



OCCASIONAL PAPER

DECEMBER 2016

102

'GOING DARK' IN INDIA: The Legal and Security Dimensions of Encryption

BEDAVYASA MOHANTY



OBSERVER
RESEARCH
FOUNDATION

'GOING DARK' IN INDIA: The Legal and Security Dimensions of Encryption

BEDAVYASA MOHANTY

ABOUT THE AUTHOR

Bedavyasa Mohanty is a Junior Fellow with ORF's Cyber Initiative. A lawyer by training, he is interested in the jurisprudence of privacy law and the constitutionality of state surveillance. His current research focuses on encryption, autonomous weapons and Mutual Legal Assistance Treaties. He has a keen interest in the philosophical justifications for war and the suspension of civil liberties, especially how conflict will drive regulation of future technologies. Bedavyasa completed his BA LLB (Hons) from the National University of Juridical Sciences, Kolkata, in 2015. Previously, he has interned with the Centre for Internet and Society, Bangalore; the Centre for Communication Governance, National Law University, Delhi; and the Central Information Commission, New Delhi.

‘GOING DARK’ IN INDIA: The Legal and Security Dimensions of Encryption

ABSTRACT

Encrypting communications enhances privacy and the security of information services. This, in turn, incentivises innovation in the ICT sector and contributes significantly to the growth of the internet economy. India's (now withdrawn) Draft National Encryption Policy was single-minded in its approach. It sought only to prescribe standards that would enable law enforcement agencies to access encrypted data. There are, however, multifarious concerns of users, internet companies and the intelligence community that need to be addressed. The second iteration of the encryption policy should incentivise the adoption of strong encryption standards by both the government as well as the private sector. It must explore technologically sophisticated solutions to protect information flows in the digital economy. This paper highlights some of these solutions that can help ensure that the policy remains relevant over the next few decades.

INTRODUCTION

With digital networks increasingly becoming the preferred conduit for commerce and personal correspondence, encryption is critical to maintaining security and trust in the medium. It involves scrambling readable text (*plaintext*) with a secret *key* to transform it into *ciphertext*, incomprehensible to anyone not in possession of the said key.¹ This is a complex process with trillions of possible combinations depending on the

key length and may be impossible to crack with conventional computers. Cryptography, however, predates technology. It has been around for as long as there has been information to protect. It is hardly surprising then, that some of the earliest references to encryption appear among pottery traders in 1500 B.C. Mesopotamia for the protection of trade secrets, and in 400 B.C. India for the protection of information relating to conjugal relations.² Communications during those times involved messages that were written down. These were hidden through rudimentary alphabet-substitution ciphers.

Encryption has since become ubiquitous. Google, for instance, has made the Secure Socket Layer (SSL) encryption the default standard for its Gmail service and Google searches since 2010 and 2011, respectively.³ Internet users are also obtaining access to more sophisticated end-to-end encryption services for free, through applications like Whatsapp⁴ and Telegram.⁵ Encryption is also available as built-in security for devices such as Apple's iPhone.⁶ This ubiquity has seen the resurgence⁷ of claims by law enforcement agencies that their ability to 'lawfully' intercept communication for criminal and terrorism-related investigations has been hampered. Encrypted channels allow their users to "go dark,"⁸ maintain law enforcement agencies. Thus, they demand that companies retain access to all user communications and data, including encrypted data, and extend that access to law enforcement entities upon request. These demands have been met with strong resistance from supporters of encryption in both industry and civil society. They argue that any deliberate weakening of encryption would not only affect user privacy but also set back the overall standard of security in the market by many years.

While no easy answers to the debate have emerged, it appears that the result of this latest iteration of 'crypto wars' will change the nature of online exchanges.⁹ India, for its part, has taken steps to resolve this debate. In September 2015, the Indian government released a Draft National Encryption Policy (hereinafter Draft Policy) that sought to set encryption standards and lay down conditions for decryption of information for

lawful investigation. The draft was laudable in its intent to calibrate policy in response to rapid technological developments in India and abroad. However, the conditions set out under the Draft Policy were problematic enough that it drew widespread criticism, resulting in its swift withdrawal. The Indian government is now in the process of finalising a second draft of the National Encryption Policy and has solicited inputs from the ICT industry and civil society to make it more balanced and acceptable.

As complex as the issue of encryption is, its fundamental dilemmas can perhaps be encapsulated in one question: Is it paradoxical to seek secure law enforcement access to encrypted data? The answer, however, varies from one country to the next. 'Preferable' levels of encryption depend on a complex network of legal, political, economic and even social factors unique to each country. They will depend on how the country has traditionally treated privacy and what restrictions on free speech exist. They will also depend on the extent to which the country's ICT industry is reliant on international services. Predominantly, they will depend on two things: the technological security and self-reliance of the country's information infrastructure, and the expertise of cyber security personnel. The Indian narrative around encryption is one of considerable complexity.

