CARNEGIE INDIA

WORKING PAPER

SEPTEMBER 2021

Understanding the Encryption Debate in India

Anirudh Burman and Prateek Jha

Understanding the Encryption Debate in India

Anirudh Burman and Prateek Jha

Research for this paper was made possible in part by support from WhatsApp. The views expressed herein, however, are the responsibility of the authors alone. The paper is an output of Carnegie India's Technology and Society Program.

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

Carnegie India
Unit C-5 & C-6, Edenpark,
Shaheed Jeet Singh Marg
New Delhi – 110016, India
P: +011 4008687
CarnegieIndia.org

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

Contents

Summary

Encryption has become a contentious instrument for protecting the security and confidentiality of online communication. Rapid digitalization in the past decade has led to the proliferation of domestic and foreign online communication services that use encryption and, consequently, pose challenges to national security bodies and law enforcement agencies (LEAs). To address these challenges, the Indian government introduced new regulations in February 2021.

These regulations require large social media platforms to enable traceability, or the ability to provide information concerning the originator of online communications. Technology companies and privacy activists have opposed such a move on the grounds that traceability would require the breaking of the end-to-end encryption used by many online communication platforms like WhatsApp and therefore would compromise the security of online communications on such platforms.

This traceability requirement, however, is only the latest development in a drawn-out, contentious debate over the use of encryption. The contestation between maintaining higher degrees of online security and issuing new rules to grant technological exceptions for security agencies and LEAs is not specific to India. One of the first serious discussions on the issue took place in the United States in the 1990s, when public opposition warded off an early government attempt to sidestep encryption protections with a court order.

In the past decade, the use of encryption has only grown more pronounced. The revelations that the United States' National Security Agency was collecting vast amounts of communications data led to the introduction and increased adoption of end-to-end encryption for online communications. End-to-end encryption is now used widely by online communication platforms like WhatsApp, Signal, and Threema. Its use presents law enforcement and national security agencies with new challenges. Even though these agencies today have greater and easier access to more information than ever before, the absolute confidentiality provided by encrypted online communication platforms makes it harder for these agencies to engage in real-time surveillance to investigate crimes and identity wrongdoers.

While some policymakers from India and other countries argue that encryption must only be weakened to solve specific problems, most experts agree that, as of today, there is no technological solution that would weaken encryption for specific law enforcement and national security purposes, while managing to maintain preexisting levels of security and confidentiality for general use. The introduction of any mechanism for specific access would, it is claimed, introduce both known and unknown vulnerabilities into these communications platforms. Such a mechanism would have a systemic effect on all online communication dependent on encryption for ensuring security and confidentiality.

In India, these developments create challenges in specific ways. For example, India reports the highest number of child pornography cases worldwide, and encrypted communications makes it difficult to identify culpable parties. Similarly, as India has digitized rapidly, there has been a surfeit of fake and offensive online news that has, in some cases, led to mob lynchings. In addition, terrorist networks have been found to be using encrypted communication channels while planning and carrying out terrorist attacks in India.

Over the years, the Indian government's approach to encryption has responded to these concerns in a variety of ways. Indian financial regulators mandated the use of encryption for banking and financial services as they realized the security of such transactions was best protected through encryption. At the same time, the Indian government prohibited telecom operators from implementing bulk or mass encryption in telecommunication services. Starting in 2015, the government introduced different regulatory proposals requiring that messaging platforms and other communication service providers provide plaintext copies of communications to Indian government agencies on request. These proposals, however, faced significant opposition and were withdrawn.

Earlier in 2021, the Indian government's new rules requiring traceability have been officially notified. The mechanisms through which they will be implemented are not yet clear. It is also unclear if these rules are the last demands the Indian government will make to weaken encryption, or whether further demands will arise in the future. To weigh the relative benefits and drawbacks of the Indian government's proposal, analysts should consider relevant factors such as (but not limited to) whether such changes will offer law enforcement officials the access they desire, how the security of encrypted communications will be affected, and how citizens' civil liberties will be impacted, among others.

Introduction

Encryption and cryptographic techniques for preserving the security of online communication have become increasingly contested in India. Rapid digitalization in the past decade has led to the proliferation of domestic and foreign online communication services that use encryption and, consequently, pose challenges to national security bodies and law enforcement agencies (LEAs). To help overcome these challenges, the Indian government issued controversial new rules in February 2021 that require messaging communication providers to supply information regarding the originators of messages. Many providers argue that this requirement significantly weakens the end-to-end (E2E) encryption they deploy.[1]

The contestation between maintaining higher degrees of online security and issuing new rules to grant technological exceptions for security agencies and LEAs is not specific to India. Conflicts between LEAs and companies that use encryption to protect personal data and communication have become public in many countries. For example, in 2016, there was a contentious public debate in the United States when the Federal Bureau of Investigation asked Apple to provide a backdoor to the smartphone of a suspected criminal by breaking its encryption protections.[2] Apple refused. While the bureau found a workaround, this did not create a durable solution to the issue.[3] In 2019, the Australian government passed a law that enables government agencies to force businesses to break encryption.[4] The law has faced opposition from those arguing that this approach will weaken encryption and have adverse economic consequences.[5] And in October 2020, the LEAs of the Five Eyes intelligence-sharing pact (which includes Australia, Canada, New Zealand, the United Kingdom, and the United States) issued a statement that called on technology companies to find a solution to the issue of E2E encryption.[6] India supported this statement.[7]

On the one hand, thanks to digitalization, India's security agencies and LEAs now have access to significantly more types of data—via mobile devices, over-the-top (OTT) platforms, and cloud storage, for example; they therefore can tap into more personal information for surveillance and investigation purposes. And for service providers, advances in encryption offer obvious benefits in terms of ensuring confidentiality, protecting the security of online communications and transactions, and authenticating the identities of individuals. But security agencies and LEAs argue that as more forms of secure and confidential communication become widely available, malicious actors are increasingly using them as shields to conceal criminal or terrorist activities. They further assert that the demands to cope with the negative effects of digitalization currently outweigh the advantages.

While other countries are dealing with similar issues, the solutions to India's concerns must reflect its particular legal and market structures and its security and law enforcement imperatives. The growth of mobile phone usage, internet access, and broadband networks has led to the significantly increased usage of OTT services for messaging, voice calls, and other forms of communication. Many of the industry's major companies, such as WhatsApp and Signal, use E2E encryption. OTT messaging services are provided by businesses who are not telecom service providers.[8] Therefore, these services function very differently from traditional infrastructure, such as phone lines and towers.

This first paper in a series explores the prevailing tensions and countervailing demands in the use of E2E encryption in the context of India's online communications. A second paper will assess the possible pathways to a solution for India. This paper will detail the evolution of the debate on encryption in India and what has led to the government's recent rules that mandate traceability. Finally, it will propose a framework for analyzing the merits and demerits of possible policy designs.

