in India owing to the notification of the Information Technology (Intermediaries Guidelines and Digital Media Ethics Code) Rules, 2021 ('**New Intermediary Guidelines**') which alter the intermediary liability regime in India.[46] These guidelines mark an important moment in the country's journey on technology policy and may be indicative of greater regulation of encryption, influenced by its perceived hindrance to enabling government access to data. The implementation will impact the economy of the world's largest democracy, and determine in part whether technology strengthens or impedes fundamental rights and freedoms.

---

[42] <https://www.nytimes.com/2014/12/22/world/asia/in-2008-mumbai-attacks-piles-of-spy-data-but-an-uncompleted-puzzle.html>.

[43] Draft Encryption Policy 2015.

[44] 'FAQ: Legal Position of Encryption in India' (*SFLC.in*, 11 November 2017) <https://sflc.in/faq-legal-position-encryption-india> accessed 12 November 2020; Nandita Mathur, 'What was the Draft Encryption Policy and Why it was Withdrawn?' (*LiveMint*, 22 September 2015) <https://www.livemint.com/Politics/RZtAGhM6IjDBWujiK6ysEP/What-was-the-encryption-policy-and-why-it-was-withdrawn.html> accessed 12 November 2020.

[45] The addendum exempted mass use encryption products used in web applications, social media sites, and social media applications such as WhatsApp, Facebook, Twitter etc.; SSL/TLS encryption products used in Internet-banking and payment gateways; and SSL/TLS encryption products being used for e-commerce and password-based transactions.

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

III. The Intermediary Liability Rules: Traceability and the Challenge to Encryption

The New Intermediary Guidelines supersede the Information Technology (Intermediaries guidelines) Rules, 2011, which set out the guidelines that intermediaries were bound to follow under the IT Act. Non-compliance with such guidelines would render intermediaries ineligible for protection under the 'safe harbour' provision – section 79 of the IT Act – which exempts intermediaries from liability for third party content as long as the stated conditions are fulfilled. Because of the extremely limited extent to which social media platforms can moderate user content when it is encrypted end-to-end, strong protection against liability for users' statements on social media platforms is essential to their operation, and to their users' rights to express themselves.

A draft of an amendment to the guidelines that intermediaries are bound to follow was first introduced in 2018 ('**Draft Intermediaries Guidelines**').[47] The Draft Intermediaries Guidelines proposed to impose a new traceability requirement that would severely undermine encryption and jeopardise privacy and security. Online intermediaries[48] such as messaging services and social media networks would be obligated to assist the government with identifying the source of any content when required by the government. This would also have a negative impact on the right to freedom of expression as the threat of losing protection from liability would compel companies to over-comply, to the absolute detriment of users.

When the Draft Intermediaries Guidelines were put through public consultation,[49] civil society, technology companies, and technical experts strongly opposed the traceability mandate,owing to its negative implications for encryption, privacy, and free expression.[50] However, the New Intermediary Guidelines, the revised language of which did not undergo any

---

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

[48] An 'intermediary' is defined extremely broadly under s 2(w) of the IT Act and includes a wide range of services beyond messaging and social media platforms. The definition states: ''intermediary', with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes'.

[49] 'Comments Invited on Draft of Intermediary Guidelines 2018' (*Ministry of Electronics & Information Technology*, 2018) <https://www.meity.gov.in/comments-invited-draft-intermediary-rules> accessed 8 March 2021.

[50] 'Public Comments on Draft Intermediary Guidelines Rules, 2018' (*Ministry of Electronics & Information Technology*, 2018) <https://www.meity.gov.in/writereaddata/files/public_comments_draft_intermediary_guidelines_rules_2018.pdf> accessed 8 March 2021.

public consultation, continue to impose a problematic traceability mandate, albeit different from the traceability mandate in the Draft Intermediaries Guidelines.

The traceability provision in Rule 4(2) of the New Intermediary Guidelines is applicable to any 'significant social media intermediary'(SSMI) providing services primarily in the nature of messaging. An SSMI is defined as 'a social media intermediary having number of registered users in India above such threshold as notified by the Central Government.'[51] The central government has set this threshold at 50 lakh (5 million) users.[52] The New Intermediary Guidelines also empower the government to require any intermediary, which is not an SSMI, to comply with the traceability requirements and the other obligations set out in Rule 4.[53]

The traceability provision obligates SSMIs and such other intermediaries as are designated by the government to enable the identification of the 'first originator' of any information as may be required by a judicial order or an order passed under section 69 of the IT Act, if certain conditions are met. Section 69 empowers the Central and State Governments, or any of their authorized officers, to direct any government agency to monitor, intercept or decrypt information.[54] Such an order requiring identification of the first originator has to be passed for the purposes of prevention, detection, investigation, prosecution or punishment of an offence, or incitement of an offence, pertaining to the sovereignty, integrity, and security of the state, foreign relations, public order, rape, sexually explicit material or child sexual abuse material, punishable with imprisonment for at least five years. Rule 4(2) also states that where other less intrusive means are effective in identifying the originator, a traceability order shall not be passed[55] and compliance with an order would not require disclosure by the SSMI of the content of any

---

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

[52] Ministry of Electronics and Information Technology, Notification Dated 25 February 2021 <https://www.meity.gov.in/writereaddata/files/Gazette%20Significant%20social%20media%20threshold.pdf> accessed 12 November 2020.

[53] New Intermediary Guidelines, rule 6.

[54] In terms of Rule 2(d) of the Decryption Rules, the 'competent authority' for issuing such orders is the Secretary in the Ministry of Home Affairs, in case of the Central Government; or the Secretary in charge of the Home Department, in case of a State Government.

[55] It is worth noting that this limitation applies at the stage of the order being passed by a court or an authorized government agency. These authorities, which do not possess the technical expertise to determine whether other less intrusive measures are available, would not have the benefit of receiving representations from experienced professionals or the intermediary that would have to comply with the order. An intermediary does not have an opportunity to present alternate means that are less intrusive. The practical value of this limitation is therefore limited and will likely not meaningfully restrict the number of such orders that are passed.

message. Finally, where the first originator is located outside India, the first originator within India would be deemed the first originator for the purpose of the clause.

The New Intermediary Guidelines were introduced with the purported aim of preventing the misuse of social media by criminals and 'anti-national elements'[56] and combating the spread of fake news[57] online.[58] These are undeniably important concerns impacting jurisdictions around the world. However, undermining encryption by mandating traceability is not a legitimate solution and none of the asserted goals are demonstrable or provable outcomes of such a measure. As the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has said, governments 'have not demonstrated that criminal or terrorist use of encryption serves as an insuperable barrier to law enforcement objectives'.[59] Traceability is not a viable solution because, as WhatsApp has argued, it would not correctly identify the originator of content given how users typically use the internet.[60] It would facilitate the attribution of unlawful content

---

[56] The term 'anti-national elements' mentioned in the press release accompanying the Draft IT rules has no legal definition. 'Draft IT rules issued for public consultation' (Ministry of Electronics & Information Technology, 24 December 2018) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1557159> accessed 12 November 2020.

[57] 'Fake news' in itself is a dubious term that lacks an agreed upon definition. Premising the traceability requirement on the goal of fighting the ambiguous conception of 'fake news' exacerbates the provision's potential to thwart the freedom of expression and impinge upon the right to privacy. Human rights experts, including the UN Special Rapporteur on Freedom of Opinion and Expression, have warned that restrictions on the dissemination of information predicated on vague concepts such as 'fake news' should be abolished as they are incongruous with international standards on freedom of expression, *see*: UNSRFOE, OSCE & OAS, 'Joint declaration on freedom of expression and 'fake news', disinformation and propaganda' (2017).

[58] 'Government notifies Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021' (*Ministry of Information & Broadcasting*, 25 February 2021) <https://www.pib.gov.in/PressReleseDetail.aspx?PRID=1700766> accessed 8 March 2021.

[59] *See*: UNHRC 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (22 May 2015) A/HRC/29/32; Soumyarendra Barik, 'Encryption and Issues Related to Misinformation' (*Medianama*, 15 June 2020) <https://www.medianama.com/2020/06/223-encryption-misinformation/> accessed 12 November 2020; 'Fact Sheet: Intermediaries and Encryption' (*Internet Society*, 2 June 2020) <https://www.internetsociety.org/resources/doc/2020/fact-sheet-intermediaries-and-encryption/> accessed 12 November 2020.

[60] *See* WhatsApp's response to a proposal in *Antony Clement Rubin v Union of India* 2018 SCC OnLine Mad 13519 before the Madras High Court on enabling traceability without compromising E2EE, *see*: Aditi Agarwal, 'Exclusive: WhatsApp's Response to Dr. Kamakoti's Recommendation for Traceability in WhatsApp' (*Medianama*, 21 August 2019) <https://www.medianama.com/2019/08/223-exclusive-whatsapps-response-kamakotis-submission/> accessed 26 July 2021; *see also* 'What is Traceability and why does WhatsApp Oppose it?' (*WhatsApp*) <https://faq.whatsapp.com/general/

to innocent users by bad actors, and subject innocent users to investigation and prosecution for having shared content for purely legitimate concerns.[61]

The ambiguity surrounding who might be considered the 'first originator' in practice exacerbates the potential for an adverse impacton user. Is the 'first originator' the person who first sent the information on the platform that is subject to the traceability requirement? Or is the 'first originator' the first person to send the information in a particular chain of communications carried on the platform, even if the same information was sent across multiple communications chains on the same platform, in which case there would be numerous 'first originators' of the same information? For instance, a WhatsApp or Signal user who shares a screenshot of a tweet for the first time on the platform, may not in fact be the first originator of that content. Further, content on messaging platforms often has several different branches and sources. For instance, user A was the first to share it on the platform with user B. Thereafter, at a later stage, user C, having obtained the content from elsewhere and not from users A or B, shares it with multiple other users after which the content becomes viral. In such cases, it is not clear under the New Intermediary Guidelines who the 'first originator' of the content is, who presumably would be held accountable for it. Such ambiguity may stifle expression by creating concern that a user might be regarded as a 'first originator' when in fact they might not be so.

Traceability requirements can also erode user privacy and lack effectiveness, as illustrated by the expert analysis that Dr. Prabhakaran submitted to the Madras High Court.[62] He argued that traceability is not a demonstrable deterrent as is apparent from the ubiquity of fake news on social media platforms and that it has limited utility until untraceable messaging services become prevalent. Further, he argued that phone numbers have little identification value and equally, tracing the originator of the content does not have

---

security-and-privacy/what-is-traceability-and-why-does-whatsapp-oppose-it/?lang=en> accessed 26 July 2021.

[61] *See* WhatsApp's response to a proposal in *Antony Clement Rubin v Union of India* 2018 SCC OnLine Mad 13519 before the Madras High Court on enabling traceability without compromising E2EE, *see*: Aditi Agarwal, 'Exclusive: WhatsApp's Response to Dr. Kamakoti's Recommendation for Traceability in WhatsApp' (*Medianama*, 21 August 2019) <https://www.medianama.com/2019/08/223-exclusive-whatsapps-response-kamakotis-submission/> accessed 12 November 2020.

[62] Dr. Prabhakaran, On a Proposal for Originator Tracing in WhatsApp, *Antony Clement Rubin v Union of India* 2018 SCC OnLine Mad 13519. Dr Prabhakaran submitted his expert analysis on behalf of the Internet Freedom Foundation, which was made an intervener in the case, in response to Dr Kamakoti's proposal, *see*: <https://drive.google.com/file/d/1B2ShWywwVpPX1zTz25UgPMSOokZbcJBx/view>;

any practical value.[63] Most importantly, the negative impact of compromising encryption on privacy and security is immense and inevitable and far outweighs any perceived benefit.