FRAMING THE "GOING DARK" DEBATE IN THE INDIAN CONTEXT

The Draft Policy sought to establish the protocols and algorithms for encryption, key exchanges and digital signatures for all government entities, businesses and citizens. It allowed businesses and citizens to use encryption as long as they handed in the plaintext, encrypted text and the hardware/software used for encryption when such information was sought by law enforcement agencies. In what was among the most controversial provisions of the Policy, it mandated all businesses and citizens using encryption to retain the plaintext of encrypted communication for 90 days from the date of transmission or transaction. The Policy also mandated that every service provider (whether they were based in India or abroad) would need to enter into an agreement with the

government to operate within the Indian market. The nature of this agreement and what it would entail was not clarified.

The Draft Policy, therefore, wanted to ensure lawful access to encrypted data through a combination of three measures. First, it imposed a quasi-licensing model where a vendor or encryption service provider would presumably enter into an agreement with the government to allow unrestricted access to data. Without complying with this provision, they will not be allowed access to Indian markets. This would have the effect of establishing a backdoor within the service for Indian law enforcement and intelligence agencies. The Indian government is known to have deployed this pre-condition at least once in the past, when it compelled Blackberry to allow special access to its Blackberry Messenger and Blackberry Internet Service email.¹⁰

Second, the Draft Policy also required encryption service providers to provide the government with working copies of the software and hardware used for encryption. This 'key recovery' mechanism meant that even without the backdoor requirement, the government would probably retain the capability to decrypt all symmetric encryption that used the same key to encrypt and decrypt.

Third, in cases of information sent through end-to-end encryption and other methods that used asymmetric public-private keys — the government would not be able to obtain the plaintext through the service provider because the information is not retained on the service provider's servers — the policy mandated that senders of such information would have to retain the unencrypted plaintext for 90 days. This would enable the government to bypass the service provider and obtain the content of communication straight from the source.

The threat of creating backdoors in information systems has been the focal point of controversy in the recent past. The *Apple v. FBI* case¹¹ involving the iPhone 5C of the San Bernardino shooter was, in many ways,

the flashpoint for a global conversation on encryption. In the matter, Apple resisted the FBI's request to develop a new operating system that would allow it to bypass the phone's passcode to access the encrypted content within. Among other things, Apple raised the concern that being compelled to write such code would be a violation of the company's First Amendment right to freedom of speech.¹² The company also raised concerns that a backdoor such as this, once created, would compromise the security of all devices. This 'GovtOS' would be a generic software patch that could be adapted for any iPhone. Even if the leak of that particular piece of code was prevented, the knowledge that the creation of such a code was possible would undermine security. It could also make Apple employees targets for extortion.¹³

This becomes doubly important in the Indian context due to the existence of precedent in the Blackberry matter. While it is known that Blackberry provided special access to law enforcement to its devices, the means through which it was granted remains unknown.¹⁴ This uncertainty may have even catalysed the decline of Blackberry's market share in the country since 2012.¹⁵ If a similar provision regarding a clandestine agreement between the government and an encryption provider, similar to that in the Draft Policy, is retained in the second draft, it would erode considerable trust in the cyber security market. It would prompt state-of-the-art encryption providers to either exit the Indian market or, at the very least, reconsider their engagement with the country. In the long run, the lack of access to advanced encryption products and tools is likely to hinder India's projection of itself as a robust digital economy.

One of the arguments that Apple offered in its resistance of the FBI's demands was that necessitating the writing of additional software was an arbitrary deprivation by the government of its liberty under the Fifth Amendment to the United States Constitution. The Fifth Amendment also protects a person from being compelled in any criminal case to be a witness against herself. A complementary provision has been provided under Article 20(3) of the Indian Constitution which reads, "No person

accused of any offence shall be compelled to be a witness against himself.”¹⁶ If the second iteration of the encryption policy contains a provision mandating the retention of plaintext of encrypted information for 90 days, it may abrogate the right against self-incrimination under Article 20(3). The right against self-incrimination covers both oral as well as documentary evidence.¹⁷ Plaintext of one's encrypted communication would be considered documentary evidence.

While Article 20(3) does not cover testimony in the form of a handwriting or DNA sample, or blood spatter, among others, this would not apply to decrypted copies of one's messages or email. This finds support in a three-judge bench ruling of the Supreme Court in *Selvi v. State of Karnataka*. The court, while deliberating on the legality of an admission obtained through narco-analysis, expanded the remit of Article 20(3). It was held that any process that “impedes the subject's right to choose between remaining silent and offering substantive information,” cannot be allowed.

The court expanded this further by urging the need to respect the privacy of mental processes. It explains, “While the scheme of criminal procedure as well as evidence law mandates interference with physical privacy through statutory provisions that enable arrest, detention, search and seizure among others, the same cannot be the basis for compelling a person to impart personal knowledge about a relevant fact.” Besides, search and seizure must be statutorily empowered. An executive policy on encryption cannot mandate the production of decrypted communications. If the new draft of the policy retains the requirement of the 90-day plaintext retention policy, it is likely to be challenged in courts and liable to be struck down.