Encryption and Its Role in Securing Online Communications

Indian law defines encryption as the process of converting plaintext into text that cannot be deciphered or cannot be accessed without using a decryption process.[9] A report of the U.S. National Research Council describes the process of cryptography and encryption as follows:

> In the traditional application of cryptography for confidentiality, an originator (the first party) creates a message intended for a recipient (the second party), protects (encrypts) it by a cryptographic process,

> and transmits it as ciphertext. The receiving party decrypts the received ciphertext message to reveal its true content, the plaintext. Anyone else (the third party) who wishes undetected and unauthorized access to the message must penetrate (by cryptanalysis) the protection afforded by the cryptographic process . . . .[10]

Encryption increases the security of stored information on devices and that of online transactions and communications so as to ensure that transmitted data are not altered or intercepted.[11] These safeguards contribute to increased public confidence in storing and sharing information about, for example, one's health, payments, finances, political views, and sexual orientation. Encryption is also essential for protecting national security and for preventing corporate espionage through the interception of mobile communications.[12]

The use of E2E encryption is particularly relevant for communications using mobile phones. A 2017 U.S. government study summarized the threats to consumers:

> . . . call interception and monitoring, user location tracking, attackers seeking financial gain through banking fraud, social engineering, ransomware, identity theft, or theft of the device, services, or any sensitive data. This puts at risk not just mobile device users, but the carriers themselves as well as other infrastructure providers."[13]

For this reason, many global standard-setting organizations in the mobile ecosystem now require support for encryption.[14]

Historically, many governments have been opposed to granting the public access to strong encryption tools.[15] Unrecoverable encryption prevents LEAs from accessing transcripts of online communications, thereby denying them a useful tool for prosecution.[16] This is especially so because of the decoupling of services and the physical hardware used to provide the services. For example, the OTT service provider can be in a different country from the sender or receiver, and the signaling path (links that carry call setup messages) can differ from the voice path (links that carry the conversation).[17]

One of the earliest and most widely known proposals for a solution to the encryption issue was presented in the United States in the 1990s. The administration of former president Bill Clinton sought to introduce an encryption device in the form of a chipset called the Clipper Chip.[18] The Clipper Chip would encrypt voice and text communications, but the U.S. government and its approved agencies could decrypt communications that used this technology with a court order. This proposal received significant backlash and was dropped entirely.[19] However, another proposal—an export-control regulatory regime preventing the dissemination of advanced cryptographic technology to other countries—was instituted, and some elements of it are still in place.[20]

Yet, over time, policymakers came to realize the benefits of encrypted communications and their role in protecting the online economy. In the United States, export controls on cryptography were relaxed. Similarly, Indian government agencies began permitting the use of stronger encryption for securing communications.[21]

However, the technological hurdles to accessing encrypted communications create significant challenges for national security agencies and LEAs. The latter, in particular, face difficulties in (1) tracing and authenticating the identities of the communicating parties, (2) carrying out real-time monitoring and wiretapping, and (3) avoiding detection by the relevant parties while accessing the communications.[22]

In E2E encryption, only the computers or devices being directly used by the parties have access to the encryption and decryption keys.[23] This process involves encrypting conversations at both ends of the communication—the sender as well as the receiver of the communication. A public key is used to encrypt the message, while a private key, which only the receiver has access to, is used to decrypt it.[24] This prevents the communication from being compromised if any other part of the system is compromised. E2E encryption for online communication is used to secure what is termed data in transit, as it travels from one device or account to another. Meanwhile, data at rest—the term for information stored on a particular device, cloud service provider, or other location—is secured through other encryption mechanisms.[25]

There are also less secure forms of encryption where the service provider has access to the decryption key. In such cases, they can decrypt the information without the intervention of the message's sender or receiver.[26] This means that LEAs can access such communication with the cooperation of the service provider.

In India, while telecom service providers are prohibited from using bulk encryption, (where all communications passing through the system are encrypted) OTT messaging providers like Signal and WhatsApp offer E2E encrypted communication.[27] Table 1 gives an overview of popular OTT messaging service providers in India and their current security practices.

Table 1: Encryption Security and Data Collection Practices of Major OTT Companies

Service	Number of Users	E2E Encryption?	Data Collection Practices	Metadata Collected
WhatsApp	Over 390 million in India[28]	Yes	No copies stored on servers. Users can create and store chat backup data to a Google Drive/iCloud account.	Name, phone number, current profile photo and status message, time when the user has been online, contacts, names of all groups the user is a part of, device type, IP address, device build number, device manufacturer, details of the web/desktop version, and the platform used for WhatsApp Web. All the mobile phone numbers the user chatted with on WhatsApp. Privacy settings information, including for last seen, profile photo, about privacy, and status privacy.[29]
Facebook Messenger	Over 1 billion users globally	Only secret conversations are E2E encrypted	Facebook collects content data unless it pertains to secret conversations, which are E2E encrypted. Data are stored and processed in "the United States and other countries."[30]	Precise location, coarse location, physical address, email address, name, phone number, other user contact info, contacts, photos or videos, gameplay content, other user content, search history, browsing history, user ID, device ID, third-party advertising, purchase history, financial info, product interaction, advertising data, other usage data, crash data, performance data, other diagnostic data, other data types, developers, advertising or marketing, health, fitness, payment info, sensitive info, product personalization, credit info, other financial info, emails or text messages.[31]
Google Messages	Installed over 1 billion times, as of April 2020[32]	Yes, except for short message service (SMS)/ multimedia message service (MMS) messages and group messages	SMS and Rich Communication Service (RCS) messages are stored in Android's local on-device messages database. Only applications with SMS permissions can access this database.[33]	Phone numbers of senders and recipients; timestamps of the messages; IP addresses or other connection information; sender and recipient's mobile carriers; session initiation protocol (SIP), message session relay protocol (MSRP), or common presence and instant messaging (CPIM) headers, such as User-Agent strings that may contain device manufacturers and models; whether the message has an attachment; the URL on the content server where the attachment is stored; and the approximate size of the messages or the exact size of attachments.[34]

Service	Number of Users	E2E Encryption?	Data Collection Practices	Metadata Collected
Telegram	Over 500 million users[35]	Secret conversations, voice calls, and video calls are E2E encrypted; Telegram groups, channels, and one-to-one messages use cloud-based encryption	Cloud chat data are stored across multiple data centers in different parts of the world.	Name, phone number, contacts, and user ID. May also collect IP addresses, information regarding devices and Telegram apps previously used, history of username changes, etc. If collected, this metadata can be kept for a maximum of twelve months.[36]
ShareChat	Over 160 million active monthly users[37]	Unclear	Collects contents of communications, including shared media.[38]	User ID; mobile phone number; password; gender; photo and biography provided on profile; information about users from third-party platforms; mobile carrier–related information; configuration information; IP address; device's version and ID number; platform usage information, such as searches, profiles visited, the identity of other users communicated with, and the time, data, and duration of user communications; and information related to items the user has made available through the platform, such as the date, time, or location that a shared photograph or video was taken or posted. Also contacts, location data, and device information.[39]
Signal	Over 40 million users globally;[40] over 5 million users in India[41]	Yes	No copies stored on servers.	Date and time the user registered with the service, and the last date of connectivity with the service.[42] Also has a feature called "sealed sender," which encrypts data about the sender of messages.[43]
Threema	Over 10 million users globally[44]	Yes	No copies stored on servers.	Does not collect any user information.[45]

The debate around securing online communications was rekindled in the past decade due to the revelations by Edward Snowden, a former contractor working for the U.S. National Security Agency (NSA). In 2013, Snowden leaked evidence to show how the NSA engaged in mass surveillance of millions of Americans and foreign government officials, with the cooperation of telecom service providers.[46] This included access to the metadata of phone calls and access to servers of technology companies such as Google, Apple, and Facebook.