How a Traceability Requirement Undermines Encryption

Encryption evolved as a technological tool that facilitates the realization of a basic human need – to communicate without being overheard – and enabled a vast array of valuable commercial and financial services. However, law enforcement agencies and governments often view the use of encryption, particularly E2EE, as causing a 'going dark' problem whereby information is obscured in ways that the government's ability to access data is reduced.[64,65] Governments around the world have called for encryption 'backdoors' that would allow government entities and law enforcement agencies to circumvent

---

[63] Dr. Prabhakaran, On a Proposal for Originator Tracing in WhatsApp, *Antony Clement Rubin v Union of India* 2018 SCC OnLine Mad 13519, *see*: <https://drive.google.com/file/d/1B2ShWywwVpPX1zTz25UgPMSOokZbcJBx/view>; Aditi Agarwal, 'Kamakoti's Proposals will Erode User Privacy, Says IIT Bombay Expert in IFF Submission' (*Medianama*, 27 August 2019) <https://www.medianama.com/2019/08/223-iff-response-kamakoti-submission-traceability-2/><https://www.medianama.com/2019/08/223-iff-response-kamakoti-submission-traceability-2/>

[64] James B. Comey, 'Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy' (*Federal Bureau of Investigation*, 8 July 2015) <https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy> accessed 12 November 2020; Bedavyasa Mohanty, "Going Dark' in India: The Legal and Security Dimensions of Encryption' (*Observer Research Foundation*, 13 December 2016) <https://www.orfonline.org/research/going-dark-in-india-the-legal-and-security-dimensions-of-encryption/> accessed 12 November 2020; 'Going Dark – Implications of an Encrypted World' (2019) Center for Advanced Studies on Terrorism <https://nsiteam.com/social/wp-content/uploads/2019/07/Going-Dark-Implications-of-an-Encrypted-World-Rev.-3.0-compressed.pdf> accessed 12 November 2020.

[65] It has been argued that this characterization is in fact highly inaccurate. In reality, far from engendering a 'going dark' problem, new technology has in fact enabled a 'golden age of surveillance' by adding an abundance of new vectors of information, see: 'Don't Panic: Making Progress on the 'Going Dark' Debate' (2016) The Berkman Center for Internet & Society <https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf> accessed 12 November 2020; Peter Swire, "Going Dark' Versus a 'Golden Age for Surveillance'' (Center for Democracy & Technology, 28 November 2011) <https://cdt.org/insights/%e2%80%98going-dark%e2%80%99-versus-a-%e2%80%98golden-age-for-surveillance%e2%80%99/> accessed 12 November 2020; Peter Swire & Kenesa Ahmad, 'Encryption and Globalization' (2012) 23 Columbia Sci & Tech L Rev 416, 463-473.

the authentication process and intercept encrypted communications.[66,67] Attacks on encryption by governments typically take either the form of proposed laws requiring intermediaries to build technical capabilities to decrypt data and assist the government with access[68] or laws imposing a traceability requirement such as the one under the New Intermediary Guidelines.[69]

The Indian government has so far proposed two methods for implementing the traceability mandate;[70] (a) Dr. Kamakoti's proposal[71] which entails tagging each message on the E2EE platform with the originator's information;[72] and (b) using a catalogue of alpha-numeric hashes maintained by the intermediary to compare the hash of the problematic message.[73]

a. Message Tagging Model: Dr. Kamakoti's proposal envisages two levels of encryption on an E2EE platform. The content of the message would be encrypted, as it currently is. Separately, the originator's information would also be encrypted and tagged with the message. Platforms would be required to retain the decryption key to the originator's information in an escrow. A

---

66 Five Country Ministerial, 'Joint Meeting of FCM and Quintet of Attorneys-General' <https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety>; <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822818/Joint_Meeting_of_FCM_and_Quintet_of_Attorneys_FINAL.pdf> accessed 18 November 2020.

67 These statements acknowledge the importance of encryption for security and privacy but require companies to institute mechanisms that would create backdoors for the government. The creation of such backdoors fundamentally destroys the privacy promise of encryption as there is no such thing as a backdoor only for good actors – the same backdoors can be exploited by malicious actors and repressive regimes. The statements are therefore self-contradicting and based on an inaccurate understanding of how encryption works.

68 Examples: Australia, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018; United Kingdom, Investigatory Powers Act 2016; and United States of America, Proposed Lawful Access to Encrypted Data Bill (S. 4051, 116th Cong.) 2020.

69 The proposed Brazilian Internet Freedom, Responsibility and Transparency Act, known as the 'Fake News Bill', initially imposed a traceability mandate. It was removed following public criticism.

70 Aditi Agarwal, 'Traceability and end-to-end encryption cannot co-exist on digital messaging platforms: Experts' (*Forbes India*, 16 March 2021) accessed 30 July 2021.

71 Dr. V Kamakoti, Report on Originator Traceability in WhatsApp Messages, *Antony Clement Rubin v Union of India* 2018 SCC OnLine Mad 13519, <https://www.medianama.com/wp-content/uploads/Dr-Kamakoti-submission-for-WhatsApp-traceability-case-1.pdf> accessed 3 May 2021.

72 Dr. V Kamakoti, Report on Originator Traceability in WhatsApp Messages, *Antony Clement Rubin v Union of India* 2018 SCC OnLine Mad 13519, <https://www.medianama.com/wp-content/uploads/Dr-Kamakoti-submission-for-WhatsApp-traceability-case-1.pdf> accessed 3 May 2021.

73 Surabhi Agarwal, 'Govt Proposes Alpha-Numeric Hash to Track WhatsApp Chat' (*ET CIO*, 23 March 2021) <https://cio.economictimes.indiatimes.com/news/social-media/govt-proposes-alpha-numeric-hash-to-track-whatsapp-chat/81643144> accessed 3 May 2021.

government agency would approach such an intermediary with the necessary order, when investigating a problematic message, to decrypt the originator's information.

Dr. Kamakoti recommended that messages should be marked as either 'forwardable' or 'not-forwardable' to account for users' consent. If a user marks a message as 'forwardable' they consent to their information being tagged with the message as the originator. Whereas if a user tags a message as 'non-forwardable' and the recipient forwards it, the recipient who forwards the 'non-forwardable' message becomes the originator.

The practical effectiveness of this proposal is highly suspect. The originator's information would only travel with the message for the purpose of traceability when it is simply forwarded on the same platform. The function would be futile if any other form of sharing is used. For instance, if a user copies and pastes the message, or adds a caption to an image or a video before sharing it, or sharesa screenshot of the message, the originator would change. Further, the focus on forwarded messages ignores the fact that the intent and context with which the message was shared, by any user along the message's travel footprint, cannot be discerned. For example, a user could forward a message and in the next moment, send a second message to the recipients of the forwarded message that debunks it. At the very least, if implemented, this proposal will deter users from sharing information and communicating freely and in the worst-case scenario, it will result in attributing culpability to the wrong people and for the wrong reasons.

A technical measure such as this, which requires the retention of a decryption key in an escrow is fundamentally contrary to E2EE. The inability of the intermediary to access any encrypted information linked to the messages circulating on its platform is central to E2EE. The storage of such a key also makes intermediaries and users' information extremely vulnerable to attacks and undermines the practice of data minimization for privacy and security.

When the originators' identity is permanently linked to a message, users' anonymity and privacy are compromised and this causes a chilling effect on the right to freedom of expression. The traceability model will deprive users of safe spaces for communication and information-sharing on the internet. For a model whose effectiveness is purely theoretical, it carries far too great a threat to data security and users' fundamental rights and freedoms.

b. Message hashing model: The other model of implementing traceability would involve requiring platforms to maintain a library of alpha-numeric hashes of all messages sent on their platforms. It was advocated by Rakesh

Maheshwari, senior director and group co-ordinator of cyberlaw and eSecurity at MeitY.[74] Hashing is a mathematical process of attaching a piece of data with a fixed value.[75] This is typically used to verify the authenticity of data, including for password verification. The government wants WhatsApp and other E2EE platforms to assign an alpha-numeric hash to every single message on their platform. For instance, the hash value of a message that reads 'Good Morning' may be '4ch77da'. The government's demand is that the intermediary must maintain a library of hashes associated with each message so that the originator of problematic content can be traced when the problematic content is presented to the platform.[76]

This proposal is technically infeasible. It rests on the assumption that the hash value of a message remains constant if the content is unchanged. However, on E2EE platforms like WhatsApp and Signal, the generation of a hash value also accounts for the unique identity of the sender and the recipient.[77] Therefore, the hash value of the message 'good morning' from user A to B changes when user B forwards the same 'Good Morning' to user C. An investigation into the 'Good Morning' from user B to C would not reveal the involvement of user A at all.[78] This is because WhatsApp and Signal have a forward secrecy feature enabled by the double ratchet algorithm which

---

[74] New IT Rules: Empowering Control or Controlled Empowerment? Deciphering the Intermedia (CCAOI India, 4 March 2021) <https://www.youtube.com/watch?v=E8wk-fidXaWs> accessed 3 May 2021; Surabhi Agarwal, 'Govt Proposes Alpha-Numeric Hash to Track WhatsApp Chat' (*ET CIO*, 23 March 2021) <https://cio.economictimes.indiatimes.com/news/social-media/govt-proposes-alpha-numeric-hash-to-track-whatsapp-chat/81643144> accessed 3 May 2021.

[75] Mehab Quresi, 'What is hashing & why does Indian govt want WhatsApp to use it?' (*The Quint*, 25 March 2021) <https://www.thequint.com/tech-and-auto/what-are-hashes-and-why-does-india-wants-whatsapp-to-implement-them#:~:text=Hashing%20is%20a%20process%20where,be%20easily%20traced%20when%20needed.&text=The%20Indian%20government%20wants%20WhatsApp%20to%20implement%20traceability%20in%20its%20services.> accessed 3 May 2021.

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

[77] *See* Amit Panghal, 'WhatsApp's End to End Encryption, How does it work?' (*Medium*, 6 October 2018) <https://medium.com/@panghalamit/whatsapp-s-end-to-end-encryption-how-does-it-work-80020977caa0> accessed 26 July 2021; *see also* 'WhatsApp Encryption Overview – Technical White Paper' (*WhatsApp*, 22 October 2020) <https://scontent.whatsapp.net/v/t39.8562-34/122249142_469857720642275_2152527586907531259_n.pdf/WA_Security_WhitePaper.pdf?ccb=1-3&_nc_sid=2fbf2a&_nc_ohc=ObtXRc807aoAX-KKts4&_nc_ht=scontent.whatsapp.net&oh=554bfa3edd8370b7da89ab37be249187&oe=61026BD9> accessed 26 July 2021.

[78] Aditi Agarwal, 'Traceability and End-to-End Encryption Cannot Co-exist on Digital Messaging Platforms: Experts' (*Forbes India*, 16 March 2021) accessed 3 May 2021.

essentially changes the key between two users for each message.[79] Enabling traceability in the way the government proposes would require WhatsApp and Signal to give up forward secrecy, a vital feature of E2EE. It would also mean that the intermediaries would then be able to track the entire chain of each communication on its platform which is antithetical to E2EE.

Further, the slightest change in the content of a message would alter its hash value. For instance, the hash of a message that reads 'Good Morning' will be different from the hash of 'Good Morning…'.Similarly, if user A sends the same message to user B twice, the double ratchet algorithm ensures that the hash value of each of those messages is different, despite the identical content.[80] This will make it practically impossible to trace a message back to the first originator with the use of alpha-numeric hashes on an E2EE system. The practical infeasibility of this proposal is also exacerbated by the sheer volume of messages that would have to be hashed, and the size of the hash library that would have to be maintained. Billions of messages are sent on WhatsApp every minute.[81] Message hashes would have to be stored for years in order to facilitate traceability for crimes associated with a message that are committed or prosecuted years later. Intermediaries that have large message volume cannot reasonably be expected to create the ability to store hashes and track each message. Even if this ability were to be developed somehow, such extensive storage would be violative of data minimization principles.

Dr. Debayan Gupta, cryptographer and assistant professor of computer science at Ashoka University, is firmly of the view that E2EE is compromised the moment anyone except the sender and recipient can tell which message was sent to whom: 'On an end-to-end encrypted platform, if I have an option of sending a message 'abc' or 'def', nobody except the recipient should be able to tell which of the two was sent.'[82] At present, the 'forward' icon on WhatsApp serves to mark the message on the receiver's phone as having been 'forwarded' and count if it has been forwarded more than five

---

[79] Trevor Perrin and Moxie Marlinspike, 'The Double Ratchet Algorithm' (*Signal*, 20 November 2016) <https://signal.org/docs/specifications/doubleratchet/ > accessed 3 May 2021.

[80] *See* Trevor Perrin and Moxie Marlinspike 'The Double Ratchet Algorithm' (*Signal*, 20 November 2016) <https://signal.org/docs/specifications/doubleratchet/> accessed 26 July 2021.