The Draft Policy of 2015 had other concerning provisions. It was withdrawn because it failed to account for the additional vulnerabilities that would arise as a result of centrally retaining the tools to decrypt information. It also ignored the fact that creation of 'exceptional access' for

law enforcement would compromise forward secrecy. Dynamic standards (such as OpenSSL and Transport Layer Security) ensure forward secrecy through the use of a non-deterministic algorithm to generate a new set of public-private keys for each session. This set of public-private keys is used only to generate the session key for that particular session and is never used again. The loss or theft of one private key does not compromise information exchanged in a past or future transaction. If a universal decryption key is created for the government, then its accidental compromise would leave all past conversations on a certain platform open to whoever is in possession of the key.

The response to the Draft Policy, in no small part owed to its executive overreach, was largely reactionary and not constructive. Concerns regarding security are important as it affects not just the state but citizens and businesses that operate within it. The government needs access to information in order to be able to investigate and prosecute crime. It also needs to monitor information exchanges in a timely manner to thwart threats to national security. However, information gathering must align with the rights of the very citizens that the state is safeguarding. It is now well established within the technical community that the security provided by encryption is a prerequisite for the development of e-commerce and online banking.¹⁸ It is also a critical tool for investigative journalists and whistleblowers. Any policy that stops short of actively encouraging the adoption and proliferation of secure communications will hinder the growth of information and communication technologies. The new policy must, therefore, find a middle ground between the need to access data and the need to maintain security of ICT architecture.

The encryption policy is likely to have far-reaching effects. At a time when India is deliberating on a Constitutional recognition of the right to privacy¹⁹ and the data protection regulations have been found wanting in handling international data,²⁰ the policy represents an opportunity to strengthen India's information security landscape.

ENCRYPTION AND DATA VULNERABILITY IN INDIA

The crypto wars in India may have lessons to learn from the conflict between Silicon Valley and the United States government. Still, there are many unique considerations that Indian policymakers must keep in mind. India's domestic legal system, after all, suffers from a lack of privacy legislation, inadequate data protection rules, and a surveillance regime that is, for the most part, guided by colonial legislation. How the country regulates encryption will have implications on rights, commerce and national security. It will need to harmonise the regulatory landscape so that the multifarious interests of various stakeholders are balanced.

There is no explicit Constitutional recognition of the right to privacy in India. Instead, it has emerged through a series of (often contradictory) pronouncements by Indian courts to gain recognition as a penumbral right under other fundamental freedoms. This position, however, is tenuous at best. The government, through the Attorney General, has claimed that there is no right to privacy available to Indian citizens.²¹ The Supreme Court of India, in 2015, convened a Constitution Bench to adjudicate upon the issue.²² The apex court is expected to finally rule on the contours of the right within the next year. In the meantime, traditional privacy-based arguments against decryption of information by the government are not as readily applicable.

This is further complicated by India's surveillance regime which lacks safeguards in the form of judicial review. Interception of communications in India is authorised by an executive order under Section 5(2) of the Telegraph Act, 1885 and Section 69B of the Information Technology Act, 2000 (hereinafter IT Act).²³ Orders of interception under Section 5(2) also follow improperly defined standards such as “on the occurrence of public emergency” or “expedient... in the interest of national security” as preconditions.²⁴ Similarly, under Section 69B, the government can order collection of information from any computer resource to “enhance cyber security.” Without the guidance of a privacy law, orders for surveillance are

left to the subjective determination of a non-judicial authority. These broad powers of interception can also include access to encrypted information.

The Data Protection Rules drafted under Section 87(2)(ob) of the IT Act classify passwords as “sensitive personal data or information”.²⁵ Password, in turn, has been defined to include encryption and decryption key.²⁶ However, the rules also mandate that a body corporate that collects this sensitive data will share it with a government agency upon receiving a request in writing.²⁷ As a result, India's data protection laws have faced criticism both at home and overseas.²⁸ The European Union, for one, views Indian data protection regulation as being inadequate for European data. A recent survey by the Data Security Council of India (DSCI) estimates that this may have resulted in an opportunity loss of USD 2-2.5 billion.²⁹

Even technical standards that are available for data protection do not prescribe a high standard for encryption. Earlier, the licensing agreement between the Indian Department of Telecommunications and Internet Service Providers (ISPs) stipulated that no ISP would be permitted to use encryption standards higher than 40-bit symmetric keys. Any use of higher encryption would involve obtaining express approval from the government and the submission of decryption keys.³⁰ The license agreement also prohibited the use of bulk encryption by ISPs. Curiously, the Unified Licensing Agreement that replaced the erstwhile service-specific licensing agreements dropped the upper limit mandating 40-bit encryption. It, however, retained the prohibition on bulk encryption and specified that the use of encryption by the ISP's subscriber will be governed by a policy drafted under the Information Technology Act.³¹ The absence of the 40-bit standard has removed an upper ceiling on what is permissible encryption, but the rule has not been supplanted by any provision that clarifies the issue.