As a result, consumers grew more conscious of the security of their online communications.[47] One report estimated that U.S. technology companies were beginning to suffer serious adverse economic consequences in the aftermath of the Snowden revelations.[48] This was especially so in foreign markets that were major sources of growth potential for U.S. technology companies. Many of these companies adopted E2E encryption because of this fallout.[49] The development of E2E encryption was therefore (at least initially) designed to mitigate the negative consequences of the direct and indirect role of technology companies in aiding government surveillance. In addition, technology companies' embrace of E2E encryption also weakened support for LEAs' demands to weaken encryption for online communications in the United States.[50]

The growing use of encryption does not mean that encryption is completely secure or that it is a comprehensive solution for online security and confidentiality. For one, the proliferation of new communication mediums has also increased the number of forums through which such communication can be tracked and accessed.[51] Email services usually provide encryption from their clients to mail servers, and emails reside in plaintext on the mail servers.[52] Second, there are other vulnerabilities that can be exploited. For example, even though Skype was using E2E encryption, the locations of users could be tracked.[53] Third, data stored or backed up on cloud storage services and local devices are often easier to access.[54] Lastly, as detailed in table 1, most service providers collect a significant amount of metadata that are made available to security agencies and LEAs.

Therefore, while E2E encryption poses challenges for security agencies and LEAs, there are many other mechanisms through which similar data can be accessed. The ability to access such data is, however, also contingent on market structures and the regulatory regime for data access. For example, Indian LEAs are unable to access content data stored in the United States within a reasonable period.[55] Easing these constraints may enable easier access to data stored on devices that are not E2E encrypted. Similarly, the technological capabilities of Indian security agencies and LEAs are crucial determinants in seeking alternatives to breaking encryption. The next section discusses the context in which Indian security agencies and LEAs have made demands for seeking exceptional access to encrypted information.

Encryption and India's Security and Law Enforcement Challenges

The Indian government's demands for weakening encryption have been made for both national security and law enforcement reasons. Multiple government officials have pointed to the difficulties encryption poses in preventing terrorism, fake news, and crimes against women and children.[56] While these difficulties explain why access to encrypted data is needed, the demands conflate many different policy objectives. Until recently, it was hard to disentangle the exact set of criteria that would require the government to access encrypted data. This section examines how the government's demands and corresponding regulatory changes have evolved.

Discussions of Indian government policy on encryption started escalating in the 1990s. The internet was made publicly available in India in 1995 by VSNL, a state-owned network service provider.[57] The Information Technology Act, passed in 2000, mandated the use of digital signatures for online transactions. It endorsed the use of public key infrastructure for these digital signatures.[58] Regulatory bodies such as the Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI) also recognized the need to provide secure transactions over the internet. In 2001, the RBI and SEBI issued guidelines recommending the use of a 128-bit cryptographic protocol, the Secure Sockets Layer, for ensuring browser protection and security for e-commerce.[59]

Following the conflict between India and Pakistan in Kargil in 1999, the Kargil Review Committee noted that adequate attention and resources had not been dedicated toward developing encryption and decryption skills.[60] The committee also highlighted that organized crime and anti-national elements were increasingly relying on encrypted communications.

This historical lack of capacity in dealing with the use of encryption has become more pronounced due to rapid digitalization. Even as digitalization increases, India continues to face terrorist and national security threats and continues to rank high on the Global Terrorism Index.[61] In addition, it has hostile, nuclear-armed neighbors on both its land borders. As communications continue to move online at a tremendous pace, the internet has become a key tool of information exchange for terrorist outfits. Reports by several international bodies attest to this.[62] Reports also document that domestic cells of international terrorist groups have relied heavily on E2E encryption.[63]

The first major act of terrorism that highlighted India's national security concerns with E2E encryption was the attack in Mumbai in 2008. The terrorists were found to be using BlackBerry devices. Consequently, the Indian government required RIM, the device manufacturer, to locate communication servers in India. In 2012, it agreed to hand over messages of communications to Indian agencies in plaintext.[64]

Law enforcement issues arising from online communications have become more widespread over the past decade. Since 2017, there have been several reports of mob violence and lynchings incited by misinformation shared on WhatsApp. Between 2017 and 2018, the spread of unchecked malicious content and fake messages were reported to be directly linked to mob violence. It was said that thirty-four people had been lynched across nine Indian states because of misinformation on social media.[65] LEAs have also cited instances where the spread of misinformation during violent protests or riots have greatly exacerbated already tumultuous law and order predicaments.[66]

Another issue faced by LEAs is the increase in child pornography cases in India. According to the National Center for Missing and Exploited Children (NCMEC), India reported the highest number of child pornography cases in the world between 1998 and 2017.[67] NCMEC argues that its ability to report child pornography cases to LEAs will be severely circumscribed if E2E encryption is implemented without a solution to safeguard children.[68] Though OTT messaging companies like WhatsApp use mechanisms to detect such material, their techniques are limited to the analysis of all unencrypted material such as profile and group photos.[69] WhatsApp bans 300,000 accounts per month for suspected child sexual abuse material in response to user reports.[70]

At the same time, the Indian government has claimed that social media companies refuse to cooperate with it for legitimate law enforcement activities. The problems Indian LEAs face in getting access to personal data from foreign technology companies further exacerbate this issue.[71] In January 2021, protests by some Indian farmers against newly enacted laws turned violent. The Indian government blamed social media companies for not being responsive to official demands for taking inflammatory content down.[72] This specific incident served as the catalyst for recent changes to India's regulations of intermediaries and social media companies, including a mandatory provision requiring OTT communication services to provide information about the originators of messages to LEAs.

While this latest change seems like a major disruption to the existing policy landscape, the Indian government has consistently taken the position that there must be exceptions to encrypted communications on grounds of protecting national security and combating crime. This is evident in the direction of regulatory developments in the country over the last two decades.

Regulatory Developments Regarding Encryption in India

India has an established process for accessing communications built into its laws, but this process is designed primarily to access information from telecom service providers. In 1999, the Indian Ministry of Communications' Department of Telecommunications prescribed that service providers use up to a 40-bit symmetric key length—an archaic standard even for the time—to encrypt their networks.[73] But in 2013, this requirement was dropped. Telecom service providers are now prohibited from relying on bulk encryption, thereby making access to telecom data by LEAs easier.