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

[82] Aditi Agarwal, 'Traceability and End-to-End Encryption cannot Co-exist on Digital Messaging Platforms: Experts' (*Forbes India*, 16 March 2021) accessed 3 May 2021.

times.[83] WhatsApp itself does not know how many times a message has been forwarded.[84]

According to Dr. Debayan Gupta, E2EE breaks the moment something is attached to a message which can be tracked by the service provider – such as the originator's information in Dr. Kamakoti's proposal. Each of the proposed models for traceability is inconsistent with a communications service that is fully encrypted end-to-end. Thus, each would weaken the protections that encryption provides, and is incongruous with users' expectations about the privacy and confidentiality of their communications in an encrypted environment. E2EE platforms would have to fundamentally alter their architecture to eliminate the very features that prioritize privacy and security and inspire users' trust.[85]

The utility of techniques that providers are likely to pursue in order to implement a traceability requirement, such as tagging the originator's information with each message and maintaining a library of hashes to trace messages back to their originators is unclear.[86] This might result in intermediaries being compelled to implement an alternate model with backdoors

---

[83] 'FAQ: How to Forward Messages' (*WhatsApp*) <https://faq.whatsapp.com/web/chats/how-to-forward-messages/?lang=en> accessed 12 November 2020; 'FAQ: About Forwarding Limits' (*WhatsApp*) <https://faq.whatsapp.com/general/chats/about-forwarding-limits/?lang=en> accessed 24 February 2021. WhatsApp marks a message that is five forwards away from its original sender with a 'Forwarded many times' icon. Such messages can then only be forwarded to one chat at a time.

[84] 'FAQ: About Forwarding Limits' (*WhatsApp*) <https://faq.whatsapp.com/general/chats/about-forwarding-limits> accessed 24 February 2021; 'FAQ: Coronavirus Product Changes- About Forwarding Limits' (*WhatsApp*) <https://faq.whatsapp.com/general/coronavirus-product-changes/about-forwarding-limits> accessed 12 November 2020; Katitza Rodriguez & Seth Schoen, 'FAQ: Why Brazil's Plan to Mandate Traceability in Private Messaging Apps will Break User's Expectation of Privacy and Security' (*Electronic Frontier Foundation*, 7 August 2020) <https://www.eff.org/deeplinks/2020/08/faq-why-brazils-plan-mandate-traceability-private-messaging-apps-will-break-users> accessed 12 November 2020.

[85] WhatsApp's submission in a case before the Madras High Court that considers the issue of traceability. WhatsApp stated that a traceability mandate would force WhatsApp to fundamentally change its platform and undermine E2EE. The case has been transferred and is now pending in the Supreme Court of India, *see*: *Antony Clement Rubin & Janani Krishnamurthy v Union of India* (TP (C) 1943-46/2019); Aditi Agarwal, 'Exclusive: WhatsApp's Response to Dr Kamakoti's Recommendation for Traceability in WhatsApp' (*Medianama*, 21 August 2019) <https://www.medianama.com/2019/08/223-exclusive-whatsapps-response-kamakotis-submission/> accessed 12 November 2020; Aditi Agarwal, 'Kamakoti's Proposals will Erode user Privacy, says IIT Bombay Expert in IFF Submission' (*Medianama*, 27 August 2019) <https://www.medianama.com/2019/08/223-iff-response-kamakoti-submission-traceability-2/>.

[86] Internet Society, Traceability and Cybersecurity: Experts' Workshop Series on Encryption in India, <https://www.internetsociety.org/resources/doc/2020/traceability-and-cybersecurity-experts-workshop-series-on-encryption-in-india/#_ftnref2> accessed 23 February 2021.

to encryption in order to remain eligible for safe harbour protection and steer clear of liability. The New Intermediary Guidelines essentially present intermediaries with a Hobson's choice – they may either retain design components that strengthen privacy and security or expose themselves to liability. To penalize platforms for choosing to prioritize users' rights and freedoms is patently undemocratic.

Government officials are likely to point to the third proviso in the traceability provision in the New Intermediary Guidelines as they argue that the New Intermediary Guidelines do not undermine encryption. It states that 'in complying for an order for identification of the first originator, no significant social media intermediary shall be required to disclose the contents of any electronic message.'[87] This proviso offers little reassurance with respect to the inviolability of the encrypted message. First, in most cases, if the government is seeking to trace the first originator of a problematic message, government officials must already have access to the content of the relevant message. Second, there is a distinction between not requiring intermediaries to 'disclose' the content of a message, and not requiring intermediaries to be able to 'access' the content at all.

The second proviso, which states that a traceability order shall not be passed where other less intrusive means are effective in identifying the originator of the information, also fails to serve as a meaningful limitation. This limitation applies at the stage of the order being passed by a court or an authorized government agency. These authorities, which do not possess the technical expertise to determine whether other less intrusive measures are available, would not have the benefit of receiving representations from experienced professionals or the intermediary that would have to comply with the order. An intermediary is not granted an opportunity to present alternate means that are less intrusive. Therefore, the practical value of this limitation is therefore limited and will likely not meaningfully restrict the number of such orders that are passed.

A more meaningful limitation would exempt SSMIs from complying with a traceability order if the only technically feasible method of doing so would require the implementation of a new mechanism that enables access to end-to-end encrypted content. Implementation of the traceability requirement by tagging originator's information or using alpha-numeric hashes or other methods involving digital attribution through signatures associated with

[87] New Intermediary Guidelines, rule 4(2).

every message[88] and increased collection and storage of metadata[89] is not fully reliable and is vulnerable to impersonation and misuse by bad actors. It can therefore result in false attributions.

Further, even in circumstances where access to the content of messages is not required by the government, the traceability mandate, as set out in the New Intermediary Guidelines, would still undermine encryption. Representatives of the Ministry of Electronics and Information Technology have stated that only the metadata relating to the first originator will be tracked, and not that relating to the entire chain of communication.[90] However, this is not practically feasible. For instance, the fourth proviso to Rule 4(2) provides that where the first originator of content is outside India, the first originator within India will be deemed the first originator for the purpose of this clause. This can arguably not be done without tracking the entire chain of communication,[91] or at least the chain until the message reaches a user located in India. Thus, re-engineering of the platform to enable capturing substantially more metadata and tracking of entire chains of communications could become necessary for compliance. The introduction of features that enable access to and storage of more information about users and their communications is synonymous with the introduction of weaknesses that will make sensitive data vulnerable to unauthorized access by third parties. The direct result, whether intended or unintended,will be an erosion of the data minimization principle as platforms are compelled to track and store more data, and an overall weakening of the privacy and security features that constitute the core tenets of E2EE platforms enabling secure communication.

---

[88] Megha Mandavia, 'India asks WhatsApp to Fingerprint Messages to Ensure Traceability' (*The Economic Times*, 18 June 2019) <https://tech.economictimes.indiatimes.com/news/mobile/india-asks-whatsapp-to-fingerprint-messages-to-ensure-traceability/69833913> accessed 12 November 2020; Shweta Ganjoo, 'WhatsApp Maintains its Stand on Govt's Request for Message Traceability in India' (*India Today*, 18 June 2019) <https://www.indiatoday.in/technology/news/story/whatsapp-maintains-its-stand-on-govt-s-request-for-message-traceability-in-india-1551098-2019-06-18> accessed 12 November 2020.

[89] Increased metadata collection to implement traceability would be contrary to data minimization and privacy by design principles and create security risks owing to longer retention of data.

[90] New IT Rules: Empowering Control or Controlled Empowerment? Deciphering the Intermedia (CCAOI India, 4 March 2021) https://www.youtube.com/watch?v=E8wkfidX-aWs accessed 8 March 2021.

[91] 'What is the Originator or Traceability provision in the Information Technology (Intermediary Guidelines and Digital Media Ethics Code), 2021?' (*SFLC.in*, 12 April 2021) <https://sflc.in/what-originator-or-traceability-provision-information-technology-intermediary-guidelines-and> accessed 11 May 2021.

Among the most popular examples of E2EE platforms in India are WhatsApp with 400 million users as of July 2019,[92] and Signal with 26.4 million downloads within two weeks in January 2021 and a projected growth of up to 200 million users in the next two years.[93] WhatsApp and Signal have a security by default design that ensures that no third party, not even WhatsApp and Signal, can access the messages, photos, videos, voice messages, documents, and calls exchanged on the platform.[94] Further, Signal can only access the date and time a user registered with Signal and the last date of a user's connectivity to the Signal service.[95] This prevents the storage of hashes and the attribution of the originator's information to each message, as envisioned in the leading traceability implementation proposals. Such features that strengthen privacy and security will be severely undermined by the New Intermediary Guidelines. WhatsApp, Signal,and other E2EE platforms would have to be redesigned to either weaken encryption or introduce backdoors that would effectively destroy E2EE.[96]

Irrespective of how intermediaries' systems are re-engineered to comply with the traceability requirement, the result will be a blow to encryption that steers technology away from formats that focus on privacy and respect data-minimization principles. The traceability mandate would compel a drastic alteration of such privacy-by-design architecture and expose to service providers of E2EE platforms, and potentially other parties, information that has hitherto been private.

The Negative Impact of Traceability on Cybersecurity

Once the ability to trace the origin of a thread of communication has been created and encryption is weakened, there is no fail-safe method of ensuring

---

[92] Prasid Banerjee, 'WhatsApp Announces 2 Billion Users Worldwide' (*LiveMint*, 12 February 2020) <https://www.livemint.com/technology/tech-news/whatsapp-announces-2-billion-users-worldwide-11581516342061.html> accessed 12 November 2020.

[93] Prasid Banerjee, 'Signal Logs in 26.4 Million Downloads in India in Less than Two Weeks' (*LiveMint*, 19 January 2021) <https://www.livemint.com/technology/tech-news/signal-logs-in-26-4-million-downloads-in-india-in-less-than-two-weeks-11611053954964.html> accessed 7 April 2021; 'Signal Targets 100-200 mn users in India: Brian Acton' (*National Herald*, 13 January 2021) <https://www.nationalheraldindia.com/science-and-tech/signal-targets-100-200-mn-users-in-india-brian-acton> accessed 7 April 2021.

[94] 'WhatsApp Security' (*WhatsApp*) <https://www.whatsapp.com/security/> accessed 7 April 2021; 'Is it private? Can I Trust it?' (*Signal*) <https://support.signal.org/hc/en-us/articles/360007320391-Is-it-private-Can-I-trust-it-> accessed 7 April 2021.

[95] 'Grand Jury Subpoena for Signal user Data, Eastern District of Virginia' (*Signal*) <https://signal.org/bigbrother/eastern-virginia-grand-jury/> accessed 7 April 2021.

[96] 'Building Traceability would Undermine End-to-End Encryption WhatsApp' (*The Economic Times*, 24 August 2018) <https://economictimes.indiatimes.com/tech/internet/building-traceability-would-undermine-end-to-end-encryption-whatsapp/articleshow/65515114.cms?from=mdr>accessed 7 April 2021.

that only the intended party, whether it is the service provider or the government, will be able to exploit the mechanism that facilitates traceability. The requirement of building a capability to allow government access to encrypted information online would essentially amount to mandating insecurity.[97] It is technologically impossible to create a backdoor that works only for legitimate actors or the 'good guys.'[98] E2EE platforms are valuable precisely because they keep information exchanged between parties secure indiscriminately from *all* third parties, including the one that created and makes the platform available, and therefore provide robust protection for information online and internet users' right to privacy. Once a vulnerability has been introduced into the system, it significantly aggravates the risk of data breaches and malicious attacks.[99] Therefore weakening security on the internet with the aim of strengthening national security is counter-logical. It would also be contrary to the provision in the New Intermediary Guidelines which requires intermediaries to take all reasonable measures to secure information.[100]

Further, the blanket assumption that the government is a 'good' actor is inherently flawed. Repressive governments often use surveillance to monitor citizens' actions[101] and encryption offers a degree of freedom from such sur-

---

[97] Hareld Abelson, Daniel Weitzner, et al, 'Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications' (2015) Computer Science and Artificial Intelligence Laboratory Technical Report MIT-CSAIL-TR-2015-026 <https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8&isAllowed=y> accessed 12 November 2020.

