INTERNATIONAL ENCRYPTION BRIEF

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

PRINCETON UNIVERSITY

CITP CENTER FOR INFORMATION TECHNOLOGY POLICY

MAY 2019

The Encryption Debate in India

Bedavyasa Mohanty

The Encryption Debate in India

Bedavyasa Mohanty

For your convenience, this document contains hyperlinked source notes as indicated by teal colored text.

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.

CONTENTS

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 briefing paper 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.

The Encryption Working Group will continue its efforts to study this important issue and plans on releasing further briefings on aspects of the encryption policy debate.

Members of the Encryption Working Group include:

Jim Baker
Former General Counsel, Federal Bureau of Investigation

Katherine Charlet
Program Director, Technology and International Affairs, Carnegie Endowment for International Peace

Tom Donahue
Visiting Fellow, George Mason National Security Institute, and former Senior Director for Cyber Operations, National Security Council, White House

Ed Felten
Robert E. Kahn Professor of Computer Science and Public Affairs, Princeton University

Avril Haines
Senior Research Scholar at Columbia University's Columbia World Projects and former Deputy Director, Central Intelligence Agency

Susan Hennessey
Executive Editor, Lawfare, and Senior Fellow in Governance Studies, the Brookings Institution

Chris Inglis
Managing Director, Paladin Capital Group, and former Deputy Director, National Security Agency

Sean Joyce
US Cybersecurity and Privacy Leader, PwC, and former Deputy Director, Federal Bureau of Investigation

Susan Landau
Bridge Professor of Cyber Security and Policy, Tufts University

Christy Lopez
Distinguished Visitor from Practice, Georgetown Law Center

Alex Macgillivray
Board Member, Data & Society, and former Deputy Chief Technology Officer of the United States

Jason Matheny
Founding Director, Georgetown Center for Security and Emerging Technology, and former Director, Intelligence Advanced Research Projects Activity

Tim Maurer
Co-Director and Fellow, Cyber Policy Initiative, Carnegie Endowment for International Peace

Denis McDonough
Visiting Senior Fellow, Technology and International Affairs, Carnegie Endowment for International Peace, and former White House Chief of Staff

Lisa Monaco
Distinguished Senior Fellow, Reiss Center on Law and Security, New York University School of Law, and former Assistant to the President for Homeland Security and Counterterrorism

Laura Moy
Executive Director, Center on Privacy & Technology, Georgetown Law Center

Michelle Richardson
Director, Privacy and Data Project, Center for Democracy and Technology

Ronald L. Rivest
Institute Professor, Massachusetts Institute of Technology

Ari Schwartz
Managing Director of Cybersecurity Services, Venable LLP

Harlan Yu
Executive Director, Upturn

Denise Zheng
Senior Associate (Non-resident), Technology Policy Program, Center for Strategic and International Studies

Note: This is not a comprehensive list of all members. Some wish to remain anonymous for the time being and to contribute in their personal capacity.

Despite being a rapidly maturing digital economy, India has not yet experienced its version of the Crypto Wars. However, policy developments—such as the draft Personal Data Protection Bill, the draft e-commerce policy, and the proposed amendments to India's intermediary liability laws—indicate that regulation on encryption based on its perceived hindrance of lawful data collection is imminent. The exact nature of the regulation remains undecided because of a need to balance law enforcement needs, apprehensions about the proliferation of unsecured devices, concerns about the security of digital payments and freedom of expression. Whatever the outcome of this debate, it will significantly affect India's newly recognized fundamental right to privacy, burgeoning economic activity in cyberspace, and security architecture as a whole.

Introduction

The technology policy debate in India has undergone a tectonic shift in the past few years. This can be generally attributed to the natural progression of technology-based services and their growing importance for commerce and the delivery of welfare. However, three specific developments have made cyber governance a top policy priority. First, in 2014, the Modi government set an unprecedented goal for Aadhaar—India's national biometric identity program—to enroll over 1 billion Indian citizens and their sensitive personal information into a centralized database. By February 2018, there were 1.17 billion Aadhaar card holders. Aadhaar has not only made data a part of the public infrastructure but also made technologies like encryption critical to protecting India's national security. In fact, the Indian government often touts the strength of encryption used by Aadhaar's central database when it is accused of mismanaging the identity program.

Second, in 2017, a nine-judge bench of the Supreme Court recognized the right to privacy as a fundamental right under the Indian Constitution. The ruling reconciled over six decades of conflicting judicial pronouncements on the issue.[1]

Third, in 2018, the Ministry of Electronics and Information Technology (MEITY) finalized the draft of India's first comprehensive legislation on data protection and will soon table it in the parliament. The law, when passed, will introduce new accountability measures for technology companies and create a specialized institution to oversee data protection enforcement. All of these developments have put the security of India's information architecture at the forefront of policymaking. And, yet, the future of encryption, a fundamental building block for a secure information ecosystem, remains uncertain.