In 2015, the Indian government released a draft of the country's National Encryption Policy for public comment.[74] In its preamble, the draft policy highlighted the importance of securing internet transactions while also balancing the requirements of national security agencies and LEAs. However, the policy did not prescribe the encryption standards to be used; instead, it merely stipulated that the central government would set the standards for citizens, businesses, and government entities. The draft policy puts the onus on these three categories of service providers to make the plaintext of communications available on demand for law enforcement purposes. The policy faced significant backlash and was withdrawn in September 2015.[75]

In 2018, the Ministry of Electronics and Information Technology introduced a draft of new intermediary rules for social media platforms.[76] The primary aim was to hold social media platforms accountable under law for the spread of fake news. The new obligations included cooperating with LEAs to trace messages to their first originators and using automated tools to remove unlawful content.[77] In 2021, a modified version of these rules was officially notified in the *Gazette of India*.[78] These rules changed the conditions under which intermediaries, including OTT service providers, will enjoy safe harbor protections.[79]

The rules include obligations for two new types of intermediaries—social media intermediaries and significant social media intermediaries. A social media intermediary primarily enables interactions, and exchanges of information, between two or more users.[80] Significant social media intermediaries are those that have a minimum of 50 lakh (5 million) registered users in India.[81]

Obligations for significant social media intermediaries include the appointment of compliance officers, the establishment of a complaint mechanism, and the creation of a notice and appeal mechanism.[82] Some of the new obligations have a direct bearing on E2E encryption. The rules state that significant social media intermediaries engaged primarily in messaging

services must enable identification of the first originator of a message.[83] This stipulation is limited to cases involving serious crimes listed in the rules.[84] However, the rules do not require intermediaries to provide the contents of these messages. Significant intermediaries must also endeavor to use technology-based tools to (1) proactively identify acts depicting rape and child sexual abuse or conduct and (2) display a notice to users trying to access the information.[85] The ministry has the power to place these obligations on any other intermediary as well.[86]

The challenge for OTT messaging companies is that E2E encryption by design does not allow for tracing and filtering, which require tracking every instance a message has been sent.[87] This cannot be done since even the service provider does not have the ability to decrypt and access messages. Therefore, in stipulating these obligations, the Indian government is continuing the trend of making escalating demands on communication service providers, including OTT companies, to break encryption and cooperate more with LEAs.

However, the Telecom Regulatory Authority of India (TRAI) has struck a discordant note. In September 2020, the authority released its recommendations on a regulatory framework for OTT communications services. These recommendations were the product of a stakeholder consultation process that began in November 2018. The TRAI highlighted that "any requirements to cater to get the details of communication in an intelligible form or clear text [plaintext] would either lead to change in the entire architecture of such OTT services which might not provide same level of protection as offered today."[88] It is unclear why the ministry in charge of telecommunications and the TRAI have failed to reconcile these disparate views on the technical feasibility and security consequences of mandating traceability and/or weakening encryption through other means.

In addition, demands for weakening encryption have not always been clear and specific. The Indian government has long sought broad access to encrypted information for equally broad objectives. Draft provisions requiring access have been justified on grounds ranging from protecting India's national security to aiding investigations of serious crimes. Instead of articulating specific requirements, however, the Indian government started by objecting to the use of E2E encryption itself.[89] Concerns over the spread of fake news were added to the list of issues.[90] These demands have become more specific and defined in scope in recent times. In 2018, India's minister for electronics and information technology stated the following:

> When we talk of traceability, we don't talk of decrypting the messages but we insist on location and identification of the original sender of WhatsApp messages when such messages lead to provocation of violence, heinous offences and other serious crimes.[91]

It is this demand that has been codified in the rules published in 2021.

Concerns About Weakening Encryption

OTT service providers such as WhatsApp have claimed that identifying the originator of a message is likely to be an issue since doing so would require them to track every message.[92]

They argue that there is no way to predict which messages the government would want.[93]

An Indian scholar and member of India's National Security Advisory Board asserts that traceability can indeed be implemented by OTT services.[94] However, others state that this proposal does not take into account cryptographic practices used in E2E encryption and that it would make attribution more difficult.[95] In addition, some claim that the proposal would increase systemic vulnerability, since a third party would be able to see when a user is sending a message.[96]

The arguments for and counterarguments against traceability are emblematic of the misunderstanding of the use of encryption. As one scholar argues, the design of even a small-scale encryption process is extremely complex, and even minor changes often introduce fatal flaws.[97] He also points out that any system established for handling requests from government agencies will be vulnerable to fraudulent access from nation-state adversaries.

Prior communication systems that have been altered to comply with similar government requirements have turned out to be insecure—to the extent that vulnerabilities have been exploited for years before being discovered.[98] And, so far, no systems designed to enable exceptional access for surveillance and law enforcement have been able to avoid introducing significant vulnerabilities.[99] Access for legitimate actors creates access opportunities for bad actors too.

This risk is significant, since India fares poorly in global rankings on cybersecurity aptitude.[100] In addition, rapid digitalization exacerbated by the coronavirus pandemic has forced large segments of India's population to transact online for the first time, making them more susceptible to malicious online behavior. Any vulnerability in the security of online communications that becomes a feature of an encryption-based system could therefore increase the risk of harm to vulnerable groups.

Beyond these increased risks, requiring a system of exceptional access would significantly increase the costs of development for small entities for whom "the law enforcement access mechanism could be expected to represent almost as much design and development effort as the underlying function of the software itself."[101]

Even if the Indian government could design regulations to help incentivize technological developments that could overcome these challenges, the encryption debate is a policy issue, not just a technological one. Any system that enables access to encrypted information would have to be rooted in the specific due-process provisions of the Indian Constitution.

Breaking encryption raises concerns about the misuse of official powers and violations of civil liberties. One safeguard for ensuring due process in existing Indian law is prior authorization for encryption breaks by a judge or an otherwise independent official or body.[102] However, the current procedures for lawful access, decryption, and wiretapping under India's Information Technology Act (2000) and Telegraph Act (1885) do not require prior authorization by an independent authority.[103] Such procedures are authorized by the central government or the state authorities in question, creating the potential for the misuse of power.

For example, this power could be used to target political opponents. Last year, in the state of Rajasthan, phone conversations between a union minister, a state minister, and another political representative were leaked, causing a huge political stir.[104] The ruling government later admitted to ordering the phone tapping "in the interest of public security and order." India's Central Bureau of Investigation is currently examining a similar case in the state of Karnataka, where the phones of political leaders were allegedly tapped illegally without any written instructions.[105] Given this history, concerns about the misuse of power are well founded, especially considering that, under the new rules, interception and decryption can be ordered on broad grounds with little to no independent oversight. The recent revelations about the widespread use of the Pegasus spyware is a prime example of the potential for the misuse of such technologies including backdoors.

A Way Forward: A Policy Framework for Balancing Privacy and National Security

Solving the encryption issue is not merely a question of seeking the right balance. Past and existing efforts to facilitate access to encrypted information have all resulted in systemic vulnerabilities. The weakening of encryption generates externalities that are sometimes not well understood until much later. The solution also does not lie in adopting extreme positions: either weakening encryption to meet broad security and LEA objectives or providing no pathway to accessing encrypted information.

The right approach involves answering a series of difficult questions on the appropriate policy design for the Indian context. These questions are based on those framed in a 2018 report by the U.S. National Academies of Sciences, Engineering, and Medicine.[106] Answers to these questions will be explored in Carnegie India's next paper in this series. The following questions have been adapted from that report:

1. Will the proposed alternative effectively allow LEAs and intelligence agencies to access information with the scale, timeliness, and reliability that proponents seek?

2. (In the United States, the demands from LEAs and intelligence agencies have centered around access to plaintext information that is encrypted. In India, however, the government has clearly stated that it seeks the originator of a message rather than the content. This objective requires evaluating traceability specifically, in addition to other technical alternatives examined in existing literature).

3. How will the proposed approach affect the security of encrypted information?

4. (The Indian government is not seeking access to content data. However, there is a legitimate concern that implementing traceability mechanisms or other alternatives for providing originator information could weaken encryption).

