INTERNATIONAL ENCRYPTION BRIEF

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

PRINCETON
UNIVERSITY

CITP
CENTER FOR
INFORMATION TECHNOLOGY POLICY

MARCH 2021

The Encryption Debate in India: 2021 Update

Trisha Ray

Carnegie does not take institutional positions on public policy issues; the views represented herein are those of the author(s) and do not necessarily reflect the views of Carnegie, its staff, or its trustees.

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

About the Encryption Working Group

The Carnegie Endowment for International Peace and Princeton University have convened a small group of experts to advance a more constructive dialogue on encryption policy. The working group consists of former government officials, business representatives, privacy and civil rights advocates, law enforcement experts, and computer scientists. Observers from U.S. federal government agencies attended a select number of working group sessions. Since 2018, the working group has met to discuss a number of important issues related to encryption policy, including how the relevant technologies and uses of encryption will evolve in the future.

This brief and its companion pieces detailing the encryption debates in a select number of key countries and regions—Australia, Brazil, China, the European Union, Germany, and India—were prepared by local and area experts at the request of the Encryption Working Group. They are designed to shine light on key drivers of the debates in these countries, how they have evolved in the last five years, and the divergent approaches taken by different governments. The briefs do not take a position on encryption policy, rather they provide analysis of how debates about encryption have evolved internationally. The views are the authors' own and do not necessarily reflect the views of Carnegie or the Encryption Working Group.

Introduction

The direction of encryption policy in India remains nebulous, balancing imperatives of the privacy of the individual, the security of digital infrastructure, and government access to personal data, a balance that has only become harder to strike following the unprecedented surge in digitization of government, business, and daily life during the pandemic.

The 2019 edition of the India encryption brief in this series provided a detailed overview of the history of encryption in India, key stakeholders, and emerging regulations. It highlighted three sets of debates that serve as antecedents to the encryption policy landscape in India: law enforcement access to data, the security of emerging digital economy instruments, and platform liability.[1] The continued absence of a national encryption policy, overlaid upon a web of interwoven developments in legislation on data, encryption, and the digital ecosystem, have only complicated these issues further. This review will pick up these three threads as they have developed over the past year.

Securing Digital Infrastructure

The vision for a Digital India, outlined in a 2019 Ministry of Electronics and IT (MeitY) report, hinges on developing and expanding access to digital infrastructure to generate value in a way that empowers its billion-plus population.[2] The realization of this value is predicated on trust, built upon a secure digital ecosystem, and clear, enabling policies and guiding frameworks, of which encryption is a key building block.

The National Encryption Policy (2015) was summarily abandoned after industry, civil society, and media decried it for being "a decryption policy [rather] than an encryption policy."[3] Encryption policy remains confined to sector-specific guidelines.

The Reserve Bank of India (RBI) for instance released its Master Direction on Digital Payment Security Controls in February 2021, mandating multifactor authentication, encryption, digital certificates, and other controls to secure digital payments apps and processes.[4] It does not introduce any new or specific parameters for encryption, however, stating simply that measures "shall be strong, adopting internationally accepted and published standards that are not deprecated/ demonstrated to be insecure/ vulnerable and the configurations involved in implementing such controls are in general, compliant with extant instructions and the law of the land."

The RBI notification followed a handful of widely publicized data breaches: in January 2021, a cybersecurity researcher discovered a data dump of biometrics and masked card numbers on the dark web, coming from a compromised server of Juspay, a payments company.[5] Earlier, in May 2020, an Israeli internet security firm, vpnMentor, reported that financial information, Aadhaar card information, and other personal details of users of BHIM,[6] a mobile payments app, were exposed due to an unprotected public bucket on the website of a partnering organization, the Common Services Centre (CSC).[7]

Both breaches were not severe in terms of their impact on users but do raise questions about the patchy implementation of data security practices. Of particular concern are unsecured public buckets and endpoints, as in the CSC-BHIM case, as well as another prominent leak from Indane, a subsidiary of the Indian Oil Corporation, that affected an estimated 6 million customers.[8] These regular breaches explain why regulators like the Securities and Exchange Board of India and the RBI are keen on shoring up network and data security, including with stronger, standardized encryption and authentication measures.[9]

Platforms Under Fire

In the context of online platforms, the encryption debate in India centers on the ability of government to *trace* and prosecute individuals who spread disinformation and other content that adversely impacts public order and national security, as well as the use of platforms for illegal activities.