The Indian government's present adversarial posture toward regulating online content primarily stems from a lack of capacity to address cyber and cyber-enabled offenses. This is compounded by an inability, under the Mutual Legal Assistance Treaty (MLAT), to systemically gain access to electronic evidence stored abroad. For example, encryption has often been at the core of the confrontation between Indian law enforcement and U.S. technology companies. Indian laws, especially the Information Technology Act 2000, bestow wide powers on law enforcement agencies to intercept and decrypt communications, but these powers are rarely exercised to gather electronic evidence. Instead, agencies rely on legacy search-and-seizure provisions like Section 91 of the Code of Criminal Procedure 1973, when seeking access to electronic communications.[2] In the instances where rules around decryption have been invoked, they have largely been reactive to social and political developments (discussed in later parts of the brief) and caused significant friction between the Indian government and the tech community. The most prominent example is the Indian government's action vis-à-vis BlackBerry between 2007 and 2012, where it sought law enforcement access to the encrypted Blackberry Messenger and Blackberry Internet Service email. This episode served as an early indicator of the pressures for data localization and for reforming the MLAT framework.

This brief begins by chronicling the evolution of cryptography in India over the last few decades. It then highlights developments in technology that have been pivotal to the creation of laws and policies around encryption. In doing so, the brief reveals the tenuous position that encryption—especially mass-market encryption used widely for personal communications and digital transactions—currently occupies and discusses existing policy options to regulate it.

Background

The Early Days

Recognizing the internet's potential for e-commerce and digital banking, India formally began developing its information technology policy in the late 1990s. Notably, the Information Technology Act 2000, mandated the use of digital signatures for authentication, verification, and nonrepudiation of online transactions. The act also endorsed the use of Public Key Infrastructure (PKI) for encrypting, signing, and authenticating transactions.[3] At this time, however, PKI and other sophisticated encryption tools were not readily available in India. The first Internet Banking Guidelines released by the Reserve Bank of India (RBI) acknowledged this reality. The guidelines recommended 128-bit Secure Socket Layer (SSL) encryption as an alternative to PKI for ensuring browser security. Similarly, the Securities and Exchange Board of India (SEBI) recommended making 128-bit encryption the default for e-commerce.

Sophisticated encryption products were unavailable for three primary reasons: lack of technical know-how, departmental limitations on the use of encryption, and export restrictions in more mature markets like the United States. For instance, in 1997, Gulshan Rai (now India's national cybersecurity coordinator in the prime minister's office) bemoaned that due to license restrictions in other countries, encryption products with a key length of 56 bits or higher were not available in India. And India's tech industry was not equipped to develop its own cryptographic software. Experts speculate that export controls, such as those under the Wassenaar Arrangement, may have contributed to the lack of domestic capacity.

Export Controls

Export controls also caused great concern within India's security establishment. U.S. export controls only allowed the sale of encryption products overseas if their key length was below 40 bits, effectively ensuring that the U.S. National Security Agency could break into them if required. In 1999, India's equivalent security agency, the Defence Research and Development Organisation, issued a red alert for all network security software originating from the United States. In addition, the Central Vigilance Commission reportedly considered making it mandatory for Indian banks and financial institutions to use only domestically developed software.[4] This policy was never formalized, however, and India's crypto ecosystem remains open without restrictions on cross-border transfer of encryption technologies.

But this openness does not mean there is less concern now or that there have not been any encryption-related failures. In October 1998, equipment recovered from militant groups in Kashmir included, among other things, electronic keyboards capable of ciphering and deciphering 45 characters at a time and modems capable of transmitting "ciphered messages."[5] In the coming months, when the Indian army was embroiled in the Kargil conflict with Pakistan, their inability to listen in on digitally encrypted communications of the Pakistani Army was considered a significant shortcoming. Subsequently, the Kargil Review Committee, set up in 1999, recommended that India develop encryption and decryption capabilities for the country's intelligence agencies.

1999 License Restrictions

In 1999, the Department of Telecommunications (DOT) also introduced restrictions on the strength of encryption that its licensees—the internet and telecommunications service providers—could use on their networks. The DOT's amendment to the Internet Service Provider (ISP) license mandated that individuals, groups, and organizations could only use a 40-bit key length without prior authorization. Higher key lengths would require the provider to obtain permission and submit decryption keys, split into two parts, to the government. The same amendment also mandated that ISPs would have to provide (at their own cost) to security agencies facilities for monitoring communications. Providers were required to dedicate a room accessible only to the security agencies capable of centrally monitoring traffic from all switches and routers across the country.