Taken together, the absence of a privacy law, excesses of surveillance powers, and the inadequacy of data protection norms create inconsistent

policies that are not conducive to investments and growth in technology. The Draft Policy was a reflection of these inconsistencies.

Shortly after the release of the Draft Policy in 2015 the government issued a clarification that mass-market encryption products would be excluded from the ambit of the policy; that effectively excluded services like Whatsapp and standards like OpenSSL from the policy's effects. It is unclear whether the second iteration of the encryption policy will apply to mass-market encryption tools. It, however, should. A 'good' encryption policy can have the effect of harmonising the regulatory landscape around information security, in turn triggering changes to decades-old laws.

It is noteworthy that this time around, the Ministry of Electronics and Information Technology is seeking inputs from industry bodies and civil society while drafting the policy. This is an opportunity to avoid the same pitfalls that the Draft Policy suffered from. It is also a time to analyse and learn from other jurisdictions that have seen similar debates.

POLICY RECOMMENDATIONS

To truly emulate best-in-class security standards that encourage not only the entry of state-of-the-art communications providers but also the growth of competing domestic services, the policy must conform to the test of necessity and proportionality while setting decryption mandates. The UN Special Rapporteur for Freedom of Speech and Expression has urged state governments to not ban any comprehensive protections on encrypted services and to impose restrictions on a case-by-case basis. He has also urged them to resort to court orders for imposing specific limitations.³² India's encryption policy must, however, go beyond merely setting decryption mandates. Rather, the policy must aim to:

1. Update existing laws and regulations to deal with the proliferation of secured communication services.
2. Upgrade the overall standard of security in cyberspace to enhance free

speech and stimulate e-commerce.

3. Encourage the growth of research and development in cyber security and cryptographic tools domestically.
4. Identify and adapt international best practices in information security and data protection.
5. Prescribe limits on lawful access to encrypted communication that are proportionate and effective.

The encryption policy that is drafted now is likely to set the market standards for the coming 25 years. In that time, it is hoped that the Indian market will have replaced foreign communication providers with those that are developed domestically. It will be essential to ensure that information belonging to Indian citizens is not compromised by foreign intelligence agencies and non-state actors. To that end, the policy must keep in mind safeguards such as the Roots of Trust³³ standard proposed by National Institute of Standards and Technology and the guidelines suggested by the Reserve Bank of India.³⁴ In addition to these, the Policy should strengthen the security of the internet ecosystem by ensuring the following:

1. Mandating Forward Secrecy in the Transmission Layer

Mass-market tools like email clients and web browsers are some of the most frequently used web-based services by internet users. They are also especially vulnerable to exploitation through man-in-the-middle attacks, where an attacker intercepts encrypted communications and is then able to decrypt it by stealing a private key. The encryption policy should mandate that all providers of mass-market services transition to secure encryption protocols such as SSL/TLS. This will involve generating a new set of encryption keys for every transaction and will ensure forward secrecy. Encrypting the transmission layer will ensure that even if a user is exploited, her past transactions would remain secure and the level of potential damage would be restricted.

2. Encouraging Hardware Security-by-Design

Storing sensitive data on mobile computing devices, smartphones and portable storage drives presents an inherent vulnerability for data. Some of the more prominent data breaches and cyber-attacks in recent memory like the Office of Personnel Management hack and Stuxnet are said to have been made possible through unsecured end-devices. It is essential that the encryption policy address this lacuna in network security. The policy should mandate that employees of the government as well as the private sector, who handle sensitive data, use protective measures such as the RSA SecurID. The RSA SecurID is an authentication mechanism consisting of a hardware or software token that generates a random authentication code every 60 seconds. This helps protect data of employees that use personal/remote devices to connect to official networks. For devices such as smartphones that connect to a cloud, encryption helps protect data across devices in cases of theft. Most users do not modify the security configuration on their devices, preferring to keep the default configuration that the devices come with.³⁵ Products like the Apple iPhone are considered more secure precisely because of their encrypted-by-default feature. In markets like India, where the proliferation of cheap smartphones poses a threat to network security, it would be prudent for the policy to recommend a shift towards a secure-by-design framework.

