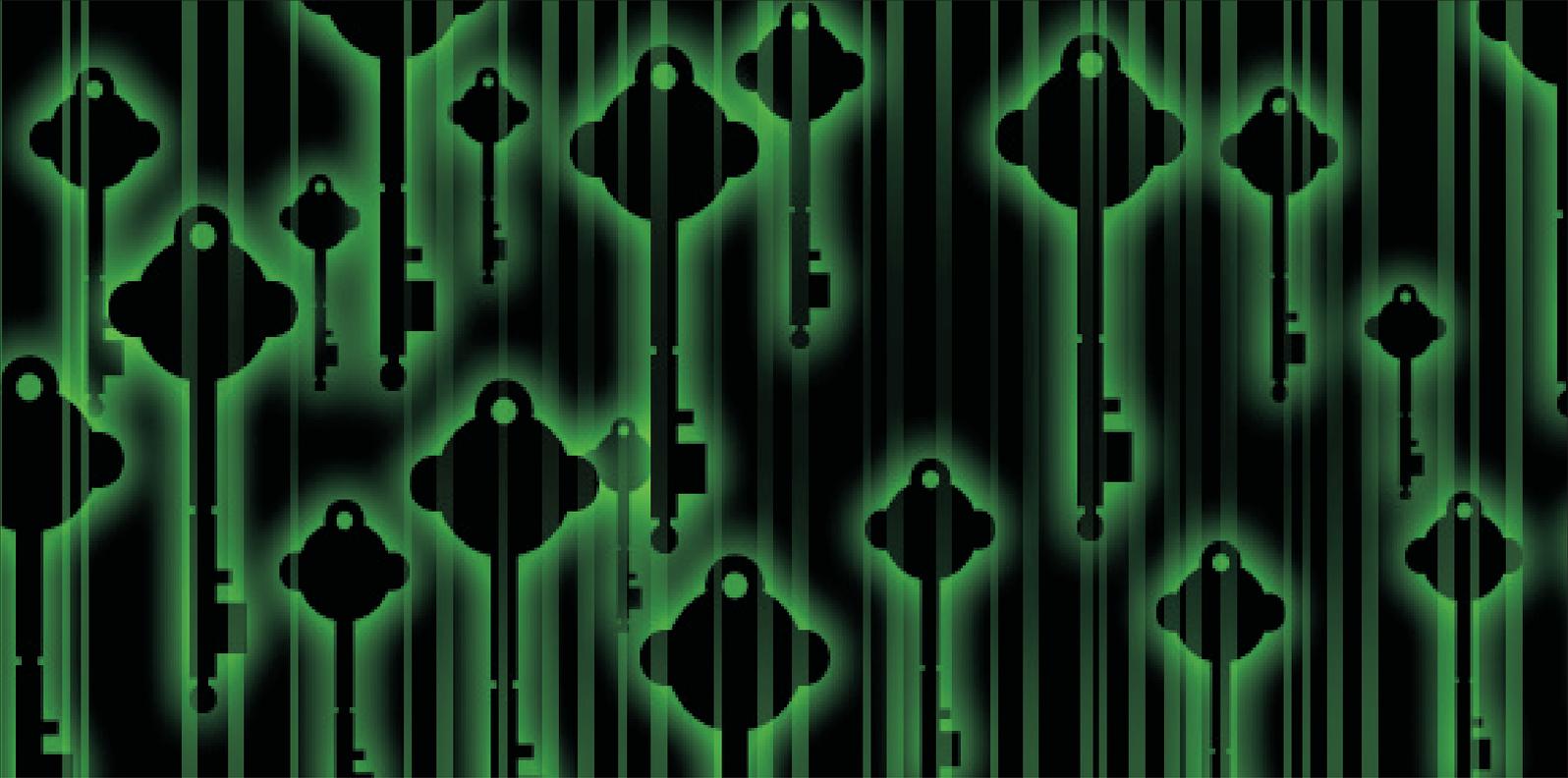


Framing Multistakeholder Conversations On Encryption

Bedavyasa Mohanty and Alexander Spalding



Abstract

On August 12, 2016 the Observer Research Foundation convened the first in a series of multistakeholder roundtables on encryption. This report is the outcome of the discussion of issues and proposal of solutions conducted at the roundtable. Being a complex, technical-legal question around access to data for law enforcement, encryption has long been a contested issue. Creating best-in-class regulation on encryption will require targeted interventions from the industry, civil society, the technical community and intelligence agencies, among other relevant stakeholders. An encryption policy must aim to enhance trust in the digital economy. This, in turn, will require the strengthening of the country's security architecture. Encrypted platforms ensure privacy and help maintain the integrity of data. The policy must, therefore, mandate stronger encryption standards and help incubate a domestic cryptography industry.