These license provisions are still in effect today, with a few exceptions. Notably, when India migrated to a Unified License in 2013—to converge internet and telecom services—the 40-bit ceiling on key lengths was dropped without explanation. And while the license continues to prohibit providers' use of "bulk encryption," the term itself remains undefined and the provision is seldom enforced. Restrictions such as these may ease law enforcement concerns, but are equally likely to be misused by intermediaries to gain unauthorized access to data.

Service providers currently deploy network-wide encryption in compliance with international standards on information technology, however, the prohibition on bulk encryption causes some service providers to impose regressive and unenforceable terms and conditions every so often. For example, in 2017, one ISP called You Broadband sought to prevent customers from adopting "any encryption system that prevents or in any way hinders" the provider from accessing user data. The ISP revised the terms and conditions soon after the media caught wind of the issue.

Key Actors

As the debate on encryption plays out in the coming years, it will involve a wide range of state and nonstate actors. On the side of the Indian government, multiple agencies—from ministries to sectoral regulators—are likely to weigh in. MEITY, which is tasked with promoting e-governance, innovation, and the overall security of India's cyberspace, will be the nexus for all policy decisions concerning encryption. Both the draft National Encryption Policy 2015 (now withdrawn) and the amendments to the intermediary liability laws are products of deliberations coordinated by MEITY. At the forefront of the deliberations lies the national cybersecurity coordinator, located within the prime minister's office and tasked with maintaining India's national security in the cyber domain.

Bodies like the RBI and SEBI also weigh in on encryption debates, albeit largely in an advisory fashion. The Department of Telecommunications, under the Ministry of Communications, oversees licensing terms with internet service providers and suggests standards for encryption used on their networks.

The Ministry of Home Affairs, which handles law enforcement, retains the powers to authorize and oversee orders for the interception and decryption of information. The ministry notifies the general public of the agencies authorized to issue interception orders and, under normal circumstances, a secretary within the ministry approves the orders.

As for nonstate actors, prominent industry associations—such as NASSCOM and its data protection arm, the Data Security Council of India—engage with the discourse by establishing and publicizing best practices, standards, and training initiatives in cybersecurity and privacy. Civil society organizations, such as the Internet Freedom Foundation and the Software Freedom Law Center, play an active role in public outreach and public consultations with government institutions. The Centre for Communication Governance at the National Law University in New Delhi is dedicated to the study of digital rights and regulations in the country and is also an active stakeholder in the encryption debate, publishing and disseminating literature on the subject. Think tanks and research organizations, such as the Observer Research Foundation and the Centre for Internet and Society, produce original research to help bridge the gap between the technology community and policymakers in India.

Legal Framework

The Information Technology Act 2000, was amended in 2008 to bring it in line with rapidly evolving technology. One significant change was the insertion of Section 84A, which empowered the government to prescribe the modes and methods for encryption to promote e-governance and e-commerce.[6] Another change fleshed out Section 69, which authorizes the central and state governments to intercept and decrypt any information necessary for protecting national security, preserving public order, or investigating crime. The section also requires users and service providers to assist law enforcement and government agencies with accessing this information.[7]

Soon after passing these amendments, the government developed the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 (hereafter referred to as the Decryption Rules). These rules clarified the parameters of decryption and the required protocol. For instance, decryption assistance was defined as allowing access to information to the extent possible and only when the intermediary has control over the decryption keys.[8] Presumably, this removes the onus from end-to-end encryption providers to decrypt information on their networks.

Arguably, the most controversial provision under the Decryption Rules is Rule 9, which deals with the specificity of a decryption request, usually issued by one of the ten agencies authorized to intercept communications. Rule 9 states that an order for decryption can relate to any information sent to or from a "person or class of persons" or relate to "any subject matter." The breadth of the provision therefore allows nontargeted decryption requests that can potentially be directed toward minorities and other vulnerable groups.

Main Issues

BlackBerry Case, 2007–2012

The first notable "encryption versus national security" incident occurred when the Indian government directed Research in Motion's (RIM) BlackBerry to give law enforcement access to its encrypted data. RIM, as a device manufacturer, was not subject to the encryption controls applicable to telecom companies under the license agreements. On December 31, 2007, realizing that they could not monitor content sent over BlackBerry devices, the DOT asked the company to stop its services in India. The Indian government threatened to direct telecom operators to cut off BlackBerry services unless the company made the lawful interception of encrypted communications possible in India. These demands only intensified when it became known that the individuals involved in the 2008 terror attacks in Mumbai had used BlackBerry devices to stay in contact with their handlers in Pakistan.