5. To what extent will the alternatives considered affect the privacy and civil liberties of India's population?

6. To what extent will the proposed approach affect India's economic competitiveness?

7. What will the direct financial costs of the proposed alternatives be?

8. Will the proposed approach improve, or at least maintain, existing legal protections against the misuse of surveillance powers?

About the Authors

Anirudh Burman is an associate research director and fellow at Carnegie India. He works on key issues relating to public institutions, public administration, the administrative and regulatory state, and state capacity.

Prateek Jha was a research assistant and program coordinator at Carnegie India.

Acknowledgments

The authors are grateful to Udbhav Tiwari, Tarunima Prabhakar, Rajesh Bansal, and Sakshe Vasudeva for their help and input. They also appreciate the assistance provided by the Carnegie India Advisory Committee on Encryption, comprising Alok Prabhakar, Michael Nelson, Saikat Datta, and Susan Landau. Research for this paper was made possible in part by support from WhatsApp. The views expressed herein, however, are the responsibility of the authors alone. The paper is an output of Carnegie India's Technology and Society Program.

Notes

1 Aashish Aryan, "Ravi Shankar Prasad: 'Govt Not in Favour of Breaking WhatsApp's Encryption, Users Have Full Right to It,'" *Indian Express*, May 29, 2021, https://indianexpress.com/article/india/ravi-shankar-prasad-whatsapps-encryption-it-rules-privacy-7334870.

2 Arjun Kharpal, "Apple Vs FBI: All You Need to Know," CNBC, March 29, 2016, https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html.

3 Ibid.

4 Sam Bocetta, "Australia's New Anti-Encryption Law Is Unprecedented and Undermines Global Privacy | Sam Bocetta," Foundation for Economic Education, February 14, 2019, https://fee.org/articles/australia-s-unprecedented-encryption-law-is-a-threat-to-global-privacy.

5 For some examples, see "New Study Finds Australia's TOLA Law Poses Long-Term Risks to Australian Economy," Internet Society, accessed August 10, 2021, https://www.internetsociety.org/news/press-releases/2021/new-study-finds-australias-tola-law-poses-long-term-risks-to-australian-economy; and Bocetta, "Australia's New Anti-Encryption Law Is Unprecedented and Undermines Global Privacy | Sam Bocetta."

6 Sam Shead, "U.S., UK and Other Countries Warn Tech Firms That Encryption Creates 'Severe Risks' to Public Safety," CNBC, October 12, 2020, https://www.cnbc.com/2020/10/12/five-eyes-warn-tech-firms-that-encryption-creates-severe-risks.html. While the Five Eyes are known for intelligence sharing, this statement came from the countries' LEAs, not the intelligence agencies.

7 U.S. Department of Justice, "International Statement: End-To-End Encryption and Public Safety," October 11, 2020, https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety.

8 "Regulatory Framework for Over-the-Top (OTT) Services," Telecom Regulatory Authority of India, Consultation Paper No. 2/2015, March 27, 2015, 4, https://www.trai.gov.in/sites/default/files/OTT-CP-27032015.pdf.

9 Per the Schedule V of the 2000 Information Technology (Certifying Authority) Rules. See Indian Ministry of Electronics and Information Technology, "Information Technology (Certifying Authority) Rules," October 17, 2000, https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Certifying%20Authority%29.pdf.

10 National Research Council, *Cryptography's Role in Securing the Information Society*, ed. Kenneth W. Dam and Herbert S. Lin (Washington, DC: National Academies Press, 1996), https://doi.org/10.17226/5131.

11 National Academies of Sciences, Engineering, and Medicine, "Decrypting the Encryption Debate: A Framework for Decision Makers" (Washington, DC: The National Academies Press, 2018), https://doi.org/10.17226/25010.

12 See Mieke Eoyang and Michael Garcia, "Weakened Encryption: The Threat to America's National Security," Third Way, 2020, https://www.thirdway.org/report/weakened-encryption-the-threat-to-americas-national-security; and Elad Yoran and Edward G. Amoroso, "The Role of Commercial End-to-End Secure Mobile Voice in Cyberspace," *Cyber Defense Review* 3, no. 1 (2018): 57–66.

13 U.S. Department of Homeland Security Science and Technology Directorate, "Study on Mobile Device Security" (Washington, DC: U.S. Department of Homeland Security, April 2017), i, https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf.

14 Ibid., 12–15.

15 See, for example, this document on the prohibition on bulk encryption in India. Indian Ministry of Communications and Information Technology, Department of Telecommunications, "License Agreement for Unified License," last accessed June 1, 2021, https://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf. For a description of the recent demands by LEAs in the United States to weaken encryption, see National Academies of Sciences, Engineering, and Medicine, "Decrypting the Encryption Debate."

16 James Andrew Lewis, "The Crypto Wars Are Over," Center for Strategic and International Studies, February 4, 2021, https://www.csis.org/analysis/crypto-wars-are-over.

17 Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau, "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet," *SSRN Electronic Journal* 12, no. 1 (2013): 9–10, https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1209&context=njtip.

18 Steven Lewy, "Battle of the Clipper Chip," *New York Times*, June 12, 1994, https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all.

19 A few key reasons include (1) the grounds for agencies to "listen in" were vague; (2) since the technology was classified, a nongovernmental agency could not test the strength of the encryption; and (3) concerns were raised about illegal access to decryption keys by foreign governments. See "The Clipper Chip," Electronic Privacy Information Centre, last accessed June 1, 2021, https://epic.org/crypto/clipper.

20 See chapter four of the National Research Council, *Cryptography's Role in Securing the Information Society*.

21 See the following source for a chronology of the relaxation of controls on encryption starting around 2000. "Expert Stakeholder Consultation Report on the Indian Encryption Debate," Dialogue, accessed June 10, 2021, 8, https://thedialogue.co/wp-content/uploads/2021/06/Report-on-Expert-Stakeholder-Consultation-on-the-Indian-Encryption-Debate-The-Dialogue.pdf.

22 National Research Council, *Cryptography's Role in Securing the Information Society*, 89. (See Box 3.2.)

23 For an explanation of how E2E encryption works, see Justino Mora, "Demystifying the Signal Protocol for End-to-End Encryption (E2EE)," Medium, August 17, 2017, https://medium.com/@justinomora/demystifying-the-signal-protocol-for-end-to-end-encryption-e2ee-ad6a567e6cb4.

24 "What Is End-to-End Encryption and How Does It Work?," ProtonMail.com (blog), March 7, 2018, https://protonmail.com/blog/what-is-end-to-end-encryption.

25 For more on how encryption or forward secrecy works in online communication, see National Academies of Sciences, Engineering, and Medicine, "Decrypting the Encryption Debate."

26 Rishab Bailey, Vrinda Bhandari, and Faiza Rahman, "Backdoors to Encryption: Analysing an Intermediary's Duty to Provide 'Technical Assistance,'" Data Governance Network Working Paper 15, March 15, 2021, 7, https://datagovernance.org/report/backdoors-to-encryption-analysing-an-intermediarys-duty-to-provide-technical-assistance.

27 See Clause 37 of the following government document. Indian Ministry of Communications and Information Technology, Department of Telecommunications, "License Agreement for Unified License."