The past year has seen a few policy and legal developments in this space, which the overview below briefly captures.

WhatsApp, Traceability, and Public Safety

The 2019 India Encryption Brief highlighted public order concerns—notably a series of mob lynchings targeting minorities that were triggered by WhatsApp forwards—that became the rallying point for Indian government demands that WhatsApp dilute its end-to-end (E2E) encryption.[10] Increasingly, the proliferation of other kinds of illegal content and activities over WhatsApp is also coming to the forefront of legal and legislative action.

The Supreme Court in October 2020 sought a response from the Government of India on a writ petition to devise a verification mechanism for social media to "uproot fake social media profiles" and make it easier to track and trace cyber offenders.[11] The plea is not the first of its kind: in 2018, a number of petitions asked the Madras High Court to direct social media networking services to link user accounts to their Aadhaar cards.[12]

Another specific use case for diluting E2E encryption was a 2020 report by the Ad Hoc Committee of the Rajya Sabha (the upper house of parliament) on pornography, which recommended permitting breaking E2E encryption to trace originators and distributors of child sexual abuse material.[13]

Personal Data Protection Bill and New Intermediary Guidelines

Over a year after it was first drafted, the Personal Data Protection (PDP) Bill was tabled in the Lok Sabha (parliament's lower house) in December 2019. The PDP Bill, if passed, would become the overarching legislation on data processing, storage, and protection across sectors. The bill would also create a new regulatory body, the Data Protection Authority (DPA) to ensure compliance with the act.

Section 24 (1) of the bill requires data fiduciaries to implement necessary security safeguards such as encryption, methods to prevent de-identification, and integrity of personal data.[14]

Concurrently, the newest draft also adds the controversial Section 35, which grants the central government the power to exempt any agency from the act. The bill elicited pushback from civil society and industry: Justice B. N. Srikrishna, chairman of the committee that drafted the bill in 2018, for instance called the 2019 bill "dangerous," saying it will turn India into an Orwellian State.[15]

These concerns are compounded by the Intermediary Guidelines (2021), [16] which state:

> A significant social media intermediary providing services primarily in the nature of messaging shall enable the identification of the first originator of the information on its computer resource as may be required by a judicial order passed by a court of competent jurisdiction or an order passed under Section 69 of the Act by the Competent Authority as per the Information Technology (Procedure and Safeguards for interception, monitoring and decryption of information) Rules, 2009, which shall be supported with a copy of such information in electronic form.[17]

The guidelines also mandate that intermediaries appoint a nodal officer who is available 24-7 to coordinate with law enforcement agencies for compliance with orders.

The Software Freedom Law Center, a pro-bono legal services organization, noted that Section 69 of the IT Act, under which tracing orders would be made, "does not offer adequate procedural safeguards." The grounds for decryption requests under Section 69 as well as those for exemption under Section 35 of the PDP Bill are also excessively broad.[18]

In sum, the PDP Bill advocates for stronger data protections, including encryption on the part of private data fiduciaries, but grants the central government the power to exempt all government agencies from putting in place adequate safeguards on the collection, use, and protection of personal data. The Intermediary Guidelines additionally grant government agencies the power to order intermediaries to make data available for prosecution or prevention of offences, which may involve weakening E2E encryption. An anonymous statement from a senior official, made while MeitY was in the process of formulating the guidelines, would appear to support this assumption: "Notifying the guidelines is the only way to deal with the current situation where content is being created on one platform – like Tik-Tok — and being circulated on other social media like WhatsApp, with companies not able to control it citing end-to-end encryption."[19]

Over the Horizon: A Policy Space in Flux and Alternatives

Presently, the parameters for decryption and tracing requests remain within Section 69 of the IT Act and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009. However, both only truly work when the intermediary holds the decryption key. This fact left E2E encrypted services like WhatsApp in a gray area over which the state is attempting to assert control.[20]