India's Intelligence Bureau rejected RIM's intermediate solutions, such as reducing its 256-bit Advanced Encryption Standard, since they could hamper user privacy. Instead, the Indian government demanded that RIM relocate its servers to India and hand over its encryption keys. After a protracted battle, in 2010, RIM finally agreed to locate its servers in India and, in 2012, agreed to submit the plaintext of communications sent over the BlackBerry Messenger to Indian law enforcement agencies. However, this set a precedent that the government could lower the security of a communication service by sustaining backchannel pressure and strong-arming the operator. It may have also contributed to the reduction in Blackberry's popularity and market share in the following years.

Draft National Encryption Policy 2015

The next significant incident occurred in September 2015, when the central government circulated the draft National Encryption Policy. The policy aimed to establish protocols and algorithms for encryption, key exchange, and digital signatures for government agencies, businesses, and individual users. In a departure from previous provisions, such as those under the Unified Services license, this policy did not directly impose any limits on the strength or nature of deployed encryption. Instead, it allowed the unbridled use of encryption as long as users cooperated with law enforcement agencies when asked to do so. To ensure this cooperation, the policy imposed stringent obligations on businesses and citizens alike. The policy required:

- Vendors of encryption products (except those providing mass-use services like SSL and Transport Layer Security) to register their products with the government and submit working copies of software and hardware used for encryption.[9]
- Service providers using encryption to enter into an agreement with the Indian government.[10] While the nature of the agreement was not clarified, this was a precondition to doing business in India.
- Businesses to hand over the encrypted text, plaintext, hardware, and software used for encryption upon receiving a request from law enforcement.[11]
- Users of encryption to retain the plaintext of encryption on their devices for ninety days, in the event that law enforcement sought access to this information.[12]

Unsurprisingly, the draft policy faced a massive backlash from technologists, civil society, and the media, causing it to be withdrawn within a few days of being released for public comment. It was clear from the policy's language that its goal was not securing user data but rather ensuring that government agencies could access data in an expeditious manner. In this sense, it was more a decryption policy than an encryption policy.

Critics argued that the policy's provisions were neither enforceable nor technologically feasible. For instance, many noted the wide availability of global encryption tools online. If the Indian government decided to ban an unregistered product, users could always find alternatives on the internet. The ambiguity within the policy also indicated that it may have been an attempt to install backdoors into widely used products and services. The mandate to submit working copies of hardware and software used by the vendor to encrypt data only supported this theory. In the case of end-to-end encryption, where backdoors would be of little use, the policy obligated users to store plaintext of communications—potentially conflicting with the right against self-incrimination under the Indian Constitution.[13]

Ultimately, the government disavowed the draft, stating that the policy's language did not reflect the government's "final view" on the matter.

Draft Personal Data Protection Bill 2018

In the recent years, the Indian government has assumed a protectionist stance toward personal data. It has recognized privacy as a fundamental right and the need to respond to the misuse of personal data by private companies. Controversies like the Cambridge Analytica scandal and allegations of anti-conservative bias within Twitter have made the Indian government increasingly concerned about losing strategic control over the data ecosystem. Consequently, demands for localizing user data within Indian borders have now become a familiar refrain.

The draft Personal Data Protection Bill 2018, for instance, mandates that sensitive personal data be stored on mirror servers in India and all critical personal data related to Indian citizens be processed domestically. However, if passed, the bill is likely to affect privacy adversely and raise the cost of compliance for technology companies. Without an accompanying encryption policy in place, law enforcement will have greater access to private data without any additional oversight. The draft National Policy Framework for E-Commerce currently under consideration by the Ministry of Commerce and Industry similarly endorses data localization and calls upon MEITY to fast-track the draft National Encryption Policy. It has been speculated by commentators that this means re-introducing the 2015 policy rather than an entirely reworked version—which, for the reasons described above, is cause for concern.

Recent developments in India's encryption debate have been driven primarily by internal and national security priorities within the government. But in addition to the threat of foreign surveillance, the Indian government has also become seriously concerned about the perceived threat of encryption to public order. In particular, WhatsApp, a service used by over 200 million Indians, has become the focus of attention.

WhatsApp and Public Order

Over the last two years, approximately thirty individuals have reportedly been killed by lynch mobs agitated by WhatsApp forwards. The forwards themselves appear to be part of coordinated misinformation campaigns that use edited videos and images to warn people of child abductors in their area. This has caused entire communities—especially in rural and underdeveloped areas—to become suspicious of "outsiders," often leading to mob violence.