Introduction

Following the publication of India's draft National Encryption Policy (NEP) in September 2015—which has since been withdrawn—debates have ensued on questions related to the regulation of encryption technologies across telecommunications services, over-the-top Internet intermediaries, and voice-over IP services. On 12 August 2016, the Observer Research Foundation organised a multistakeholder discussion on encryption, bringing together representatives from the government, civil society, and industry and trade associations, as well as global internet companies. The consultation sought to generate a comprehensive dialogue on the future of encryption, in the hope that future engagements on encryption will prove to be more inclusive of the various stakeholders who play a crucial role in the management of the country's contemporary digital ecosystem.

The multistakeholder panel discussion arrived at some key conclusions. First, that it is in the best interest of India's digital economy to strive for best-in-class encryption norms that can rival those of other leading data protection nations such as Israel, the United States and Germany. Second, that the concerns of encryption policies need to go beyond raw economic considerations, and must also take into consideration the end-user privacy of individual digital consumers. Third, all stakeholders (governments or otherwise) who are to be involved in the evolution of encryption practices in India should acknowledge that encryption standards and technologies are difficult to engage solely at the policy level. As a result, those charged with approaching the issue of encryption may consider moving away from conventional State-centric regulatory practices, and instead allow their regulatory initiative to embody a true multistakeholder—and perhaps, even autonomous—form. Finally, there is a need for a more concerted effort to understand the inherent benefits of encryption, as well as for increased transparency in the rationale given by the government for increased state involvement in the calibration of encryption standards.

This report begins with a discussion of the details of the now-withdrawn draft NEP. The report will then outline various comments that were provided by the stakeholders present at the consultation with regards to how the Indian government can work with civil society, members of the national judiciary, as well as the private sector in order to design a more comprehensive approach to regulating encryption.

The 2015 Draft Encryption Policy

The NEP stipulated a hybrid licensing regime requiring suppliers of encryption technologies and platforms providing encrypted communication channels to deposit their decryption keys with the Indian communications regulator. This requirement complements Clause 37.1 of the Unified License Agreement that explicitly forbids bulk encryption on the licensee's communications networks. The NEP also required for the storage of encrypted messages in plaintext form for 90 days in case law enforcement personnel would need access to the contents of said messages during criminal investigations. Many elements of the NEP drew heavily from both the US Communications Assistance for Law Enforcement Act and the British Regulation of Investigatory Powers Act.

What was therefore being proposed was a hybrid model combining elements of both key escrows as well as backdoors to encrypted devices. The policy mandated that every encryption vendor or service provider operating within the Union of India would need to provide the government with working copies of the software and hardware that have been used for encrypting communications. In the event that law enforcement personnel would require access to a specific communications device, the service provider would be obligated to provide a backdoor through which said law enforcement agency could access the device of interest.

The three principal weaknesses with the NEP that were identified by the stakeholders were as follows:

First, key escrows and the centralisation of encryption keys (as was being stipulated within the NEP) leaves encrypted conversations vulnerable to malicious attacks. The skepticism towards using key escrows in contemporary digital systems stems primarily from two historical precedents: a) debates that took place in the 1990s when the Clinton administration debated the “Clipper

Chip” escrow mechanism in the United States; and b) debates within the Council of Europe during the drafting of the Budapest Convention on Cyber Crime during the early 2000s. A recent report by Abelson et al. addresses the dangers of key localisation, and subsequently makes it clear that the provision of backdoors within encrypted communications networks will jeopardise the integrity of entire communications systems.

Second, the conditions outlined in the NEP raised concerns amongst stakeholders on whether or not the State would misuse its newfound powers over encryption technologies in order to expand surveillance programmes. This question of governmental misuse was of particular concern to civil society representatives who flagged it in the context of ongoing debates around the 'Right to Privacy', whose parameters are not fully defined. In addition to this, there currently exists no formal legal test for determining when a data requisition order can be justified on the basis of a 'national security' concern—a justification that is often offered by security agencies in cases of protracted and unwarranted data surveillance.

Third, concerns were also raised with regards to the lack of judicial oversight stipulated within the NEP. Article 84(A) of the Indian Information Technology Act, 2000 vests the government with the remit to regulate encryption, but the NEP should not, as a result, be twice removed from adequate judicial oversight. Several stakeholders made it clear that future encryption consultations would need to look at whether the final regulation takes the form of a legislation or executive policy, with a view to ensure direct parliamentary oversight of the matter.

Recommendations

The participants at ORF's discussion made it clear that any future attempt at regulating encryption would need to take into consideration the diverse agendas and interests of the various stakeholders involved in the management of India's ICT ecosystem.