[98] Charles Duan, Arthur Rizer, Zach Graves & Mike Godwin, 'Policy Approaches to the Encryption Debate' (2018) R Street Policy Study 133/2018 <http://2o9ub0417chl2l-g6m43em6psi2i.wpengine.netdna-cdn.com/wp-content/uploads/2018/03/133.pdf> accessed 12 November 2020; Amie Stepanovich & Michael Karanicolas, 'Why an Encryption Backdoor for Just the 'Good Guys' Won't Work' (*Just Security*, 2 March 2018) <https://www.justsecurity.org/53316/criminalize-security-criminals-secure/> accessed 12 November 2020; Steve Morgan, 'Apple's CEO on Encryption: 'You can't have a Back Door that's Only for the Good Guys'' (*Forbes*, 21 November 2015) <https://www.forbes.com/sites/stevemorgan/2015/11/21/apples-ceo-on-encryption-you-cant-have-a-back-door-thats-only-for-the-good-guys/#44910af8483a> accessed 12 November 2020.

[99] ibid.

[100] New Intermediary Guidelines, rule (3)(1)(i).

[101] Endalkachew Chala, 'Defending Against Overreaching Surveillance in Ethiopia: Surveillance Self-Defense now available in Amharic' (*Electronic Frontier Foundation*, 1 October 2015) <https://www.eff.org/deeplinks/2015/09/defending-against-overreaching-surveillance-ethiopia-surveillance-self-defense-n-0> accessed 12 November 2020; ANI, 'China Uses Tech as Tool of Repression to Monitor Citizens: US Commission' (*LiveMint*, 9 August 2020) <https://www.livemint.com/news/world/china-uses-tech-as-tool-of-repression-to-monitor-citizens-us-commission-11596931164736.html> accessed 12 November 2020; for a global overview, *see*: Adrian Shahbaz, 'The Rise of Digital Authoritarianism' (*Freedom House*, 2018) <https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism> accessed 12 November 2020.

veillance.[102] Traceability would empower repressive regimes with the ability to ascertain who interacted with a particular message that expressed dissent or encouraged protest, irrespective of the context in which they did so. Particularly in a democracy, the right to privacy is inextricably linked to the growth of a society that fosters the freedom of expression and facilitates inclusive growth.[103]

Traceability's Impact on the Fundamental Right to Privacy

The traceability requirement, in permanently attributing an identity to a private communication, would jeopardise the right to privacy[104] of internet users and thwart their right to freedom of expression,[105] both of which are fundamental rights under the Constitution of India. Anonymity, privacy, and free expression are inextricably linked and instrumental to the establishment of a healthy democratic society.[106] As former UN Special Rapporteur on Freedom of Expression Frank La Rue notes, 'throughout history, people's willingness to engage in debate on controversial subjects in the public

---

[102] ibid; R Street Paper; Andy Greenberg, 'Encryption App 'Signal' Is Fighting Censorship with a Clever Workaround' (*Wired*, 21 December 2016) <https://www.wired.com/2016/12/encryption-app-signal-fights-censorship-clever-workaround/> accessed 12 November 2020.

[103] Lord Bauer, Ramon Diaz, et al, *Freedom, Democracy and Economic Welfare: Proceedings of an International Symposium* (Fraser Institute 1986) 96-100; 'Keystones to foster inclusive Knowledge Societies: Access to information and knowledge, Freedom of Expression, Privacy, and Ethics on a Global Internet' (2015) United Nations Educational, Scientific, and Cultural Organization Draft Study, 7 <https://unesdoc.unesco.org/ark:/48223/pf0000232563> accessed 12 November 2020.

[104] In *K.S. Puttaswamy v Union of India* (2017) 10 SCC 1, a nine-judge bench of the Supreme Court of India unanimously held that the right to privacy is protected under the fundamental rights and freedoms set out in Part III of the Constitution of India. Several petitions challenging the New Intermediary Guidelines, partially or in their entirety, are currently pending before various Indian High Courts. The government has filed a transfer petition seeking that certain petitions be transferred to the Supreme Court to be heard together. Some of cases involving a challenge to Part II of the New Intermediary Guidelines including the traceability provision on the grounds that it violates the fundamental rights to privacy and freedom of expression, among other things, include *Live Law Media (P) Ltd. v Union of India* WP (C) 6272 of 2021 ; *Facebook Inc v Union of India* WP (C) No. 679 of 2019, decided on 24-9-2019*; WhatsApp LLC v CCI* 2021 SCC OnLine Del 2308; *Sanjay Kumar Singh v Union of India and others* WP(C) 3483 of 2021; *TM Krishna v Union of India* WP (C) No. 12515/2021; *Nikhil Wagle v Union of India* PIL/14204/2021; *Sayanti Sengupta v Union of India* WPA(C) No. 153 of 2021; *Uday Bedi v Union of India* WP(C) No. 6844 of 2021. This is not an exhaustive list of all the challenges to the New Intermediary Guidelines.

[105] Constitution of India, art 21.

[106] The importance of anonymity in a democracy was perhaps best captured by Justice John Paul Stevens in the majority opinion in *McIntyre v Ohio Elections Commission*, 1995 SCC OnLine US SC 36 : 514 US 334 (1995), wherein he stated 'anonymity is a shield from the tyranny of the majority'.

sphere has always been linked to possibilities for doing so anonymously.'[107] He further recognizes the revolutionizing and pivotal role that the internet plays in enabling anonymity: '[a]nonymity of communications is one of the most important advances enabled by the internet, and allows individuals to express themselves freely without fear of retribution or condemnation.'[108] The perception of lack of privacy has an acute and demonstrable chilling effect on the freedom of expression[109] and the imposition of traceability will inevitably lead to this undesirable outcome. In other words, '[i]t's disingenuous when the Indian government says that they want traceability but 'not at the cost of encryption or privacy'[110] Traceability is bound to be at the cost of privacy - as well as encryption - even if it means getting meta-data.'[111]

Owing to its inescapable negative impact on the right to privacy, a traceability mandate would have to clear the four-pronged proportionality and necessity test laid down by the Supreme Court of India in the seminal case of *K.S. Puttaswamy v Union of India*.[112] In *Puttaswamy*, a nine-judge bench of the Supreme Court unanimously held that 'the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III (fundamental rights) of the Constitution.'[113] The court observed that the right to privacy is an inalienable right that is inherent in every individual simply by virtue of being human.[114] In acknowledging the distinction between rights that are inherent and natural, and rights that the government has the power to confer and

---

[107] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (16 May 2011) A/HRC/17/27.

[108] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (17 April 2013) A/HRC/23/40.

[109] Jon Penney, 'Chilling Effects: Online Surveillance and Wikipedia Use' (2016) 31(1) Berkeley Tech L J 117, 161-169. The article analyzes an empirical study evidencing the chilling effect of government surveillance on Wikipedia users. It uses Wikipedia data or web traffic data to explore how the traffic to privacy-sensitive articles reduced significantly after revelations of mass surveillance.

[110] Nikhil Pahwa, 'Intermediary Liability: 'Many Problems Need Many Solutions', Says S Gopalakrishnan, Jt Secretary, MEITY' (*Medianama*, 19 March 2019) <https://www.medianama.com/2019/03/223-intermediary-liability-many-problems-need-many-solutions-says-s-gopalakrishnan-jt-secretary-meity/> accessed 12 November 2020.

[111] Nikhil Pahwa, 'We Need a Better Approach to WhatsApp and Traceability' (*Medianama*, 28 March 2019) <https://www.medianama.com/2019/03/223-we-need-a-better-approach-to-whatsapp-and-traceability/> accessed 12 November 2020.

[112] (2017) 10 SCC 1.

[113] (2017) 10 SCC 1 [141-142] [DY Chandrachud J]. The case recognizes nine primary types of privacy: bodily, spatial, communicational, intellectual, decisional, associational, behavioral and informational. This drew from existing literature, *see*: Bert-Jaap Koops et al., 'A Typology of Privacy' (2017) 38(2) Univ Pennsylvania J Intl L 483.

[114] (2017) 10 SCC 1 [92] [RF Nariman J].

take away,[115] the court finds that the right to privacy is a natural right that is not bestowed by the State or the Constitution for the first time – it is only recognized and preserved – and can therefore not be taken away.[116] Any statute that infringes the inalienable right to privacy without any countervailing public interest would be declared void.[117]

The proportionality and necessity test outlined by the court requires that: '(i) the action must be sanctioned by law; (ii) the proposed action must be necessary in a democratic society for a legitimate aim; (iii) the extent of such interference must be proportionate to the need for such interference; and (iv) there must be procedural guarantees against abuse of such interference.'[118] An interference is considered 'necessary in a democratic society' in pursuit of

---

[115] The idea of privacy being an inevitable outcome of such a juxtaposition of rights was espoused in the seminal article by Samuel D. Warren and Louis. D. Brandeis on the right to privacy as the right to be let alone, that is considered to be the birth of privacy law [*see*: Samuel D. Warren & Louis D. Brandeis, 'The Right to Privacy' (1890) 4(5) Harvard L Rev 193]. The court cites to this particular paragraph from the article: 'Once a civilization has been made the distinction between the 'outer' and the 'inner' man, between the light of the soul and the life of the body, between the spiritual and the material, between the sacred and the profane, between rights inherent and inalienable, and the rights that are in the power of the government to give and take away, between public and private, between society and solitude, it becomes impossible to avoid the idea of privacy by whatever name it may be called – the idea of a private sphere in which man may become and remain himself.'

[116] (2017) 10 SCC 1 [92] [RF Nariman J].

[117] (2017) 10 SCC 1 [180-81] [DY Chandrachud J].

[118] (2017) 10 SCC 1 [71] [SK Kaul J]. Chandrachud J., delivering the judgment on behalf of four judges, stated with respect to the test of proportionality that: 'A law which encroaches upon privacy will have to withstand the touchstone of permissible restrictions on fundamental rights. In the context of Article 21 an invasion of privacy must be justified on the basis of a law which stipulates a procedure which is fair, just and reasonable. The law must also be valid with reference to the encroachment on life and personal liberty under Article 21. An invasion of life or personal liberty must meet the three-fold requirement of (i) legality, which postulates the existence of law; (ii) need, defined in terms of a legitimate state aim; and (iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them.', (2017) 10 SCC 1 [509]. In *KS Puttaswamy v Union of India*, (2019) 1 SCC 1 [*Puttaswamy (2)*], the 'fundamental precepts of proportionality' have been described as: '1. A law interfering with fundamental rights must be in pursuance of a legitimate state aim; 2. The justification for rights-infringing measures that interfere with or limit the exercise of fundamental rights and liberties must be based on the existence of a rational connection between those measures, the situation in fact and the object sought to be achieved; 3. The measures must be necessary to achieve the object and must not infringe rights to an extent greater than is necessary to fulfil the aim; 4. Restrictions must not only serve a legitimate purposes; they must also be necessary to protect them; and 5. The State must provide sufficient safeguards relating to the storing and protection of centrally stored data. In order to prevent arbitrary or abusive interference with privacy, the State must guarantee that the collection and use of personal information is based on the consent of the individual; that it is authorised by law and that sufficient safeguards exist to ensure that the data is only used for the purpose specified at the time of collection. Ownership of the data must at all times vest in the individual whose data is collected. The individual must have a right of access to the data collected and the discretion to opt out.'

a legitimate aim if it answers a 'pressing social need', if it is proportionate to the legitimate aim pursued and if the reasons adduced to justify the interference are 'relevant and sufficient.'[119] The aim of the test is essentially to strike a balance between public interest and the interests of an individual.[120]

The traceability mandate in the New Intermediary Guidelines arguably does not meet the requirements of the *Puttaswamy* test. It is not a necessary or proportionate measure to meet the stated objective of protecting national security, preserving law and order, or preventing the spread of fake news.[121]

The Supreme Court referred extensively to the jurisprudence of the European Court of Human Rights (ECHR) in the *Puttaswamy* decision, giving reason to believe it would turn to ECHR jurisprudence when assessing the traceability mandate. The expression 'prescribed by law' – the equivalent of 'sanctioned by law' – has been held by the ECHR to imply the following requirements:[122]

'Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a 'law' unless it is formulated with sufficient precision to enable the citizen to regulate his conduct; he must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.'

The traceability provision in the New Intermediary Guidelines is devoid of any precision that would enable reasonable foreseeability. The circumstances in which the government may demand tracing of the originator, and the conditions or procedural requirements that must be followed, have not been defined with adequate clarity and limitations. Without clear demarcation of the applicability of the traceability mandate, it remains an opaque provision, devoid of reasonable predictability and necessary safeguards. In order to fulfil the 'sanctioned by law' requirement, the legal discretion granted to the

---

[119] ibid.