3. Setting Strong Standards for Encryption Keys

One of the core issues in the encryption debate has been about whether states should regulate the strength of communications encryption. This paper has earlier discussed the inadequacy of the 40-bit encryption key that the Indian laws seem to currently prescribe. As early as 1995, three different teams of researchers at the Massachusetts Institute of Technology, the École Polytechnique, and the RSA Data Security Conference have demonstrated that the 40-bit encryption can be broken with little effort.³⁶ It is therefore critical that the encryption policy mandate a higher standard of security for encrypting communications. The Reserve Bank of India³⁷ and SEBI³⁸ have recommended that for

financial transactions, 256-bit encryption should be made the default standard. Financial services, however, are not the only points of vulnerability. Many other government services such as the Railways and Aadhaar unique identity database also handle vast amounts of information and have been targets of cyber-attacks in the past. This is only likely to intensify in the future. The policy must therefore mandate that all government-to-government; government-to-business; government-to-citizen communications adopt a 256-bit encryption standard. This should also be made mandatory for industries identified as Critical Information Infrastructure. The policy, however, should not aim to set any limits on encryption of business-to-consumer communication—rather these standards should be allowed to develop organically.

4. Registration of Encryption Service Providers

The encryption policy must require that every vendor of an encryption product and every encryption service provider register with a designated authority within the Indian government. The information sought during registration should only include the name and address of the cryptography provider; a description of the encrypted product/service; the strength of encryption used; and a designated point of contact within the service provider for law enforcement assistance. This registration must be purely declaratory in nature and must not involve an agreement between the service provider and the government. This provision must also not mandate sharing of, or modification to the source code to allow exceptional access to the encrypted product/service. In order to expedite the registration process, the government must endeavour to respond to a registration request (to seeking clarifications if any) within 30 days of submission of the information. If the appropriate authority fails to respond within the 30 days then the registration process should be deemed to have been successful.

5. Judicial Oversight for Decryption of Information

Requiring decryption of information involves a higher degree of intrusion than standard search and seizure of electronic documents. This is because

encrypted information can generally be presumed to be sensitive material that the creator of the information would seek to protect. In this respect, India's surveillance laws, that prescribe an administrative authorisation model for interception of communication, are inadequate. The encryption policy must mandate that every request for decryption of information be warranted by a judicial magistrate.

6. 'Cryptographic Envelopes' or a Two-factor Authentication for Decryption Orders

Even proponents of strong encryption acknowledge the legitimate need of law enforcement to access data. Key escrow systems and device backdoors are not considered viable solutions because they endanger data by centralising keys and weakening devices. There are, however, alternatives that the government could explore to ensure 'lawful and secure' access to encrypted data. Cryptographic envelopes are one such alternative.³⁹ A cryptographic envelope utilises existing technology such as PGP to securely store the decryption key to a device. The envelope can only be opened by the party whose public key was used to encrypt it. In order to decentralise the decryption process, multiple envelopes can be used, one inside the other, each encrypted with a different entity's public key. These entities could be the manufacturer of the device and a designated law enforcement agency. Both the envelopes would have to be opened individually by each entity, thus preventing the unilateral misuse of a decryption key either by the government or the industry. It would also protect the data in case one of the entities' private key is compromised. Using envelope encryption in conjunction with a judicial warrant requirement for decryption would greatly increase transparency. Law enforcement agencies would have to exhibit the public safety imperative for seeking the decryption of communications; the judiciary would test the legal validity of the claim; and the manufacturer of the device would ascertain whether the decryption violates the user's privacy. Through this approach, every request for decrypting communications would undergo three layers of scrutiny. It would also minimise the threat of non-state actors gaining access to encrypted communications by exploiting backdoors.

CONCLUSION

With a plurality of actors and interests involved, encryption is perhaps the most complex issue of this decade. It implicates rights, commerce, law enforcement and intelligence. India's Draft Policy only addressed law enforcement concerns while failing to truly address the multifarious issues at play. Privacy activists and the ICT industry have long favoured stronger encryption standards. However, one important stakeholder that has not yet weighed in on the debate is the intelligence community. Not unlike law enforcement agencies, espionage organisations also prefer easy access to information. Unlike law enforcement agencies, however, intelligence organisations are mandated with maintaining 'information assurance.' This involves protecting domestic data from being intercepted and exploited by foreign intelligence agencies and non-state actors. The Snowden revelations made it clear that many foreign espionage organisations like the National Security Agency and GCHQ are ready and willing to leverage their superior technological capability to monitor the activities of even democratically elected governments. India's dual-use cyber-tech is not at par with its western competitors. India is also not a part of cooperative espionage networks like the Five Eyes. In this backdrop, sophisticated encryption is the only viable option to keep data secure both within domestic borders and without.

With more countries choosing to reflexively regulate encryption, it is important that India take a considered approach. International trends have shown that countries with influential governments and with opaque intelligence services are disfavoured end-to-end encryption.⁴⁰ These include countries like Russia,⁴¹ Pakistan,⁴² Kazakhstan,⁴³ Colombia⁴⁴ and China.⁴⁵ There are two essential reasons why India should not follow their lead in setting down standards on encryption that are more restrictive than market standards.

First, unlike, say, a Chinese citizen, an Indian internet user is heavily reliant on the services of companies that are based abroad. If India


imposes data disclosure requirements that are not compatible with their domestic standards then there is a likelihood that these requests will fail (as they do under a Mutual Legal Assistance Treaty.) Given the fact that the United States and Germany are the clear market leaders in the number of encryption products,⁴⁶ Indian policymakers must keenly watch the approach that these governments take towards encrypted platforms.