28 Brian Dean, "WhatsApp 2021 User Statistics: How Many People Use WhatsApp?," Backlinko, March 2, 2021, https://backlinko.com/whatsapp-users#whatsapp-statistics.

29 Shruti Dhapola, "What Data Does WhatsApp Collect About You? We Asked for Account Information, Here's What We Got," *Indian Express*, January 18, 2021, https://indianexpress.com/article/technology/social/whatsapp-privacy-policy-user-data-report-how-to-download-what-does-it-contain-faq-7151248.

30 "Facebook Messenger and WhatsApp: Is Your Data Private?," Orange Cyberdefense, February 18, 2021, https://orangecyberdefense.com/global/blog/data/facebook-messenger-and-whatsapp-is-your-data-private.

31 Manas Tiwari, "Moved to Signal? Good, Now Take a Look at Facebook, Instagram, and Chrome on Your Phone," *India Today*, January 12, 2021, https://www.indiatoday.in/technology/talking-points/story/moved-to-signal-good-now-take-a-look-at-facebook-instagram-and-chrome-on-your-phone-1758293-2021-01-12.

32 Ben Schoon, "Google Messages App Reaches 1 Billion Downloads Without Being Pre-installed on Android," 9to5Google, May 1, 2020, https://9to5google.com/2020/05/01/google-messages-downloads-billion-android.

33 Google, "Messages End-to-End Encryption Overview," Technical Paper, Version 1.1, June 2021, 10, https://www.gstatic.com/messages/papers/messages_e2ee.pdf.

34 For information that can be accessed on RCS servers that are operated by carriers and Google, see Google, "Messages End-to-End Encryption Overview," 10.

35 Press Trust of India, "Telegram Crosses 500 Million User Mark Led by User Additions in Asia," *Hindu*, January 13, 2021, https://www.thehindu.com/business/Industry/telegram-crosses-500-million-subscriber-mark-led-by-user-additions-in-asia/article33568032.ece.

36 Telegram, "Telegram Privacy Policy," Versions 3.4, 3.5, 5.2, last accessed July 5, 2021, https://telegram.org/privacy.

37 "ShareChat Raises $502 Million; Valuation Rises to $2.1 BN," BusinessToday, April 8, 2021, https://www.businesstoday.in/latest/corporate/storysharechat-raises-502-million-valuation-rises-to-21-bn-292974-2021-04-08.

38 ShareChat, "ShareChat Privacy Policy," last updated June 16, 2021, last accessed July 5, 2021, https://help.sharechat.com/policies/privacy-policy.

39 Ibid.

40 David Curry, "Signal Revenue and Usage Statistics (2021)," Business of Apps, June 7, 2021, https://www.businessofapps.com/data/signal-statistics.

41 Deeksha Bhardwaj, "Messaging App Signal Not in Compliance With New Rules, Say Officials," *Hindustan Times*, June 24, 2021, https://www.hindustantimes.com/india-news/messaging-application-signal-not-in-compliance-with-new-rules-say-officials-101624508925464.html.

42 Douglas Crawford, "Best WhatsApp Alternatives That Respect Your Privacy," ProtonMail (blog), February 15, 2021, https://protonmail.com/blog/whatsapp-alternatives.

43 Zack Whittaker, "Signal Rolls Out a New Privacy Feature Making It Tougher to Know a Sender's Identity," *TechCrunch*, October 29, 2018, https://techcrunch.com/2018/10/29/signal-sealed-sender-feature-messaging-security.

44 Threema, "Threema's Success Story: From the Company's Founding to Today," last accessed July 5, 2021, https://threema.ch/press-files/1_press_info/press_threema_story_en.pdf.

45 Threema, "The Threema Advantage," last accessed July 5, 2021, https://threema.ch/press-files/content/the-threema-advantage_en.html; and Divya Kala Bhavani and Praveen Sudevan, "If Not WhatsApp, Then What? Consider These Alternatives," *Hindu*, January 11, 2021, https://www.thehindu.com/sci-tech/technology/whatsapp-alternatives-signal-telegram-spike-session-threema-privacy-policy/article33549167.ece.

46 David Lyon, "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique," *Big Data and Society*, July 9, 2014, https://journals.sagepub.com/doi/pdf/10.1177/2053951714541861.

47 See Mary Madden, "Public Perceptions of Privacy and Security in the Post-Snowden Era," Pew Research Center (blog), November 12, 2014, https://www.pewresearch.org/internet/2014/11/12/public-privacy-perceptions. Also see, for example, the self-censoring by individuals documented in the following source. Jonathan Shaw, "The Watchers," *Harvard Magazine*, December 7, 2016, https://www.harvardmagazine.com/2017/01/the-watchers.

48 Danielle Kehl, Kevin Bankston, Robyn Greene, and Robert Morgus, "Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom and Cybersecurity," New America's Open Technology Institute, Policy Paper, July 2014, https://d1y8sb8igg2f8e.cloudfront.net/documents/surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity.pdf. On pages 7 and 8, the report states, "Within just a few weeks of the first disclosures, reports began to emerge that American cloud computing companies like Dropbox and Amazon Web Services were starting to lose business to overseas competitors . . . Economic forecasts after the Snowden leaks have predicted significant, ongoing losses for the cloud-computing industry in the next few years. An August 2013 study by the Information Technology and Innovation Foundation . . . estimated that revelations about the NSA's PRISM program could cost the American cloud computing industry $22 to $35 billion over the next three years."

49 Ibid., 12.

50 Dustin Volz, Mark Hosenball, and Joseph Menn, "Push for Encryption Law Falters Despite Apple Case Spotlight," Reuters, May 27, 2016, https://www.reuters.com/article/us-usa-encryption-legislation-idUSKCN0YI0EM.

51 Bellovin et al., "Lawful Hacking," 14.

52 Ibid., 15.

53 Joel Schectman, "Skype Knew of Security Flaw Since November 2010, Researchers Say," *Wall Street Journal*, May 1, 2012, https://www.wsj.com/articles/BL-CIOB-286.

54 Carnegie Encryption Working Group, "Moving the Encryption Policy Conversation Forward," Carnegie Endowment for International Peace, September 10, 2019, https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573.

55 Anirudh Burman and Upasana Sharma, "How Would Data Localization Benefit India?," Carnegie India, April 2021, https://carnegieendowment.org/files/202104-Burman_Sharma_DataLocalization_final.pdf.