In failing to make arrests and ensure public order, the Indian government has chosen to ascribe blame to WhatsApp's end-to-end encryption. It has demanded that WhatsApp's messaging service allow tracing to help identify the original sender of messages. WhatsApp has so far resisted this demand and instead implemented other measures, such as adding labels to forwarded messages and restricting the forwarding of messages to five individuals at a time. Given WhatsApp's resistance, combined with apprehensions around the spread of fake news in the run up to the general elections in April and May 2019, the government introduced amendments to its intermediary guidelines. The amendments are likely to have a significant bearing on encryption.

Draft Amendments to Intermediary Guidelines

On December 24, 2018, MEITY released draft amendments to the Information Technology (Intermediary Guidelines) Rules 2011. The amendments require intermediaries—defined under Indian law to include ISPs as well as communication platforms—to trace the originator of information on their platform when ordered to by an authorized government agency.

On communications platforms, this would entail examining a chain of forwards to track down who composed the original message or first uploaded the media file in question. For end-to-end encrypted services, this is not technologically feasible because the communication service providers do not have access to the message content. While MEITY has insisted that the traceability requirement does not automatically mean breaking encryption, an international coalition of civil society organizations and security researchers believes that to comply some companies would have to reduce encryption, introduce backdoors, or roll back end-to-end encryption entirely.

Outlook

Prime Minister Narendra Modi's administration is increasingly looking at the impact of technology on security. The National Security Council secretariat has always been concerned about the inordinate power that global technology companies exercise with limited accountability to foreign governments. In 2014, India's national security adviser, Ajit Doval, highlighted how a significant amount of control over information systems is concentrated in the United States with little accountability to other governments. Previously, sectoral regulators like RBI and SEBI seemed to be in favor of strengthening the overall security of information systems by recommending stronger encryption standards. That seems to be changing. Earlier this year, RBI was among the first Indian agencies to mandate the local storing of data for financial services. MEITY and the Ministry of

Commerce made similar mandates soon after. Other regulators, like the Telecom Regulatory Authority of India, are also likely to wade into the data privacy debate once again.

While it is unclear how the issue will finally be resolved, the Indian government seems to be increasingly leaning toward a regulatory framework where U.S. technology companies become more accountable to Indian policymakers and actively respond to law enforcement demands, even if it comes at the cost of securing communications.

About the Author

Bedavyasa Mohanty is a lawyer by training and an associate fellow with the Observer Research Foundation's Cyber Initiative. His research spans encryption, cross-border data sharing, and the regulation of lethal autonomous weapon systems. As a Grotius Fellow, Bedavyasa will be pursuing graduate studies at the University of Michigan Law School.

The author would like to thank Ananth Padmanabhan and Cherian Samuel for their review of the manuscript.

Notes

1 K. S. Puttaswamy v. Union of India, Writ Petition (Civil) No. 494 of 2012 (Sup. Ct. India Aug. 24, 2017).

2 Section 91 authorizes any law enforcement agent to request the submission of any document or thing in possession of any person if necessary for a criminal investigation. For a broad overview of data collection practices by Indian law enforcement agencies, see Bedavyasa Mohanty and Madhulika Srikumar, "Hitting Refresh: Making India-US Data Sharing Work," Observer Research Foundation, Special Report no. 39 (August 2017) available at: https://www.orfonline.org/research/hitting-refresh-india-us-data-sharing-mlat/.

3 Section 3, Information Technology Act 2000.

4 Mayur Shetty, "Red Alert Issued Against US Network Software," *Economic Times*, January 12, 1999.

5 "Arms From Kashmir Draw Crowds," *Hindu*, October 23, 1998.

6 Section 84, Information Technology Act 2000.

7 Section 69, Information Technology Act 2000.

8 Rule 2(g)(i), Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption Rules) 2009; and Rule 13(3) Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption Rules) 2009.

9 Clause V(1), Draft National Encryption Policy 2015.

10 Clause IV(6), Draft National Encryption Policy 2015.

11 Clause IV(4), Draft National Encryption Policy 2015.

[12] Clause IV(5),(7), Draft National Encryption Policy 2015.

[13] See, *Selvi v. State of Karnataka* (2010) 7 SCC 263 and the right of an accused against compulsion to impart personal knowledge about a relevant fact as protected under Article 20(3), Constitution of India. Also see, Bedavyasa Mohanty, "Going Dark in India: The Legal and Security Dimensions of Encryption," ORF Occasional Paper no. 102, December 2016, available at: https://www.orfonline.org/research/going-dark-in-india-the-legal-and-security-dimensions-of-encryption/.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

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

CarnegieEndowment.org