Germany has already adopted a pro-encryption policy⁴⁷ and the United States Government has declined to endorse the controversial Burr-Feinstein Bill that favoured strong restrictions on encryption.⁴⁸ The United States government's approach, however, is clear from the provisions of the Trans-Pacific Partnership (TPP) that it has spearheaded and endorsed. The TPP chapter on 'Technical Barriers to Trade' addresses cryptographic services head-on from a surveillance and access to decrypted data angle. The chapter does not prevent law enforcement agencies of member countries from legally demanding decrypted data from encryption service providers.⁴⁹ In no uncertain terms, however, it restricts member countries from imposing onerous technical regulation on and demanding backdoors to encrypted products. It reads, "No Party shall impose or maintain a technical regulation or conformity assessment procedure that requires a manufacturer or supplier of the product... [to] transfer or provide access to a particular technology, production process or other information, for example, a private key or other secret parameter, algorithm specification or other design detail."⁵⁰ Critics have claimed, and reasonably so, that the provision is little more than lip service by the United States government to data integrity and that many other loopholes exist to force homegrown encryption providers to install backdoors.⁵¹ This, however, is a distinct advantage for countries that have an abundant number of domestic encryption services. This is a luxury that India cannot afford.

Second, as a corollary to India's reliance on foreign encryption tools, it is important for the Indian industry to keep these services in circulation until such time that India's domestic services are able to offer a similar

standard of security. A restrictive encryption policy can cause the exit of state-of-the-art encryption services from the market. Consequently, the market that develops domestically will be technologically stunted from a lack of competition. In the long term, this will leave Indian data vulnerable to exploitation. In the short term, however, the exit of foreign encryption platforms from the Indian market would mean that even the metadata that assists law enforcement agencies would be lost. In essence, this would be a lose-all scenario for Indian law enforcement and intelligence agencies.

Whatever form the encryption policy finally takes, it must bear in mind the plurality of issues involved. It must address the needs of internet users, the ICT industry and the intelligence community in addition to law enforcement agencies. This will require a more direct engagement with multistakeholder platforms that discuss these issues. It must also follow technology neutrality by not treating services differently depending on their willingness to cooperate with law enforcement. Further, the policy must adopt principles that will stay relevant over the next few decades and are not rendered redundant by technology. Digital India's increasing reliance on digital payments and the Aadhaar database means that the government will need to find technologically advanced ways to keep data safe. If India favours the adoption of technologies like Blockchain⁵² for this purpose, it will need to be enabled by a strong encryption policy. Lastly, it must look inward and help develop a domestic cryptography industry that over the next five years is not only able to compete with its global counterparts but be sought after worldwide.

The policy recommendations in this paper offer a starting point towards that goal. They will, however, require engagement with the technical community to create an encryption policy that is truly future-proof. 

ENDNOTES

1. Wilfred Diffie and Susan Landau, "Privacy on the Line: The Politics of Wiretapping and Encryption," MIT Press, (Cambridge, 2007), p. 13
2. Kaveh Waddell, "The Long and Winding History of Encryption," *The Atlantic*, January 13, 2016, <http://www.theatlantic.com/technology/archive/2016/01/the-long-and-winding-history-of-encryption/423726/>.
3. Nicolas Lidzborski, "Staying at the Forefront of Email Security and Reliability: HTTPS-Only and 99.978% Availability," *Official Gmail Blog*, March 20, 2014, <https://gmail.googleblog.com/2014/03/staying-at-forefront-of-email-security.html>.
4. WhatsApp Support Team, "End-to-End Encryption," *WhatsApp.com*, accessed November 10, 2016, <https://www.whatsapp.com/faq/en/general/28030015>.
5. Telegram, "MTProto Mobile Protocol," *Telegram.org*, accessed November 10, 2016, <https://core.telegram.org/mtproto>.
6. Apple Inc. "iOS Security Whitepaper," Apple Inc., May 2016 accessed November 10, 2016, https://www.apple.com/business/docs/iOS_Security_Guide.pdf.
7. US Law enforcement, in the 1970s called for a ban on hard drive encryption of Microsoft
8. Berkman Center for Internet & Society at Harvard University, "Don't Panic: Making Progress on the "Going Dark" Debate," Berkman Center for Internet & Society at Harvard University, February 1, 2016, https://cyber.harvard.edu/pubrelease/dontpanic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.
9. Steven Levy, "Why Are We Fighting the Crypto Wars Again?," *Backchannel*, March 11, 2016, <https://backchannel.com/why-are-we-fighting-the-crypto-wars-again-b5310a423295#.saxlftve3>.
10. Josh Horwitz, "After a Lengthy Battle, BlackBerry Will Finally Let the Indian Government Monitor Its Servers," *The Next Web*, July 10, 2013, <http://thenextweb.com/asia/2013/07/10/after-a-lengthy-battle-blackberry-will-finally-let-the-indian-government-monitor-its-servers/>.
11. In the matter of the search of an Apple iPhone seized during the execution of a search warrant on a Black Lexus IS300, California license plate 35kgd203
12. Apple Inc.'s Reply To Government's Opposition To Apple Inc.'s Motion To Vacate Order Compelling Apple Inc. To Assist Agents In Search in the matter of the

search of an Apple iPhone seized During the execution of a search warrant on a Black Lexus IS300, California license plate 35kgd203 <https://www.eff.org/files/2016/03/15/apple-reply-to-govt-opposition-to-apple-motion-to-vacate.pdf>