56 From 2016 to 2021, government officials provided statements on issues such as the impact of E2E encryption on catching criminals, the rise of fake news, lynchings, sharing of objectionable content, and the need for traceability. For example, see Marya Shakil, "National Security and Freedom Equally Important: Ravi Shankar Prasad on Encryption Policy," *News18*, April 18, 2016, https://www.news18.com/news/india/national-security-and-freedom-equally-important-ravi-shankar-prasad-1231411.html; Kubra Fatima, "WhatsApp Hoax: There Isn't a Ministry of Interior Regulation, and It's Not Tapping Your Calls," *News Minute,* June 7, 2017, https://www.thenewsminute.com/article/whatsapp-hoax-there-isnt-ministry-interior-regulation-and-its-not-tapping-your-calls-63283; Aroon Deep, "Exclusive: Government Makes Notices to WhatsApp, Responses Public," Medianama, August 24, 2018, https://www.medianama.com/2018/08/223-government-letters-whatsapp-meity; Aditi Agrawal, "RS Prasad: Traceability Will Be WhatsApp's Job; WhatsApp Demurs," Medianama, July 29, 2019, https://www.medianama.com/2019/07/223-rs-prasad-traceability-will-be-whatsapps-job-whatsapp-demurs/; Parliament of India, Rajya Sabha, "Report of the ADHOC Committee of the Rajya Sabha to Study the Alarming Issue of Pornography on Social Media and Its Effect on Children and Society as a Whole," January 25, 2020, https://rajyasabha.nic.in/rsnew/Committee_site/Committee_File/ReportFile/71/140/0_2020_2_16.pdf; and Manish Singh, "Facebook, Twitter, WhatsApp Face Tougher Rules in India," *TechCrunch*, February 25, 2021, https://techcrunch.com/2021/02/25/india-announces-sweeping-guidelines-for-social-media-on-demand-streaming-firms-and-digital-news-outlets.

57 "India's First Internet Connection: VSNL's 1995 Plan Offered 40 Mins Per Day Usage at Rs. 15000," *News18*, August 13, 2020, https://www.news18.com/news/tech/indias-first-internet-connection-vsnls-1995-plan-offered-40mins-per-day-usage-at-rs-15000-2780411.html.

58 The definition is provided in Section 2(f) of India's Information Technology Act. See "The Information Technology (IT) Act, 2000," Indian Ministry of Electronics and Information Technology, 2000, https://www.meity.gov.in/content/information-technology-act-2000. (It is subsequently mentioned in chapters two, six, seven, and eight). Public key infrastructure is a term used to encompass everything that is used to set up and run public key encryption.

59 Reserve Bank of India, "Internet Banking in India—Guidelines," DBOD.COMP.BC.No.130/ 07.03.23/ 2000–2001, June 14, 2001, https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=414&Mode=0. For the SEBI guideline, see Securities and Exchange Board of India, "Committee on Internet Based Securities and Trading Services—First Report," press release, last accessed May 31, 2021, https://www.sebi.gov.in/sebi_data/commondocs/99290report_p.pdf.

60 Kargil Committee, "From Surprise to Reckoning: Kargil Committee Report Executive Summary," February 25, 2000, NuclearWeaponArchive.org, http://nuclearweaponarchive.org/India/KargilRCA.html.

61 According to the Global Terrorism Index 2020, India ranks as the eighth most highly impacted country from terrorism globally; see "Global Terrorism Index 2020: Measuring the Impact of Terrorism," Institute for Economics and Peace, November 2020, https://www.visionofhumanity.org/wp-content/uploads/2020/11/GTI-2020-web-1.pdf.

62 See, for example, "The Use of the Internet for Terrorist Purposes," United Nations Office on Drugs and Crime, September 2012, https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

63 Kritika Bansal, "Forget Telegram, Signal: ISIS Terrorists in India, Abroad Using Much More Secure Messenger 'Threema,'" India.com, January 16, 2021, https://www.india.com/technology/forget-telegram-signal-isis-terrorists-in-india-abroad-using-much-more-secure-messenger-threema-4334501.

64 Bedavyasa Mohanty, "The Encryption Debate in India," Carnegie Endowment for International Peace, May 30, 2019, 6, https://carnegieendowment.org/2019/05/30/encryption-debate-in-india-pub-79213.

65 "Lynching Due to Social Media Content, Says Govt Panel," *Hindustan Times*, August 29, 2018, https://www.hindustantimes.com/india-news/lynching-due-to-social-media-content-says-govt-panel/story-yEOBxigFNZjgQlnwLHDfFI.html.

66 For example, during the 2017 Dera Sacha Sauda riots in northern India, police officials in neighboring towns complained about the difficulty of containing rumors spread on WhatsApp. See Preetika Khanna, Abhiram Ghadliyal, and Shaswati Das, "Death by Social Media," *Mint*, August 2, 2018, https://www.livemint.com/Politics/jkSPTSf6IJZ5vGC1CFVyzI/Death-by-Social-Media.html.

67 Prerna Sindwani, "A Third of the World's Child Porn Is Flagged Off in India, Indonesia and Thailand," *Business Insider*, October 1, 2019, https://www.businessinsider.in/law-order/crime/news/a-third-of-the-worlds-child-porn-is-flagged-off-in-india-indonesia-and-thailand/articleshow/71385866.cms.

68 "NCMEC's Statement Regarding End-to-End Encryption: Ignoring Abuse Won't Stop It," National Center for Missing and Exploited Children, October 3, 2019, https://www.missingkids.org/blog/2019/post-update/end-to-end-encryption.

69 WhatsApp, "WhatsApp Help Center—What Is Traceability and Why Does WhatsApp Oppose It?," accessed June 9, 2021, https://faq.whatsapp.com/general/security-and-privacy/what-is-traceability-and-why-does-whatsapp-oppose-it/?lang=en.

70 WhatsApp, "How WhatsApp Helps Fight Child Exploitation," February 2021, https://faq.whatsapp.com/general/how-whatsapp-helps-fight-child-exploitation/?lang=en.

71 Burman and Sharma, "How Would Data Localization Benefit India?"

72 FE Bureau, "Centre Accuses Twitter of Trying to Dictate Terms to It," *Financial Express*, May 28, 2021, https://www.financialexpress.com/industry/technology/centre-accuses-twitter-of-trying-to-dictate-terms-to-it/2260416.

73 Indian Ministry of Communications and IT Department of Telecommunications, "[Letter Issuing Directions on the Subject of the] ISP Licence Agreement," No. 820-1/98-LR (Pt. II), August 6, 1999, https://dot.gov.in/sites/default/files/amendment_isp_6-8-1999_0.pdf?download=1.

74 A copy of the draft of the National Encryption Policy 2015 can be found here: Parliament of India, "Draft National Encryption Policy," Netzpolitik, last accessed May 31, 2021, https://netzpolitik.org/wp-upload/draft-Encryption-Policyv1.pdf.

75 Nandita Mathur, "What Was the Draft Encryption Policy and Why Was It Withdrawn?," *Mint*, September 22, 2015, https://www.livemint.com/Politics/RZtAGhM6IjDBWujiK6ysEP/What-was-the-encryption-policy-and-why-it-was-withdrawn.html.

76 Komal Gupta, "Govt Readies New Rules to Check Misuse of Social Media," *Mint*, December 25, 2018, https://www.livemint.com/Politics/HSXu9xkT9XESvui4AV8QUI/OPEC-allied-oil-producers-to-hold-extra-meeting-if-output-c.html.

77 See Clause 3(5) and 3(9) of the following Indian government document. Indian Ministry of Electronics and Information Technology, "Draft Information Technology (Intermediary Guidelines) Rules," 2018, last accessed June 1, 2021, https://www.meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf.

78 Indian Ministry of Electronics and Information Technology, "The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules," February 25, 2021, https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf.

79 According to Section 2(1)(w) of the Information Technology Act, 2000, the term "intermediary" includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online auction sites, online marketplaces, and cyber cafes.

80 See Rule 2 (w) of the 2021 Intermediary Guidelines. Indian Ministry of Electronics and Information Technology, "The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules."