Alternatives to Weakening E2E Encryption

In an attempt to provide a balanced solution to the competing imperatives of strong encryption and privacy on one hand, and law enforcement access on the other, two industry bodies—the National Association of Software and Service Companies (NASSCOM) and the Data Security Council of India (DSCI)—co-published "Discussion Paper: The Road Ahead for Encryption in India" in September 2020.[21] This paper encouraged further discussion and clarification on the following key questions, among others:

The need for an overarching encryption framework, as opposed to existing sector-specific frameworks. This could involve a revitalization of the National Encryption Policy, in a more responsive avatar that addresses concerns raised by privacy advocacy groups and cybersecurity experts.

Alternatives including local key escrow for law enforcement agency access to encrypted information. The paper suggests a local key escrow, whereby the decryption key is stored in the device itself, meaning that decryption will be possible if agencies are in lawful possession of the device in question. This would limit remote decryption and is one pathway that treads the line between access to data for prosecution of legal offences and government overreach.

MeitY, meanwhile, has recently sought to resolve the apparent contradiction between ease of law enforcement access and the digital economy's need for strong data security by emphasizing traceability over decryption. An unnamed official told reporters at the *Economic Times*: "We don't want WhatsApp to decrypt any messages, we have only asked them to trace the source of a malicious message. In the past we have seen malicious messages are relayed in the same area, same region and [that] has led to cases of mob lynching and this doesn't require rocket science."[22] Two anonymous officials, commenting on the new Intermediary Guidelines, said that messaging intermediaries like WhatsApp, Signal, and Telegram can comply with the "first originator" requirement by assigning a "hash constant" to each message to help trace the originator without breaking encryption.[23] The existence of this "hash constant" exception as well as its practicability remains up for question.