13. Supplemental Declaration Of Nicola T. Hanna In Support Of Apple Inc.'S Reply To Government's Opposition To Apple Inc.'S Motion To Vacate Order Compelling Apple Inc. To Assist Agents In Search in the matter of the search of an Apple iPhone seized during the execution of a search warrant on a Black Lexus IS300, California license plate 35kgd203 <https://www.justsecurity.org/wp-content/uploads/2016/03/FBI-Apple-CDCal-Apple-Reply-Declarations.pdf>
14. Kadhim Shubber, "BlackBerry Gives Indian Government Ability to Intercept Messages" Wired, July 11, 2013, <http://www.wired.co.uk/article/blackberry-india>.
15. Adam Matthews, "BlackBerry's India Problem," OPEN Magazine, April 30, 2011, <http://www.openthemagazine.com/article/business/blackberry-s-india-problem>.
16. The Constitution of India, 1950, Article 20(3).
17. M.P Sharma v. Satish Chandra, AIR 1954 SC 300.
18. Internet Architecture Board, "IAB Statement on Internet Confidentiality, Internet Architecture Board, accessed November 10, 2016, <https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/>.
19. Sidharth Pandey, "Is Privacy a Fundamental Right? Constitution Bench of Supreme Court to Decide," NDTV, August 11, 2015, <http://www.ndtv.com/india-news/is-privacy-a-fundamental-right-constitution-bench-of-supreme-court-to-decide-1206100>.
20. CRID – University of Namur, "First Analysis of the Personal Data protection Law in India," Directorate General Justice, Freedom and Security, European Commission, Accessed November 10, 2011 http://ec.europa.eu/justice/data-protection/document/studies/files/final_report_india_en.pdf.
21. Press Trust of India, "Right to Privacy Not a Fundamental Right': Centre Tells Supreme Court," NDTV, July 3, 2015, .
22. Sidharth Pandey, "Is Privacy a Fundamental Right? Constitution Bench of Supreme Court to Decide," NDTV, August 11, 2015, <http://www.ndtv.com/india-news/is-privacy-a-fundamental-right-constitution-bench-of-supreme-court-to-decide-1206100>.

23. Information Technology Act, 2000, §69(B)
24. Bedavyasa Mohanty, "Inside the Machine: Constitutionality of India's Surveillance Apparatus," *IJLT* Issue 12 (To be published)
25. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 3(i)
26. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 2(1)(h)
27. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 6(1)
28. See, Bhairav Acharya, "Comments on the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011", Centre for Internet and Society, March 31, 2013, <http://cis-india.org/internet-governance/blog/comments-on-the-it-reasonable-security-practices-and-procedures-and-sensitive-personal-data-or-information-rules-2011>
29. NASSCOM, "NASSCOM Update on EU Data Protection Regime," NASSCOM http://www.nasscom.in/sites/default/files/policy_update/EU%20data%20Protection%20Regulation.pdf
30. Department of Telecommunications, "Licence Agreement For Provision Of Internet Service (Including Internet Telephony) Amendments," Department of Telecommunications, Ministry of Communications, Government of India, accessed November 11, 2016, Clause 1.10.1, <http://dot.gov.in/granted-issue-guidelines>.
31. Department of Telecommunications, "License Agreement For Unified License," Department of Telecommunications, Ministry of Communications, Government of India, January 8, 2014, Clause 37(1), http://www.dot.gov.in/sites/default/files/Amended%20UL%20Agreement_0_1.pdf?download=1.
32. David Kaye, "Report on Encryption, Anonymity, and the Human Rights Framework," Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32 May 22, 2015, accessed November 10, 2016, <http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx>.
33. Andrew Regenscheid, "Roots of Trust in Mobile Devices" National Institute of Standards and Technology, February 2012, http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-02/feb1_mobility-roots-of-trust_regenscheid.pdf.