[120] (2017) 10 SCC 1 [134] [DY Chandrachud J].

[121] *See*: UNHRC, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (22 May 2015) A/HRC/29/32. In that report, David Kaye, the former Special Rapporteur, recommended strong protection for encryption and anonymity, and that States should not restrict these privacy tools, 'even where the restriction is arguably in pursuit of a legitimate interest, many laws and policies regularly do not meet the standards of necessity and proportionality and have broad, deleterious effects on the ability of all individuals to exercise freely their rights to privacy and freedom of opinion and expression.'

[122] Judgment in the *Sunday Times v United Kingdom*, No. 6538/74, 26 April 1979, para 49. *See also Malone v United Kingdom*, No. 8691/79, 2 August 1984, paras 67-68.

government with respect to traceability ought not to be a practically unfettered power and the scope must be set out with sufficient clarity.

An important aspect of necessity is that the chosen measure must be one that is effective and least intrusive.[123] The traceability mandate fails on both counts. First, it is not clear that a traceability mandate will be effective. The originator of a message on a particular platform is not necessarily the creator of the content. In addition, sender signatures that could have to be affixed to messages to facilitate traceability can be spoofed by malicious actors,[124] creating another risk to efficacy. In any event, discerning malicious intent on the originator's part is a dubious prospect, further calling into question the efficacy of such a mandate. Additionally, tracing the chain of communication would amount to attributing culpability devoid of the context in which the content was shared – mere virality of a message would unfairly become a valid cause for suspicion. Finally, as indicated above, the traceability mandate could cause some providers to abandon the end-to-end encryption they now offer to all of their users, making users' data vulnerable to malicious actors. As a further indication of ineffectiveness, this result will pertain, even while the malicious actors simply use other methods to encrypt their communications — such as PGP (an acronym for the encryption system known as Pretty Good Privacy[125]) — or devise their own encryption algorithm with the help of a YouTube video[126] or a step-by-step guide[127] available online.[128]

Second, a traceability mandate creates new risks to communications security that makes it a very intrusive measure that is unlikely to be the least intrusive approach. As indicated above, it completely undermines anonymity, which is essential to the ability to communicate without fear of retribution. And, it could require the provider to affix the originator's information

---

[123] EDPS, 'The EDPS Quick-Guide to Necessity and Proportionality' (January 2020) <https://edps.europa.eu/sites/edp/files/publication/20-01-28_edps_quickguide_en.pdf> accessed 23 February 2021.

[124] Internet Society, Traceability and Cybersecurity: Experts' Workshop Series on Encryption in India, <https://www.internetsociety.org/resources/doc/2020/traceability-and-cybersecurity-experts-workshop-series-on-encryption-in-india/#_ftnref2> accessed 23 February 2021.

[125] Jeff Petters, 'What is PGP Encryption and How Does it Work?' (*Varonis*, 4 June 2020) <https://www.varonis.com/blog/pgp-encryption/> accessed 25 November 2020.

[126] For example, <https://www.youtube.com/watch?v=TZT7wvTeVyY>.

[127] One such guide is available from Wikihow. <https://www.wikihow.com/Create-an-Encryption-Algorithm> accessed 25 November 2020.

[128] Robert E. Endeley, 'End-to-End Encryption in Messaging Services and National Security—Case of WhatsApp Messenger' 9 (2018) J Info 95, 98; Antonis Michalas, 'How WhatsApp Encryption Works—And Why There Shouldn't be a Backdoor' (*The Conversation*, 28 March 2017) <https://theconversation.com/how-whatsapp-encryption-works-and-why-there-shou ldnt-be-a-backdoor-75266> accessed 13 November 2020.

in the form of a digital fingerprint to each message, or require the creation of alpha-numeric hashes of each message, both of which are sensitive data that would otherwise not exist and that is vulnerable to exploitation by malicious actors.

Moreover, the traceability mandate is disproportionate in so far as it threatens to infringe the right to privacy of all internet users, and chills their free expression by undermining anonymity, without any demonstration as to how it would practicably lead to achieving the stated aims.[129] Lawmakers, and courts, ought to consider whether the possibility of identifying a few bad actors is worth imperilling the constitutional rights and freedoms of hundreds of millions of Indian users. In the absence of proportionality and any demonstration as to how the interference is 'relevant and sufficient,' the traceability proposal fails to fulfil the 'necessary in a democratic society' limb of the test laid down by the Supreme Court.

Finally, safeguards against abuse are lacking. No meaningful procedural safeguards limit the conditions under which the traceability provision may be invoked. The proposed law does not provide for notice and disclosure requirements and an adequate judicial redress mechanism for individuals affected by a traceability order. In any event, the significant harms of the measure to the inalienable and fundamental right to privacy far outweigh any of the measure's hypothetical benefits.[130]

The Indian government will likely continue to press proposals to strengthen traceability and weaken encryption,[131] as is apparent from the

---

[129] UNHRC, 'Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (June 2018) Research Paper 1/2018. In 2018, as states were intensifying efforts to weaken encryption and compel the installation of encryption backdoors, the former Special Rapporteur's Encryption and Anonymity issued a follow-up to his 2015 report. It correctly indicates that 'despite [their] threat to the privacy and security of *all* users, States have failed to demonstrate the necessity of backdoors, particularly given the wide range of investigative tools at their disposal'.

[130] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (22 May 2015) A/HRC/29/32. Herein, the former UN Special Rapporteur on freedom of opinion and expression, David Kaye cautioned governments against restricting privacy tools such as encryption on the grounds of fighting terrorism and maintaining public order: 'Laws, practices and policies that ban, restrict, or otherwise undermine encryption and anonymity – all in the name of public order or counter-terrorism – do significant, and I would say disproportionate, damage to the rights at the heart of my mandate'; Angela Marie Rulffes, 'Privacy vs. Security: Fear Appeals, Terrorism and the Willingness to Allow Increased Government Surveillance' (Dissertation, Syracuse University 2017) 24-28; 'Protecting Individual Privacy in the Struggle Against Terrorists' (2008) National Research Council Report, 71-75 <https://epic.org/misc/nrc_rept_100708.pdf> accessed 13 November 2020.

[131] On the other hand, the sector specific regulator, the Telecom Regulatory Authority of India (TRAI) recently released its recommendations on the Regulatory Framework for

New Intermediary Guidelines and a recent joint statement the government made with the Five Eyes nations – New Zealand, the United States, United Kingdom, Canada and Australia – and Japan demanding backdoors for law enforcement to access encrypted content.[132] Whether this approach towards encryption is incorporated in legislation is ultimately the legislature's bailiwick. A recent recommendation by an ad-hoc committee of the upper house of the parliament to break encryption and enable traceability[133] suggests that the parliament might go along with the executive. However, the future of encryption in India will to a significant extent also be informed by the jurisprudence on the interaction between encryption, traceability and the fundamental right to privacy that is evolving in the Supreme Court.[134]

Over-The-Top (OTT) Communication Services in which it rightly acknowledges that encryption protects the end users and any requirement to obtain decrypted content would require changes to the fundamental architecture of encrypted platforms and make the parties involved in the communication vulnerable to unlawful actors. 'Recommendations on Regulatory Framework for Over-The-Top (OTT) Communication Services' (*Telecom Regulatory Authority of India*, 14th September 2020) 7 <https://www.trai.gov.in/sites/default/files/Recommendation_14092020.pdf> accessed 13 November 2020.

[132] 'International Statement: End-To-End Encryption and Public Safety' (*Department of Justice*, 11 October 2020) <https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety> accessed 13 November 2020.

[133] A 14-member ad-hoc committee of the Rajya Sabha, led by Jairam Ramesh, recommended that law enforcement agencies should be permitted to break end-to-end encryption to trace the distributor of child pornography on social media; *see*: Neha Alawadhi, 'RS Panel Suggests Breaking Encryption To Curb Child Pornograhy Distribution' (*Business Standard*, 27 January 2020) <https://www.business-standard.com/article/technology/rs-panel-suggests-breaking-encryption-to-curb-child-pornograhy-distribution-120012600705_1.html> accessed 14 November 2020.

[134] In addition to the legal challenges to the traceability provision in the New Intermediary Guidelines, including those mentioned in footnote 104, certain cases relating to traceability, and encryption, that were earlier being heard by the High Courts in three states were transferred to the Supreme Court of India in October 2019 in view of the complex legal and technological questions involved that would impact the fundamental rights of internet users [*Facebook Inc v Union of India* 2019 SCC OnLine SC 1717]: (1) In *Antony Clement Rubin v Union of India* 2019 SCC OnLine Mad 11784, two animal rights activists approached the Madras High Court, separately but with verbatim applications, under its writ petition, praying for the issuance of a writ directing the government to declare linkage of Aadhar (a unique identity number) as mandatory for authentication while using any social media account to enable traceability.; (2) *In Sagar Rajabhau Surywanshi v Union of India* (PIL/147/2018) (not found), the petitioner prayed the Bombay High Court to issue a writ directing the government to ensure that all users of social media platforms are identifiable, with Indian nationals linked with Aadhar, and foreign nationals linked by their platform to an identity. This case was disposed by the Court since the Petitioner intended to directly intervene in the proceedings before the Supreme Court; and (3) In *Amitabha Gupta v Union of India* (WP (C) No 13076/2019), the petitioner approached the Court to direct Facebook (which owns WhatsApp) to verify new users via some statutorily authorized identity proof documents, such as Aadhaar or voter ID number. These cases have been tagged with other relevant cases in the Supreme Court and the group of matters is pending with no specific date listed for the next hearing. These are: (1) *S.G. Vombatkere v Union of India* (WP (C) No 679/2019)(pending), which involves a writ petition challenging Aadhaar Ordinance, 2019 and Aadhaar Regulations, 2019 as violative of Right to Privacy because

IV. The Case for Protecting and Encouraging Encryption

Surveillance Stifles Privacy and Free Expression; Encryption Preserves Both

Privacy is essential to forge interpersonal relationships and to freely communicate thoughts and ideas, especially unconventional or unpopular thoughts and ideas.[135] Even in public spaces, a degree of anonymity is necessary to preserve freedoms that are central to a democratic and open society.[136] Constant surveillance alters human behaviour for fear of disapproval or of retaliation. As the philosopher Jeffrey Reiman observed, '[t]o the extent that a person experiences himself as subject to public observation, he naturally experiences himself as subject to public review. As a consequence, he will tend to act in ways that are publicly acceptable.'[137]

The stultifying effect of surveillance could inhibit a range of individuals who know they are being watched. As the European Court of Human Rights has observed, the mere existence of law that authorizes the secret surveillance of communications amounts to an interference with the right to

---

it enables State and private actor surveillance as well as commercially exploits the personal information of citizens; (2)-(3) *Manohar Lal Sharma v Union of India* (WP(Crim) No 1/2019)(pending) and *Amit Sahni v Union of India* (WP(C) No 2 of 2019)(pending), which involve writ petitions challenging government notification authorizing 10 central agencies to intercept, monitor and decrypt any computer system; (4) *PUCL v Union of India* (WP(C) No 61 of 2019)(pending), which challenges said notification and s 5(2) of the Telegraph Act; (5) *Mahua Moitra v Union of India* (WP(C) No 916 of 2018, decided on 17-12-2019 (SC), which involves a PIL challenging the 'Social Media Communication Hub' created by the central government as invasion of citizen's social media activity, thus violative of Right to Privacy; (6) *Internet Freedom Foundation v Union of India* (WP(C) No 44 of 2019) (pending), which involves a writ Petition challenging constitutionality of s 69, IT Act, the Decryption Rules, and the aforementioned notification.

[135] Charles Fried, 'Privacy' (1968) 77 Yale L J 475.

[136] Christopher Slobogin, 'Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity' (2002) 72 Mississippi L J 213, 240-51.