81 See Rule 2 (v) of the 2021 Intermediary Guidelines. Indian Ministry of Electronics and Information Technology, "The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules." The minimum number of registered users is 50 lakhs; see "New Intermediary Rules: What Social Media Giants Stand to Lose, and Why You Should Be Worried," *Economic Times*, May 26, 2021, https://economictimes.indiatimes.com/news/et-explains/intermediary-tag-what-social-media-giants-stand-to-lose-and-why-you-should-be-worried/articleshow/82943504.cms?from=mdr.

82 See Rules 4(1), 4(6), and 4(8) of the 2021 Intermediary Guidelines. Indian Ministry of Electronics and Information Technology, "The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules."

83 See Rule 4(2) of the 2021 Intermediary Guidelines. Indian Ministry of Electronics and Information Technology, "The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules."

84 ". . . prevention, detection, investigation, prosecution or punishment of an offence related to the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order, or of incitement to an offence relating to the above or in relation with rape, sexually explicit material or child sexual abuse material, punishable with imprisonment for a term of not less than five years." See the first proviso to Rule 4(2) of the Indian Ministry of Electronics and Information Technology, "The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules."

85 See Rule 4(4) of the 2021 Intermediary Guidelines. Indian Ministry of Electronics and Information Technology, "The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules."

86 The reasons for doing so must be recorded in writing. According to the rules, the Ministry of Electronics and Information Technology can do so "if the services of that intermediary permits the publication or transmission of information in a manner that may create a material risk of harm to the sovereignty and integrity of India, security of the State, friendly relations with foreign states, or public order." Indian Ministry of Electronics and Information Technology, "The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules."

87 Riana Pfefferkorn, "New Intermediary Rules Jeopardize the Security of Indian Internet Users," Brookings Institute *TechStream* (blog), March 3, 2021, https://www.brookings.edu/techstream/new-intermediary-rules-jeopardize-the-security-of-indian-internet-users.

88 Telecom Regulatory Authority of India, "Recommendations on Regulatory Framework for Over-the-Top (OTT) Communications Services," September 14, 2020, 7, https://www.trai.gov.in/sites/default/files/Recommendation_14092020_0.pdf.

89 FE Online, "WhatsApp Viral Message: 'Modi Government to Ban WhatsApp Use in Country?' Here's the Truth," *Financial Express*, June 19, 2018, https://www.financialexpress.com/india-news/whatsapp-viral-message-modi-government-to-ban-whatsapp-use-in-country-heres-the-truth/1211861.

90 Krishna Pokharel and Rajesh Roy, "India Says Rumors About Child Snatching on WhatsApp Led to Mob Killings," *Wall Street Journal*, July 5, 2018, https://www.wsj.com/articles/india-admonishes-whatsapp-after-deaths-1530730096; and Deep, "Exclusive: Government Makes Notices To WhatsApp, Responses Public."

91 Yuthika Bhargava, "Be Ready to Trace the Origin of Messages, WhatsApp Told," *Hindu*, October 31, 2018, https://www.thehindu.com/news/national/whatsapp-not-seeking-decryption-but-location-identity-of-those-sending-provocative-messages-says-centre/article25380482.ece.

92 WhatsApp, "WhatsApp Help Center—What Is Traceability and Why Does WhatsApp Oppose It?"

93 Ibid.

94 V. Kamakoti, "Report on Originator Traceability in WhatsApp Messages," July 31, 2019, http://archive.org/details/reportofprof.kamakotiinwpnos.20214and20774of2018.

95 For example, see Manoj Prabhakaran, "On a Proposal for Originator Tracing on WhatsApp," accessed June 22, 2021, https://drive.google.com/file/d/1vivciN8tNSbOrA9eZ8Ej0mCAUBzRWu5N/view?usp=embed_facebook.

96 "Traceability and Cybersecurity," Internet Society, accessed November 27, 2020, https://www.internetsociety.org/resources/doc/2020/traceability-and-cybersecurity-experts-workshop-series-on-encryption-in-india.

97 Deciphering the Debate Over Encryption: Hearings Before the Comm. on Energy and Commerce Subcommittee on Oversight and Investigations, 114th Cong. (2016) (testimony of Matt Blaze, computer science professor, April 19, 2016), https://docs.house.gov/meetings/IF/IF02/20160419/104812/HHRG-114-IF02-Wstate-BlazeM-20160419-U3.pdf.

98 Harold Abelson et al., "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," *Journal of Cybersecurity* 1, no. 1 (September 1, 2015): 69–79, https://doi.org/10.1093/cybsec/tyv009.

99 Bellovin et al., "Lawful Hacking."

100 Nikhil Rampal, "India's Cybersecurity a Joke for Hackers, Ranks Among Worst in the World," *India Today*, February 7, 2019, https://www.indiatoday.in/india/story/india-cybersecurity-privacy-data-breach-crypto-hackers-aadhaar-1450572-2019-02-07.

101 Deciphering the Debate Over Encryption: Hearings Before the Comm. on Energy and Commerce Subcommittee on Oversight and Investigations, 114th Cong. (2016) (testimony of Matt Blaze, computer science professor, April 19, 2016).

102 Smriti Parsheera and Prateek Jha, "Cross-Border Data Access for Law Enforcement: What Are India's Strategic Options?," Carnegie India, November 23, 2020, 8, https://carnegieindia.org/2020/11/23/cross-border-data-access-for-law-enforcement-what-are-india-s-strategic-options-pub-83197.

103 For interception, monitoring, and decryption, see Section 69 of the 2000 Information Technology Act. Indian Ministry of Electronics and Information Technology, "The Information Technology (IT) Act, 2000," 2000, https://www.meity.gov.in/content/information-technology-act-2000. For wiretapping, see Section 5 of the Telegraph Act (1885). Indian Ministry of Communications Department of Telecommunications, "The Telegraph Act (1885)," https://dot.gov.in/act-rules-content/2442.

104 Hamza Khan, "Months After Political Crisis, Gehlot Govt Admits to Phone Taps," *Indian Express*, March 15, 2021, https://indianexpress.com/article/india/rajasthan-congres-govt-ashok-gehlot-sachin-pilot-illegal-phone-taps-7228400.

105 T.A. Johnson, "Karnataka Phone-Tapping: CBI Set to Look at Role of Officers," *Indian Express*, September 6, 2019, https://indianexpress.com/article/india/karnataka-phone-tapping-cbi-set-to-look-at-role-of-officers-5970698.

106 National Academies of Sciences, Engineering, and Medicine, "Decrypting the Encryption Debate," 3.

Carnegie India

Founded in 2016, Carnegie India, based in New Delhi, is part of a robust global network that includes over 150 scholars in Beijing, Beirut, Brussels, Moscow, and Washington. The center focuses primarily on three interrelated programs: technology and society, political economy, and security studies. Led by Indian experts with decades of international and domestic policy experience, Carnegie India engages with governments, policymakers, academics, students, industries, practitioners, and civil society to provide insightful and fresh analysis on India's pressing challenges and the rising role of India in the world.

Carnegie Endowment for International Peace

The Carnegie Endowment for International Peace is a unique global network of policy research centers in Russia, China, Europe, the Middle East, India, and the United States. Our mission, dating back more than a century, is to advance peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decision-makers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

CARNEGIE
INDIA

CarnegieEurope.eu