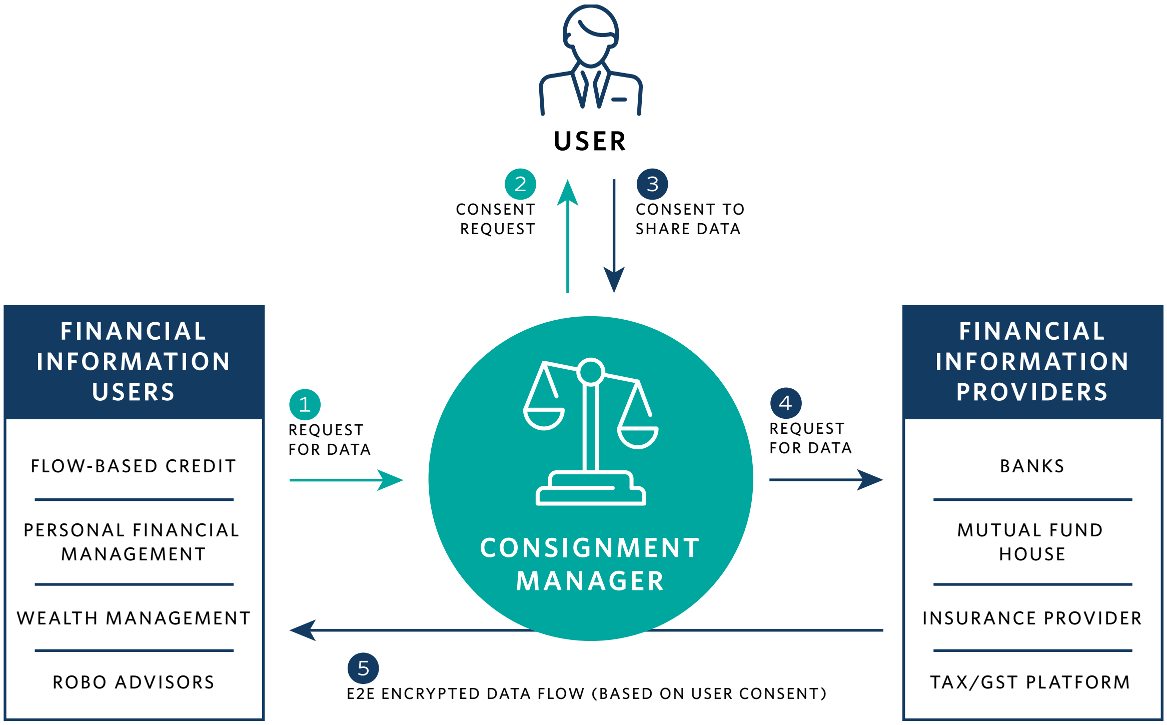
New Developments

New policy proposals put forth in 2020–21 add further nuance to ongoing encryption debates. The Report by the Committee of Experts on Non-Personal Data Governance Framework seeks to create a separate Non-Personal Data Authority for the governance of all data not associated with an identified person, which includes anonymized data.[24] Under technology-related guiding principles, the report mentions homomorphic encryption as a means for preventing the de-anonymization of data.[25]

NITI Aayog's Data Empowerment and Protection Architecture (DEPA) framework was released as a discussion paper in August 2020.[26] DEPA builds upon the PDP Bill's concept of a "consent manager"—a type of data fiduciary that serves as a conduit for data flows between data principals (users) and data fiduciaries who will use said data.

FIGURE 1

India's Data Empowerment and Protection Architecture



SOURCE: *NITI Aayog*

Consent managers cannot access the data, but simply manage access on behalf of the data principal. DEPA also necessitates end-to-end data security, which again appears to create a conflicting pressure on end-use data fiduciaries, expecting them to both be secure but also provide access on demand to government agencies.

The final development to follow in this space is the forthcoming update on the National Cybersecurity Strategy (NCSS). The NCSS call for comments cites cross-border data access and platform regulation as core challenges,[27] and the draft is now pending approval by the cabinet. The strategy's stance on encryption—whether it calls for a strengthening of standards, including key lengths, as well as its take on the risks versus benefits of E2E encryption, or if it remains completely silent on the issue—will either further deepen the fault lines among regulators, government agencies, industry, and users, or provide some much-needed reassurance that the government is willing to consider the principles of necessity and proportionality vis-à-vis decryption.

Conclusion

One year on, the state and direction of encryption in India has grown both more nuanced and more fraught. Some debates and issues have carried into the new decade, notably the legal liability of platforms versus their responsibility to their users; and the need to plug leaks that threaten to erode trust in the nation's nascent digital infrastructure. Optimistically, the evolution of crucial legislation, like the PDP Bill, as well as the long-awaited revitalization of strategy documents like the National Cybersecurity Strategy and the National Encryption Policy, may help square some of these circles. Industry and government bodies have been developing new and creative solutions to these challenges that seek to preserve privacy and aid in traceability of bad actors. In the coming years, observers of these debates should track whether and how the world's largest democracy tests and deploys these privacy-preserving measures.

About the Author

Trisha Ray is an associate fellow with the Technology and Media Program at the Observer Research Foundation.

Notes

[1] Bedavyasa Mohanty, “The Encryption Debate in India,” Carnegie Endowment for International Peace, May 30, 2019, https://carnegieendowment.org/2019/05/30/encryption-debate-in-india-pub-79213.

[2] “India's Trillion Dollar Digital Opportunity,” Ministry of Electronics and Information Technology, February 2019, https://www.meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf.

[3] Mohanty, “The Encryption Debate in India.”

[4] “Master Direction on Digital Payment Security Controls,” Reserve Bank of India, February 18, 2021, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MD7493544C24B5FC47D0AB12798C61CDB56F.PDF.

[5] Harshit Rakheja, “Data Of 10 Cr Digital Payments Transactions Leaked After Attack on Juspay's Server,” Inc42, January 3, 2021, https://inc42.com/buzz/india-data-leak-cardholders-leaked-from-juspay/.

[6] Aadhaar is a 12-digit unique identification number, issued after taking an individual's biometric and demographic information. It is issued by the Unique Identification Authority of India.

[7] “Report: Indian e-Payments App Exposes Millions of Users in Massive Data,” vpnMentor, May 31, 2020, https://www.vpnmentor.com/blog/report-csc-bhim-leak/.