34. Reserve Bank of India, Report and Recommendations of the Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds(2011) available at <http://cab.org.in/IT%20Documents/WREB210111.pdf>.
35. Berkman Center for Internet & Society at Harvard University, "Don't Panic: Making Progress on the "Going Dark" Debate," Berkman Center for Internet & Society at Harvard University, February 1, 2016, https://cyber.harvard.edu/pubrelease/dontpanic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.
36. Wilfred Diffie and Susan Landau, "Privacy on the Line: The Politics of Wiretapping and Encryption," MIT Press, (Cambridge, 2007)
37. Reserve Bank of India, Report and Recommendations of the Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds(2011) available at <http://cab.org.in/IT%20Documents/WREB210111.pdf>
38. Securities and Exchange Board of India, Report of the Committee on Internet-Based Securities, Trading and Services(2000) available at http://111.93.33.222/RRCD/oDoc/29-nettrading_200059.pdf(Accessed September 3, 2016)
39. Matt Tait, "An Approach to James Comey's Technical Challenge," Lawfare, April 27, 2016, <https://www.lawfareblog.com/approach-james-comeys-technical-challenge>.
40. Ashley Deeks, "The International Legal Dynamics Of Encryption," Hoover Institution, Series Paper no. 1609, accessed November 10, 2016, <http://www.hoover.org/research/international-legal-dynamics-encryption>.
41. Human Rights Watch, "Russia: 'Big Brother' Law Harms Security, Rights," Human Rights Watch, July 12, 2016, <https://www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights>.
42. Monitoring and Reconciliation of International Telephone Traffic Regulations, 2010, Regulation 5(6), http://www.pta.gov.pk/media/monitoring_telephony_traffic_reg_070510.pdf.
43. Kaveh Waddell, "Kazakhstan's New Encryption Law Could Be a Preview of U.S. Policy," The Atlantic, December 8, 2015, <http://www.theatlantic.com/technology/archive/2015/12/kazakhstans-new-encryption-law-could-be-a-preview-of-us-policy/419250/>.
44. Digital Rights LAC, "The Dangerous Ambiguity of Communications Encryption

Rules in Colombia” Digital Rights Latin America and the Caribbean, January 30, 2015, <http://www.digitalrightslac.net/en/la-peligrosa-ambiguedad-de-las-normas-sobre-cifrado-de-comunicaciones-en-colombia/>.

45. Emily Rauhala, “China Passes Sweeping Anti-Terrorism Law With Tighter Grip on Data Flow,” Washington Post, December 28, 2015, [-tighter-grip-on-data-flow/2015/12/28/4ac6fe06-d79b-4c4c-bda9-27f15fabf892_story.html?tid=a_inl](http://www.washingtonpost.com/archive/local/2015/12/28/4ac6fe06-d79b-4c4c-bda9-27f15fabf892_story.html?tid=a_inl)
46. Bruce Schneier, Kathleen Seidel, and Saranya Vijayakumar, “A Worldwide Survey of Encryption Products,” Berkman Klein Centre for Internet and Society at Harvard University, February 11, 2016, https://cyber.harvard.edu/publications/2016/encryption_survey.
47. Thorsten Benner and Mirko Hohmann, “The Encryption Debate We Need,” Global Public Policy Institute, May 19, 2016, <http://www.gppi.net/publications/global-internet-politics/article/the-encryption-debate-we-need/>.
48. Mark Hosenball and Dustin Volz, “Exclusive: White House Declines to Support Encryption Legislation - Sources,” Reuters, April 7, 2016, <http://www.reuters.com/article/us-apple-encryption-legislation-idUSKCN0X32M4>.
49. Trans-Pacific Partnership, Technical Barriers to Trade, Paragraph 5, Section A, Annexure 8-B, <https://ustr.gov/sites/default/files/TPP-Final-Text-Technical-Barriers-to-Trade.pdf>
50. Trans-Pacific Partnership, Technical Barriers to Trade, Paragraph 3, Section A, Annexure 8-B, <https://ustr.gov/sites/default/files/TPP-Final-Text-Technical-Barriers-to-Trade.pdf>
51. Jeremy Malcolm, “Has the TPP Ended the Crypto Wars? Hardly,” Electronic Frontier Foundation, November 18, 2015, <https://www.eff.org/deeplinks/2015/11/has-tpp-ended-crypto-wars>.
52. A blockchain is a peer-to-peer shared digital ledger that maintains records of transactions. Every participant has an identical copy of the ledger. Any change to a ledger is automatically disseminated to all other copies of the ledger. This ensures that all users have an up-to-date copy. Access to the ledgers are controlled through digital signatures and cryptographic authentication. Blockchains form the core underlying technology of Bitcoins and are what make it so secure.

Observer Research Foundation (ORF) is a public policy think-tank that aims to influence formulation of policies for building a strong and prosperous India. ORF pursues these goals by providing informed and productive inputs, in-depth research, and stimulating discussions. The Foundation is supported in its mission by a cross-section of India's leading public figures, academic and business leaders.



Ideas • Forums • Leadership • Impact

20, Rouse Avenue Institutional Area, New Delhi - 110 002, INDIA
Ph. : +91-11-43520020, 30220020. Fax : +91-11-43520003, 23210773
E-mail: contactus@orfonline.org
Website: www.orfonline.org