[137] Jeffrey H. Reiman, 'Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future', (1995) 11 Santa Clara Comp & High Tech L J 27, 38. Herein, Reiman emphasizes the impact of the knowledge of surveillance on human thoughts and deeds in saying '[w]hen you know you are being observed, you naturally identify with the outside observer's viewpoint, and add that alongside your own viewpoint on your action. This double vision makes your act different, whether the act is making love or taking a drive'.; Shoshana Zuboff, *In the Age of the Smart Machine: The Future of Work and Power* (Basic Books 1988) 344-45. Zuboff explains this phenomenon among those who know they are being watched as 'anticipatory conformity'. The reason behind the skepticism that alters behavior in this manner could be anything including uncertainty surrounding how the officer's interpretation and reaction or the inherent desire to appear compliant, but the point is that in the absence of privacy, such problematic hesitation exists.

privacy.[138] Imagine that you are being followed by a law enforcement officer at all times. You would most likely think twice before covering your face to shield yourself from the weather or break into a sprint suddenly because you may miss the train. Also imagine if the officer could access your verbal and written communications. The average person under surveillance will hesitate to pour their hearts out to loved ones, share confidential information, seek professional assistance or search for information about healthcare on sensitive topics[139] or attend protests[140] or political demonstrations.[141] In the case of some individuals – such as journalists, lawyers, medical professionals, or activists[142] – exposure of their communications to any party but the intended recipient could potentially carry grave consequences. The detriments are felt particularly severely by protestors, dissidents, and persecuted minorities in

---

[138] *Weber and Saravia v Germany* (2006) 46 ECHR 78; Gabor Rona & Lauren Aarons, 'State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace' (2016) 8(503) J Nat Sec L & Pol 503, 511-513.

[139] In the German context, a study showed that half of Germans would not correspond with psychotherapists and marriage counsellors through telephones or emails as a result of data retention. Such sensitive communication would be enabled by encryption as it would preclude access to and retention of the content of communication. *See*: Axel Arnbak, Plenary Presentation at the Taking on the Data Retention Directive Conference in Brussels: What the European Commission Owes 500 Million Europeans (Dec 3 2010) at 3, <http://www.edri.org/files/Data_Retention_Conference_031210final.pdf> accessed 25 November 2020.

[140] TUNHRC, 'Report Of The Special Rapporteur On The Rights To Freedom Of Peaceful Assembly And Of Association' (24 April 2013) A/HRC/23/39. Herein, the Special Rapporteur noted that surveillance and intelligence databases have a chilling effect on protestors; UNHRC, 'Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association: Addendum- Mission to the United Kingdom of Great Britain and Northern Ireland' (17 June 2013) A/HRC/23/39/Add.1.

[141] Roger Clarke, 'While You Were Sleeping . . . Surveillance Technologies Arrived' (2001) 73 Australian Q 10, 13. Herein, Clarke predicted, '[l]eaders of demonstrations in the future should expect both their locations and their conversations to be transparent to the police'. He states that the purpose of surveillance technologies is 'to affect the behavior of both targeted individuals, and of populations'; Stephen Owen, 'Monitoring Social Media And Protest Movements: Ensuring Political Order Through Surveillance and Surveillance Discourse' (2017) 23(6) J Study of Race, Nation & Culture 688, 690-695; Rina Chandran, 'Use of Facial Recognition In Delhi Rally Sparks Privacy Fears' (*Reuters*, 30 December 2019) <https://in.reuters.com/article/us-india-protests-facialrecognition-trfn-idUSKBN1YY0PA> accessed 13 November 2020.

[142] 'Communities At Risk: How Encroaching Surveillance is Putting A Squeeze on Activists' (*Privacy International*, 16 April 2019) <https://privacyinternational.org/news-analysis/2816/communities-risk-how-encroaching-surveillance-putting-squeeze-activists> accessed 13 November 2020; 'Unlawful Surveillance Threatens our Activism. Here's How We can Fight Back' (*Amnesty International*, 8 November 2015) <https://www.amnesty-usa.org/unlawful-surveillance-threatens-our-activism-heres-how-we-can-fight-back/> accessed 13 November 2020; Eva Galperin, 'Don't Get Your Sources in Syria Killed' (*Committee to Protect Journalists*, 21 May 2012) <https://cpj.org/2012/05/dont-get-your-sources-in-syria-killed/> accessed 13 November 2020; Julie Posetti, 'Surveillance and Data Collection are Putting Journalists and Sources at Risk' (*The Wire*, 6 May 2017) <https://thewire.in/media/surveillance-data-collection-putting-journalists-sources-risk> accessed 13 November 2020.

repressive regimes.[143] Such impediments to simply *being* – simply *existing in society* – translate quite literally in an online world, especially if encryption is weakened. Without the protection of encryption, individuals may hesitate to exchange sensitive communications through online intermediaries if they know they are being, or could be, watched. Human expression is then confined within the space of what may be deemed to be acceptable in the eyes behind the lens of surveillance.

Encryption permits the creation of a safe space for users' right to privacy and freedom of expression and protects them from becoming vulnerable to unfettered surveillance and malicious or repressive actors. It preserves communicational privacy reflected in the ability to restrict access to communications,[144] intellectual privacy which is the freedom to develop ideas without being monitored,[145] and informational privacy resting on the elements of secrecy, anonymity and control.[146] The importance of encryption is therefore amplified in jurisdictions such as India where the surveillance regime lacks adequate checks and balances and exacerbates the power imbalance between the state and the people.[147]

---

[143] Adrian Shahbaz & Allie Funk, 'Social Media Surveillance, Freedom on the Net 2019 Key Finding: Governments Harness Big Data for Social Media Surveillance' (*Freedom House*, 2019) <https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance> accessed 13 November 2020; 'Ethnic Minorities at Greater Risk of Over Surveillance After Protests' (*Privacy International*, 15 June 2020) <https://privacyinternational.org/news-analysis/3926/ethnic-minorities-greater-risk-oversurveillance-after-protests> accessed 13 November 2020; Valerie Aston, 'State Surveillance of Protest and the Rights to Privacy and Freedom of Assembly: A Comparison of Judicial and Protester Perspectives' (2017) 8(1) EJLT 1, 3-8; Elizabeth E. Joh, 'Privacy Protests: Surveillance Evasion and Fourth Amendment Suspicion' (2013) 55 Arizona L Rev 997, 1013-1022.

[144] (2017) 10 SCC 1 [141-142] [DY Chandrachud J]; *see*: 'UN: Online Anonymity, Encryption Protect Rights' (*Human Rights Watch*, 17 June 2005) <https://www.hrw.org/news/2015/06/17/un-online-anonymity-encryption-protect-rights> accessed 13 November 2020; 'Decrypting the Encryption Debate: A Framework for Decision Makers' (2018) National Academies of Sciences, Engineering, and Medicine Consensus Study Report, 32-39 <https://www.nap.edu/catalog/25010/decrypting-the-encryption-debate-a-framework-for-decision-makers> accessed 13 November 2020.

[145] Neil Richards, 'Intellectual Privacy' (2008) 87 Texas L Rev 387, 389.

[146] *Spencer v R* 2014 SCC OnLine Can SC 34 : (2014) 2 SCR 212 [38-47]; *K S Puttaswamy v Union of India* (2017) 10 SCC 1 [134] [DY Chandrachud J].

[147] 'India's Surveillance State' (2014) SLFC.in Surveillance Report <https://sflc.in/sites/default/files/wp-content/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf> accessed 13 November 2020. This report provides a comprehensive overview of the enabling statutes, case law and principles in respect of communications surveillance in India. It concludes that surveillance is conducted on very broadly worded grounds, surveillance systems have large scale data-mining and profiling abilities and the public is kept in the dark because communications surveillance is in the exclusive domain of the executive branch. It recommends a review of legislative provisions that sanction and regulate surveillance with a focus on the right to privacy.

India, the world's largest democracy, is also among the biggest surveillance states. In a 2019 report on surveillance states by a UK-based research firm, India was found to display a 'systemic failure to maintain safeguards' and was ranked third in a list of forty-seven countries, behind only Russia and China.[148] The Standard Operating Procedure followed by law enforcement agencies to surveil citizens demonstrates 'centralisation of power in the hands of an opaque and unaccountable Union Executive'[149]. Extant laws fail to ensure accountability and limit the scope of surveillance operations cloaked in secrecy.[150] The statutory preconditions based on which surveillance may be conducted are extremely broadly worded[151] and the executive branch has unfettered discretion to authorise surveillance without any independent oversight.[152]

---

[148] Paul Bischoff, 'Data Privacy Laws & Government Surveillance by Country: Which Countries Best Protect their Citizens?' (*Comparitech*, 15 October 2019) <https://www.comparitech.com/blog/vpn-privacy/surveillance-states/> accessed 13 November 2020. Each country's report, sources, and scores can be found at <https://docs.google.com/spreadsheets/d/1uPCfyzwT2b47oX0kcYg3kn3V4H6IWUikp4jMOVUWmJA/edit#gid=0>.

[149] 'Secret Operating Procedure for Digital Snooping Revealed. Confirms Fears of Centralisation of Executive Power, Zero Judicial Scrutiny and Oversight' (*Internet Freedom Foundation*, 11 March 2019) <https://internetfreedom.in/revealed-secret-operating-procedure-followed-by-the-govt-for-digital-snooping/> accessed 13 November 2020.

[150] ibid.

[151] S 69, IT Act empowers the government to direct an agency to 'intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource' if it is 'in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence'. Telephone tapping, under s 5(2), Indian Telegraph Act 1885, may be ordered on the 'occurrence of any public emergency' or 'in the interest of the public safety'. The grounds on which surveillance may be conducted are therefore extremely elastic and devoid of any meaningful limitations. Further extending this elastic scope, in December 2018, the central government issued a notification, pursuant to s 69 of the IT Act and Rule 4 of the Decryption Rules, authorizing ten security and intelligence agencies to engage in the interception, monitoring and decryption of information generated, transmitted, received or stored in any computer resource. Six petitions challenging this notification broadly on the ground that it violates the proportionality test laid down in *Puttaswamy* are currently pending before the Supreme Court. These are: (1) *Manohar Lal Sharma v Union of India* (WP (Crim) No 1 of 2019) (pending); (2) *Amit Sahni v Union of India* (WP(C) No 2 of 2019)(pending); (3) *Mahua Moitra v Union of India* (WP(C) No 916 of 2018)(pending); (4) *Internet Freedom Foundation v Union of India* (WP(C) No 44/2019) (pending); (5) *PUCL v Union of India* (WP(C) No 61 of 2019) (pending); and (6) *Shreya Singhal v Union of India* (WP(C) No 34 of 2019) (pending). The petition filed by the Internet Freedom Foundation, also challenges the constitutional validity of s 69, IT Act and the Decryption Rules.

[152] Vrinda Bhandari & Karan Lahiri, 'The Surveillance State, Privacy and Criminal Investigation in India: Possible Futures in a Post-Puttaswamy World' (2020) 3(2) Univ Oxford Human Rights Hub J 15, 46.

Human Rights

As communications increasingly take a digital form, there is growing recognition globally from the perspective of human rights that encryption is an essential element for a free and open internet because it supports free expression, access to information, anonymity, and privacy.[153] In allowing for uninhibited private communication, and protecting the confidentiality, integrity, and availability of data, encryption helps fulfil an important precondition for the freedom of communication.[154] It serves as a vital tool particularly for journalists, lawyers, activists, artists, and academics to carry out their profession and exercise human rights, and for persecuted minorities and dissidents in hostile political, social, religious, and legal environments.[155] Additionally, and crucially, it fosters meaningful inclusion and protects those disproportionately affected by online violence owing to intersectional[156] forms of discrimination based on factors such as gender identity and expression, abilities, age, sexual orientation, race, ethnicity, caste, religion, class, income, and urban and rural settings.[157]

In the report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye recommended strong protection for encryption and anonymity as they enable individuals to exercise the right to freedom of expression in the digital era.[158] He empha-

---

[153] Wolfgang Schulz & Joris van Hoboken, *Human Rights and Encryption* (United Nations Educational, Scientific and Cultural Organization 2016) 50-59; *Travel Guide to the Digital World: Encryption Policy for Human Rights Defenders* (Global Partners Digital 2017) 40-51.

[154] ibid.

[155] UNHRC, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (22 May 2015) A/HRC/29/32.

[156] Kimberle Crenshaw, 'Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory, and Antiracist Politics' (1989) 1989(1) Univ Chicago L Forum 139. Herein, the legal scholar, Kimberle Crenshaw, first introduced the term 'intersectionality' in this paper. Intersectionality focuses on how different aspects of an individual's social and political identities such as race, gender and class interact and overlap to create varying modes of privilege and discrimination.