[8] Elliot Anderson, “Indane Leaked Aadhaar Numbers: 6,700,000 Aadhaar Numbers,” Medium, February 19, 2019, https://medium.com/@fs0c131y/indane-leaked-aadhaar-numbers-6-700-000-aadhaar-numbers-3948135239f6.

[9] For more on SEBI, see the SEBI roundup in: Mohanty, “The Encryption Debate in India.”

[10] Mohanty, “The Encryption Debate in India.”

[11] Petitioners Skand Bajpai, Abhyudaya Mishra, “Writ Petition W.P.(C) No. 000799 - 000799/2020,” Supreme Court of India, https://main.sci.gov.in/case-status.

[12] A full list and analysis of court cases on traceability is available here: “The Future of Intermediary Liability in India,” Software Freedom Law Centre, January 2020, p. 15,https://sflc.in/sites/default/files/2020-01/SFLC.in%20-%20Intermediary_Liability_Report_%282020%29_1.pdf.

[13] “Report of the Adhoc Committee of the Rajya Sabha to Study the Alarming Issue of Pornography on Social Media and Its Effect on Children and Society as a Whole,” Rajya Sabha, tabled February 3, 2020, https://rajyasabha.nic.in/rsnew/Committee_site/Committee_File/ReportFile/71/140/0_2020_2_16.pdf.

[14] The Personal Data Protection Bill, 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

[15] Megha Mandavia, “Personal Data Protection Bill can turn India into ‘Orwellian State': Justice BN Srikrishna,” *Economic Times*, December 12, 2019, https://economictimes.indiatimes.com/news/economy/policy/personal-data-protection-bill-can-turn-india-into-orwellian-state-justice-bn-srikrishna/articleshow/72483355.cms.

[16] “Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021,” Ministry of Electronics and Information Technology, http://egazette.nic.in/WriteReadData/2021/225464.pdf.

[17] Per the guidelines, “significant social media intermediary means a social media intermediary having number of registered users in India above such threshold as notified by the Central Government.” And: “social media intermediary means an intermediary which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services.”

18 “Interest of the sovereignty or integrity of India, defense 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.” Section 69(1) of the IT Act, https://www.meity.gov.in/writereaddata/files/The%20Information%20Technology%20Act%2C%202000%283%29.pdf. “(i) in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order; or (ii) for preventing incitement to the commission of any cognizable offence relating to sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order.” Section 35 of the PDP Bill (2019), http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

19 Surabhi Agarwal, “Government Set to Notify New Social Media Norms,” *Economic Times*, April 9, 1010, https://economictimes.indiatimes.com/tech/internet/government-set-to-notify-new-social-media-norms/articleshow/75059440.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

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

21 “NASSCOM-DSCI Discussion Paper: The Road Ahead for Encryption in India,” NASSCOM, September 4, 2020, https://community.nasscom.in/communities/policy-advocacy/nasscom-dsci-discussion-paper-the-road-ahead-for-encryption-in-india.html.

22 Anandita Singh Mankotia and Megha Mandavia, “After Pegasus Spying Row, India Asks WhatsApp to Explain Privacy Breach,” *Economic Times*, November 2, 2019, https://economictimes.indiatimes.com/tech/internet/after-pegasus-spying-row-india-asks-whatsapp-to-explain-privacy-breach/articleshow/71851802.cms.

23 Deeksha Bhardwaj, “Hash Constant: Govt’s Solution to Tracing Originator of Viral Messages,” *Hindustan Times*, March 2, 2021, https://www.hindustantimes.com/india-news/hash-constant-govt-s-solution-to-tracing-originator-of-viral-messages-101614667706841.html.

24 “Report by the Committee of Experts on Non-Personal Data Governance Framework,” Ministry of Electronics and Information Technology, July 2020, https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf.

25 Homomorphic encryption is an encryption method that enables the processing of data without breaking encryption. See https://www.thesslstore.com/blog/what-is-homomorphic-encryption/.

26 “Data Empowerment and Protection Architecture,” NITI Aayog, August 2020, https://niti.gov.in/sites/default/files/2020-09/DEPA-Book_0.pdf.

27 “National Cyber Security Strategy 2020 (NCSS 2020) Call for Comments,” https://ncss2020.nic.in/.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

CarnegieEndowment.org