[157] UNHRC, 'Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective' (14 June 2018) A/HRC/38/47. In this report, the Special Rapporteur affirms that, '[e]ncryption and anonymity, separately or together, create a zone of privacy to protect freedom of expression and to facilitate the freedom to seek, receive and impart information and ideas, regardless of frontiers. Anonymity online is [sic] an important role for women and others at risk of discrimination and stigma, in that it allows them to seek information, find solidarity and support and share opinions without fear of being identified.' The report recommends that 'States should protect and encourage the development of technology, including of encryption and anonymity tools that protect the rights and security of women online'.

[158] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (22 May 2015) A/HRC/29/32.

sized that individuals' right to access information 'regardless of frontiers,' as first guaranteed by Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, is being impeded by 'massive blocking, throttling, and filtering of the internet.'[159] The report categorically recommends that states should not restrict encryption and anonymity, avoid measures that weaken encryption, and refrain from making identification of users a condition for access to digital communications.[160] Subsequently, in 2017, in appreciation of the importance of encryption to freedom of expression, privacy and related human rights, the UN Human Rights Council adopted a resolution encouraging 'business enterprises to work towards enabling technical solutions to secure and protect the confidentiality of digital communications, which may include measures for encryption and anonymity.'[161]

As the exercise of human rights and freedoms finds an avenue for enhanced realization in digital spheres, so does their vulnerability to attack by hostile actors. Encryption and anonymity online are no longer ancillary to the rights to freedom of expression and privacy but rather central to the evolution and realization of these rights in any democratic society. States ought to therefore encourage the use of encryption without any restrictions.[162]

---

[159] UHCHR, 'Human Rights, Encryption and Anonymity in a Digital Age' (1 July 2015)

[160] UNHRC, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (22 May 2015) A/HRC/29/32, at p. 20.

[161] UNHRC Res 34/7 (23 March 2017); UNHRC, 'Mandate of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (June 2018) Research Paper 1/2018.

[162] Some examples of best practices involving legislations that expressly protect the right to use encryption include the Law on Electronic Commerce in Luxembourg which says that '[t]he use of cryptographic techniques is free'; the Electronic Communications and Transactions Act, 2009 in Zambia which explicitly states that individuals may use encryption 'regardless of encryption algorithm selection, encryption key length chosen, or implementation technique or medium used'; and the Brazilian Civil Rights Framework for the Internet which guarantees the 'inviolability and confidentiality of [internet users'] stored private communications'.

National Security

Globally,[163] as in India,[164] the debate on encryption is often framed as 'privacy versus security' with the implication that strengthening one necessarily means weakening the other. In fact, in the encryption context, the two principles reinforce each other.[165] A cyber infrastructure made more resilient with strong encryption significantly reduces the risk of data breaches and preserves both individual privacy and national security. Encryption protects critical infrastructure, classified information, transactions, trade secrets, and personal communications and data for the government and law enforcement agencies and for the general population. The necessary corollary is that weakening encryption jeopardises security as much as it threatens privacy. The vulnerabilities in the system, whether in the form of weak encryption or 'backdoors' for exceptional access, expose individuals, businesses, and states alike to attacks by malicious actors. As such, it has been argued that a more accurate framing of the debate would be 'security versus security.'[166]

---

[163] 'International Statement: End-To-End Encryption and Public Safety' (*Department of Justice*, 11 October 2020) <https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety> accessed 13 November 2020; 'Going Dark: Encryption, Technology, and the Balances between Public Safety and Privacy' (*Federal Bureau of Investigation*, 8 July 2015) <https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy> accessed 13 November 2020; Derek E. Bambauer, 'Privacy Versus Security' (2013) 103(3) J Crim L & Criminology 667, 667-672; Morvillo Abramowitz Grand Iason & Anello PC, 'The International Encryption Debate: Privacy Versus Big Brother' (*Lexology*, 12 June 2019) <https://www.lexology.com/library/detail.aspx?g=41bce78b-f790-4901-ba88-7b9f6ffdd488> accessed 13 November 2020; Dave Weinstein, 'Privacy vs. Security: It's a False Dilemma' (*Wall Street Journal*, 6 October 2019) <https://www.wsj.com/articles/privacy-vs-security-its-a-false-dilemma-11570389477> accessed 13 November 2020.

[164] Bedavyasa Mohanty, 'The Encryption Debate in India' (2019) Carnegie Endowment for International Peace, 2 <https://carnegieendowment.org/files/WP_The_Encryption_Debate_in_India.pdf> accessed 12 November 2020; 'The Encryption Debate' (*The Hindu*, 28 March 2016) <https://www.thehindu.com/opinion/editorial/editorial-on-the-encryption-debate/article7681977.ece> accessed 13 November 2020; Varsha Rao, 'The Encryption Debate Between WhatsApp and the Indian Government' (*TechQuila*, 26 October 2019) <https://www.techquila.co.in/the-encryption-debate-between-whatsapp-and-the-indian-government/> accessed 13 November 2020.

[165] 'Policy Brief: Encryption' (*Internet Society*, 9 June 2016) <https://www.internetsociety.org/policybriefs/encryption/> accessed 13 November 2020; Elaine Lammert, 'Security and Privacy are Not Mutually Exclusive' (*The Cipher Brief*, 17 March 2016) <https://www.thecipherbrief.com/column_article/security-and-privacy-are-not-mutually-exclusive> accessed 13 November 2020; Encryption Working Group, 'Moving the Encryption Policy Conversation Forward' (*Carnegie Endowment for International Peace*, 10 September 2019) <https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573> accessed 13 November 2020.

[166] House Committee on Homeland Security, *Going Dark, Going Forward: A Primer on the Encryption Debate* (Congress 2016) 6; *Travel Guide to the Digital World: Encryption Policy for Human Rights Defenders* (Global Partners Digital 2017) 26-27.

Encryption is not a threat to security but rather an integral element of both information security and national security and it is imperative that government and law enforcement officials recognize this. The Parliamentary Committee of the Council of Europe offered a strong example when it passed a resolution in 2015 endorsing 'the European Parliament's call to promote the wide use of encryption and resist any attempts to weaken encryption and other Internet safety standards, not only in the interest of privacy, but also in the interest of threats against national security posed by rogue States, terrorists, cyberterrorists and ordinary criminals.'[167] Further, the European Data Protection Board recently recommended encryption as a necessary supplementary measure to preserve data flows from Europe to the U.S.[168] This is because U.S. law, according to the Court of Justice of the European Union, provides an inadequate level of protection,[169] so encrypting data is necessary to preclude access by U.S. intelligence agencies under those lax surveillance standards.

Similarly, in the U.S., amidst attempts to weaken encryption by the U.S. Government,[170] a former head of the National Security Agency explained that encryption boosts national security: 'American security is better served with unbreakable end-to-end encryption than it would be served with one or another front door, backdoor, side door, however you want to describe it.'[171] In India too, certain security officials have rightly expressed strong support for encryption to ensure security. A veteran of the Indian intelligence community who has worked extensively on counter-terrorism measures said in a recent interview: 'Encryption not only protects you, it makes you stable as a system [...] 68% of our cybersecurity share is the government – it is the IT-enabled sector which is critical. Look at Aadhar, look at our banking.

---

[167] Parliamentary Assembly of the Council of Europe, *Mass Surveillance* (Resolution 2045, 2015) para 17.

[168] European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Adopted on 10 November 2020) <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf> accessed 25 November 2020.

[169] Judgment in Case C-311/18, *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*

[170] *In re Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus* IS300 at 2, No. ED 15-0451M, 2016 WL 680288, at *2 (CD Cal 2016); Eliminating Abusive and Rampant Neglect of Interactive Technologies Act 2020 ('EARN IT'); Lawful Access to Encrypted Data Act ('LAED').

[171] Paul Szoldra, 'Ex-NSA Chief Thinks the Government is Dead Wrong in Asking Apple for A Backdoor' (*Business Insider*, 26 February 2016) <https://www.businessinsider.in/enterprise/security/Ex-NSA-chief-thinks-the-government-is-dead-wrong-in-asking-Apple-for-a-backdoor/articleshow/51149769.cms> accessed 13 November 2020.

You have to make this system secure, you have to make this system safe. And how do you do it? You have to do it with encryption.'[172]

In the Indian context, encryption should be seen as an enabler not just of individual privacy and the economy but also of national security. Weakening privacy by threatening encryption weakens national security.[173] Cybersecurity incidents in which confidentiality of data is put at risk are increasing.[174] Significant data breaches have occurred, including one which revealed that targeted users, including activists, journalists, and senior government officials, were being spied on through the compromise of encrypted messaging apps on their cell phones.[175] Thousands of important individuals were allegedly tracked through another data breach, including the President and the Prime Minister of India and several other ministers, business persons, and journalists.[176] These incidents ought to provide impetus to the rec-

---

[172] News 18, 'Former IPS Officer & CIC Mr Yashovardhan Azad on #DataProtectionAuthority' (9 October 2020) <https://www.facebook.com/cnnnews18/videos/858538681550688/> accessed 13 November 2020. Yashovardhan Azad added that '[…] I think that encryption is perhaps the most important methodology today to protect our interests and for data protection… there is no doubt that encryption is very important for security, in fact that is the way to go forward. Giving backdoor rooms to security agencies can lead to a lot of problems. On the other hand breaking the entire encryption system is another problem because it makes you more vulnerable. End-to-end encryption should be there because it is for the safety of the consumer, for data protection'. He advocates for a strong data protection legislation governing access to data that prioritizes consent and establishes an independent data protection authority.

[173] Apar Gupta, 'Why there cannot be any National Security without Individual Privacy' (*Hindustan Times*, 4 November 2019) <https://www.hindustantimes.com/analysis/why-there-cannot-be-any-national-security-without-individual-privacy-analysis/story-JvDaOJLW85gXR9cILtwq7M.html> accessed 13 November 2020.

[174] The Indian Computer Emergency Response Team (CERT-In), the government agency responsible for tracking and responding to cybersecurity threats, reported that it handled over 3.94 lakh (394,000) incidents in 2019 alone, *see*: PTI, '3.94 lakh cybersecurity incidents reported to CERT-In in 2019: Dhotre' (*Business Insider*, 5 February 2020) <https://www.businessinsider.in/business/news/3-94-lakh-cybersecurity-incidents-reported-to-cert-in-in-2019-dhotre/articleshow/73961329.cms> accessed 13 November 2020.

[175] Apar Gupta, 'Why there cannot be any National Security without Individual Privacy' (*Hindustan Times*, 4 November 2019) <https://www.hindustantimes.com/analysis/why-there-cannot-be-any-national-security-without-individual-privacy-analysis/story-JvDaOJLW85gXR9cILtwq7M.html> accessed 13 November 2020; FP Staff, 'WhatsApp claims it informed authorities about vulnerability in May 2019; govt sources say advisory full of 'Technical Jargon' (*First Post*, 2 November 2019) <https://www.firstpost.com/india/whatsapp-claims-it-informed-centre-about-vulnerability-in-may-2019-govt-sources-say-advisory-full-of-technical-jargon-7587621.html> accessed 13 November 2020. The Pegasus spyware exploited a vulnerability in the system and was able to illegally access a phone's camera and microphone, read messages and record keystrokes. The spyware could thus compromise the data at rest on the phone.

[176] Express Web Desk, 'Chinese firm Tracking Influential Indians also Harvested Data of over 50,000 Americans' (*The Indian Express*, 14 September 2020) <https://indianexpress.com/article/world/china-data-harvest-australia-india-zhenhua-data-information-technology-6595217/> accessed 13 November 2020; ET Online, 'Zhenhua Data leak: From

ognition that encryption aids security, significantly mitigates the risk of a breach by preventing the attacker from accessing the sensitive data,[177] and must therefore be encouraged rather than restricted. As Apar Gupta, the Executive Director of the Internet Freedom Foundation puts it, '[w]e must all recognise that national security starts with securing the smartphones of every single Indian by embracing technologies such as encryption rather than deploying spyware. This is a core part of our fundamental right to privacy.'[178]

Thus, arguments for undermining encryption that represent privacy and national security as mutually exclusive goals should be recognized and rejected for the false binary on which they are based. The bottom line is that encryption protects the nation, its security, and its government officials as much as it protects the individual citizen.

The Economic Justification

Encryption offers notable advantages to both industry and society by ensuring that transactions, communications, and industrial secrets remain safe in the virtual space. Many companies believe that the increasing demand for information security means that strict limitations on the use of encryption would result in significant financial losses as well as a steep decline in employment opportunities.[179] India is one of the largest offshoring destinations for several IT companies around the world.[180] The Indian IT industry contributed almost 8% of the country's overall GDP in 2017 and in 2019, it generated an annual revenue of approximately 180 billion USD.[181] This

---

Narendra Modi to Ratan Tata, here's the List of Prominent Indians China Spied on' (*The Economic Times*, 14 September 2020) <https://economictimes.indiatimes.com/news/defence/zhenhua-data-leak-from-narendra-modi-to-ratan-tata-heres-list-of-prominent-indians-china-spied-on/articleshow/78107743.cms?from=mdr> accessed 13 November 2020

[177] 'Encryption is a Critical Safeguard against Data Breaches' (*BSA*) <https://www.bsa.org/files/policy-filings/BSA_Encrypt_DataBreach-web.pdf> accessed 13 November 2020.

[178] Apar Gupta, 'Why there cannot be any National Security without Individual Privacy' (*Hindustan Times*, 4 November 2019) <https://www.hindustantimes.com/analysis/why-there-cannot-be-any-national-security-without-individual-privacy-analysis/story-JvDaOJLW85gXR9cILtwq7M.html> accessed 13 November 2020.

[179] Charles L. Evans, 'U.S. Export Control of Encryption Software: Efforts to Protect National Security Threaten the U.S. Software Industry's Ability to Compete in Foreign Markets' (1994) 19(3) North Carolina J Intl L & Comm Reg 469, 470; Chris Duckett, 'Home Affairs Attempts to Allay Concerns about Australian Exporters for Encryption-Busting Bill' (*Zdnet*, 26 November 2018) <https://www.zdnet.com/article/home-affairs-attempts-to-allay-concerns-of-australian-exporters-about-encryption-busting-bill/> accessed 14 November 2020.

[180] Shanglio Sun, 'Contribution of Indian IT-BPM Industry in GDP of India FY 2009-2020' (*Statistica*, 17 February 2021)https://www.statista.com/statistics/320776/contribution-of-indian-it-industry-to-india-s-gdp/accessed 14 November 2020.

[181] Shanglio Sun, 'IT Industry in India – Statistics & Facts' (*Statistica*, 12 August, 2021)<https://www.statista.com/topics/2256/it-industry-in-india/>accessed 14 November 2020.

key sector of the Indian economy could face serious setbacks if encryption is weakened as the resulting reduction in security would diminish the willingness of IT companies to outsource work to India and hurt India's reputation as a preferred IT hub.

Laws that weaken encryption can have a substantial negative impact on a country's economy. Australian legislation[182] requiring designated telecommunication service providers to give law enforcement agencies access to decrypted communication, and requiring them to build a decryption capability if they did not already have it, had a material and detrimental impact on the market. The 'perceived compliance burden' led to multinational companies blacklisting the Australian market and moving physical, operational, and legal jurisdiction offshore.[183] Further, restrictions on encryption damage innovation and economic growth stemming from the export of encryption technologies.[184]

The Organization for Economic Cooperation and Development (OECD) recognizes that the absence of cryptography is detrimental to privacy, national security, business, and electronic commerce. It makes data and communications vulnerable to unauthorized use and negatively impacts users' trust in information and communications systems, networks, and infrastructures. Therefore, OECD's Guidelines for Cryptography Policy recommend that '[t]he fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national

[182] The Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018.

[183] Asha Barbaschow, 'Home Affairs says no Problems with Encryption Laws even though Local Companies Suffer' (*Zdnet*, 5 July 2019) <https://www.zdnet.com/article/home-affairs-says-no-problems-with-encryption-laws-even-though-local-companies-suffer/> accessed 14 November 2020; Chris Duckett, 'Encryption Laws are Creating an Exodus of Data from Australia: Vault' (*Zdnet*, 5 July 2019) <https://www.zdnet.com/article/encryption-laws-are-creating-an-exodus-of-data-from-australia-vault/> accessed 14 November 2020.

[184] Sinita Radu, 'Restricting Encryption will Hurt Security and Economy, Won't Stop Terrorists from Using it Anyway' (*ITIF*, 14 March 2016) <https://itif.org/publications/2016/03/14/restricting-encryption-will-hurt-security-and-economy-won't-stop-terrorists> accessed 14 November 2020; Simrit Chhabra, Renjini Rajagopalan, & Vatsal Khullar, 'Framework for Regulating Encryption in India' (2019) The Quantum Hub Report, 6-9 <https://thequantumhub.com/wp-content/uploads/2020/08/Regulation-of-Encryption-TQH-Updated-08Apr19-Final.pdf> accessed 14 November 2020; Mohamad Ali, 'Backdoor Government Decryption Hurts My Business and Yours' (*Harvard Business Review*, 15 September 2016) <https://hbr.org/2016/09/backdoor-government-decryption-hurts-my-business-and-yours> accessed 14 November 2020.

cryptography policies and in the implementation and use of cryptographic methods.'[185]

Further, encryption benefits commerce by significantly reducing the cost of data breaches. According to a 2020 report by IBM,[186] the average cost of a data breach around the world was approximately ₹28.5 crore ($3.86 million USD). In India, data breaches cost organizations ₹14 crore ($1.9 million USD) on an average between August 2019 and April 2020.[187] The IBM report found that extensive encryption is a cost mitigating factor, decreasing the average total cost of a data breach by more than ₹1.7 crore ($237,176 USD). The findings also reflect that 52% of data breaches were caused by malicious attacks – the most expensive of the root causes as compared to system glitches and human errors[188] – the risks of which can be mitigated by encryption.

The New Intermediary Guidelines will have a debilitating impact on Indian companies, and especially start-ups. India is poised to become a global leader in the global digital economy. However, this potential rests on the ability of companies to inspire consumers' trust in their products which would be negatively impacted as companies are compelled to opt for weak encryption or not make it available at all. Such lack of trust in the global market will result in consumers outside India opting for products and services of competitors from other countries,[189] or a duality of services offered by companies with the Indian user base having access to the version that is less secure. With respect to start-ups, a study on the economic impact of safe harbours on Internet intermediary start-ups in 2015[190] revealed that an

---

[185] 'Recommendation of the Council concerning Guidelines for Cryptography Policy' (1997) Organization for Economic Cooperation and Development Legal Instrument/0289, 10 <https://dig.watch/sites/default/files/OECD%20Guidelines%20for%20Cryptography%20Policy.pdf> accessed 14 November 2020.

[186] 'Cost of a Data Breach Report' (2020) *IBM Security Report*, 5 <https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf> accessed 14 November 2020.

[187] PTI, 'Organisations in India Lost ₹14 Crore on Average to Data Breaches: IBM' (*LiveMint*, 29 July 2020) <https://www.livemint.com/companies/news/organisations-in-india-lost-rs-14-crore-on-average-to-data-breaches-ibm-11596001410186.html> accessed 14 November 2020.

[188] 'Cost of a Data Breach Report' (2020) *IBM Security Report*, 5 <https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf> accessed 14 November 2020.

[189] Soumyarendra Barik, 'Proposed Changes to Intermediary Guidelines will Put Digital India's Future at Risk: ISOC' (*Medianama,* 9 January 2020) <https://www.medianama.com/2020/01/223-isoc-intermediary-guidelines-letter/> accessed 14 November 2020.

[190] Oxera, 'The Economic Impact of Safe Harbours on Internet Intermediary Start-Ups' (2015) <https://www.oxera.com/wp-content/uploads/2018/07/The-economic-impact-of-safe-harbours-on-Internet-intermediary-start-ups.pdf.pdf> accessed 14 November 2020.

intermediary liability regime with clearly defined and low-cost compliance requirements could increase start-up success rates for intermediaries by more than 20% in India. Implementing such a regime, as opposed to the one in the New Intermediary Guidelines, would also increase the expected profit for successful start-up intermediaries by 5% in India.

Conclusion

Regulatory frameworks that would have the effect of compromising encryption, including the traceability mandate, are advanced to address grave problems such as 'fake news',[191] child sexual abuse material,[192] and offences relating to national security, public order, and sexually explicit material.[193] Such purposes lend legitimacy and urgency to the proposals. However, proposals that have the effect of breaking encryption with the purported aim

[191] Julie Posetti, Cherilyn Ireton, et al, *Journalism, Fake News & Disinformation: Handbook for Journalism Education and Training* (UNESCO 2018) 'Fake news' is an umbrella term for misinformation and disinformation. ''Misinformation' is information that is false, but the person who is disseminating it believes that it is true.'; ''Disinformation' is information that is false, and the person who is disseminating it knows it is false. It is a deliberate, intentional lie, and points to people being actively disinformed by malicious actors.' The traceability mandate in India's New Intermediary Guidelines and in initial drafts of the pending Brazilian Internet Freedom, Responsibility and Transparency Act, colloquially referred to as the 'Fake News Bill', received impetus from aim of curbing dis/mis-information.

[192] In 2020, the U.S. Senate Judiciary Committee unanimously approved S. 3398, the EARN IT Act of 2020, which was aimed at ending the spread of online child sexual abuse material. The bill compromised the ability of social media platforms to offer end-to-end encryption to their users by threatening platforms with liability if their users conveyed CSAM. Maintaining liability protection could have effectively required platforms to be able to understand the communications content they carried, which is inconsistent with EE2E. *See*: Nandita Bose, 'US Senate Committee Approves Anti-Child Porn Bill After Addressing Google, Facebook Encryption Concerns' (*Reuters*, 2 July 2020) <https://in.reuters.com/article/us-usa-legislation-encryption/us-senate-committee-approves-anti-child-porn-bill-after-addressing-google-facebook-encryption-concerns-idINKBN2432NK> accessed 14 November 2020; a 14-member ad-hoc committee of the Rajya Sabha, led by Jairam Ramesh, recommended that law enforcement agencies should be permitted to break end-to-end encryption to trace the distributor of child pornography on social media, *see*: Neha Alawadhi, 'RS Panel Suggests Breaking Encryption to Curb Child Pornograhy Distribution' (*Business Standard*, 27 January 2020) <https://www.business-standard.com/article/technology/rs-panel-suggests-breaking-encryption-to-curb-child-pornograhy-distribution-120012600705_1.html> accessed 14 November 2020.

[193] New Intermediary Guidelines, rule 4(2); To promote national security and law enforcement interests in the U.S., Senators introduced the Lawful Access To Encrypted Data Act, S. 4051, which would have forbidden providers from offering end-to-end encryption in online services and devices unless it could be circumvented by law enforcement, *see*: Riana Pfefferkorn, 'There's now an Even Worse Anti-Encryption Bill than Earn it. That doesn't Make the Earn it Bill ok' (*The Center for Internet and Society, Stanford Law School*, 24 June 2020) <https://cyberlaw.stanford.edu/blog/2020/06/there's-now-even-worse-anti-encryption-bill-earn-it-doesn't-make-earn-it-bill-ok> accessed 14 November 2020.

of achieving any such objective are richer in rhetoric than in practice. Not only does undermining encryption fail as a solution to any of these problems, but it also has the opposite effect of negatively impacting the public interest, human rights, cybersecurity, and the economy.

The online sphere is no longer an adjunct to the offline realities of society. Instead, we live our social and political lives online. It is where we exercise our rights and freedoms. Encryption makes it possible for individuals, communities, and governments to have a private space online, secure from known and unknown threats of surveillance and manipulation. Individuals can communicate and collaborate with each other, and build a democratic society that is strengthened, and not marred, by the ubiquity of the digital dimension. Preserving and strengthening encryption is in the interest of the defining ideals of a democracy - the right to privacy and the right to freedom of expression.

What Carissa Véliz of Oxford University observes in the context of privacy is equally applicable with respect to encryption and its impact on both privacy and security: '[s]ocietal choices about privacy will influence how political campaigns are run, how corporations earn their keep, the power that governments and private businesses may wield, the advancement of medicine, the pursuit of public health goals, the risks we are exposed to, how we interact with each other, and not least, whether our rights are respected as we go about our daily lives.'[194] The future of the rights and freedoms that make India a thriving democracy will be informed in no small part by the government's approach to encryption. The only way forward, if the goal is to boost technology innovation and economic growth, protect individual rights and freedoms, and secure cyberspaces for the nation and the government, is to support and encourage strong encryption. The societal costs of having diluted encryption standards are, simply put, too high.

[194] Carissa Véliz, *Privacy is Power: Why and How You Should Take Back Control of Your Data* (Bantam Press 2020).