First of all, it is clear that encryption needs to be maintained as a normative best governance practice, wherein the security of certain types of communications and transactions needs to be guaranteed. This pertains to the agendas of all of the major stakeholders. The digital economy can only prosper if the commercial transactions taking place within the Union are secure. Regulatory certainty and stability will also prove to be a vital consideration in future efforts to make India a hub for international digital infrastructure. Simultaneously, any encryption reform will also have to respect privacy and free speech—values that India has already pledged itself to protect through its participation in international instruments.

The ORF roundtable also revealed that more discussions need to be conducted to determine which institution or regulatory body is going to be given the mandate of setting technical/encryption standards and protocols. Should the process of setting standards be a bottom-up multistakeholder process, or will it be top-down, by which the government defines certain guidelines on the kind of standards that are to be maintained by communication platforms and professional suppliers of encryption technologies?

If encryption standards are going to be specified, then the appropriate regulatory authority must articulate in a clear and transparent manner the reasons for specifying such a threshold. The debate on key lengths and encryption 'thresholds' is not conclusive: at the workshop, some panellists suggested that India's encryption policy should, at a minimum, mandate the 128-bit encryption suggested by the Reserve Bank of India and the Securities and

Exchange Board of India. Others suggested that key lengths should be voluntarily adopted by the sector in line with its specific requirements. A recommendation that was favoured by many stakeholders at the consultation was to discard the concept of a maximum encryption threshold altogether, and to simply mandate minimum thresholds/ floors instead (particularly on communications implicating government actors). This would institutionalise the use of encryption in Indian digital governance practices.

The governmental agencies responsible for re-drafting the new encryption policy will also need to articulate why an encryption policy needs to be mandated in the first place, and what governmental considerations have subsequently been injected into the design of a newly reformed NEP. In this regard, both civil society as well as private sector stakeholders made it clear that any new encryption mandate must respect the concept of proportionality: encryption regulation must be justified in relation to the concrete objectives that it seeks to achieve. The Indian government should become more forthcoming with regards to what kind of data (note: not specific requests per se) it is demanding through its data requisition protocols. Companies to whom data requisition orders are issued can also play an important part in raising civil society's broader understanding of the kind of data that the government wishes to access. This could be achieved, for example, through the publishing of annual corporate transparency reports that would clearly aggregate and classify all data requisition orders that have been delivered to a company by the Indian government.

Given the fact that there currently exists no constitutionally codified 'Right to Privacy' within Indian law, many stakeholders suggested that the encryption debate in India may indeed be premature. They raised concerns over whether an encryption policy would be effective without formal legal safeguards for the protection of individual privacy.

Conclusion

An agreeable resolution to the encryption debate in India should acknowledge and balance the concerns of all stakeholders. India's digital economy can only be as robust as the measures that are in place to protect the data and transactions flowing through its networks. Businesses and consumers operating within the Indian digital economy need to be assured of the integrity and authenticity of their data, and encryption plays a major role in fulfilling these requirements. As India's digital markets prosper, they are likely to attract attacks of increasing sophistication, both from state and non-state actors, necessitating the creation of secure and encrypted networks. At the same time, law enforcement agencies in India will come under increasing strain to investigate and prosecute cyber-crimes, as well as 'offline' criminal activities coordinated through digital networks. Their capacity to enforce the rule of law is critical to the digital economy's smooth functioning and in maintaining public confidence in safe and accessible digital spaces. To the extent that pervasive encryption technologies are implicated in the process of accessing electronic data, the concerns of LEAs must also be taken into account.

Whether this 'resolution' of India's encryption debate takes place through a policy is another question altogether. Any encryption policy articulated by the Indian government should be mindful of the reality that technological developments are likely to outpace such regulations in a matter of years. Higher encryption standards, implemented first by the private sector and gradually absorbed by public-sector undertakings, can become the norm without having black letter regulations in place. Similarly, the capacity of law enforcement agencies to tackle crimes online is not strictly related to the encryption standards prescribed by the government. Given that internet users in India will increasingly rely on communication platforms and financial gateways built in the United States and Europe, law enforcement agencies have no option but to strengthen

their ability to retrieve data from foreign companies – with or without an encryption policy in place.

In India, conditions for lawful access to data are prescribed under Section 69 of the Information Technology Act, 2000 and rules made pursuant to this section. Given this legislative ability, some have wondered if it is within the remit of an encryption policy to prescribe access to electronic data. The mandate of an encryption policy, the argument goes, must only be limited to setting the modes and medium for encryption. It must not duplicate or circumvent due procedure prescribed under Indian statutes.

Regulators, therefore, are faced with three distinct choices: draft a 'future-proof' encryption policy that mandates the highest possible encryption standards, proceeding on the assumption that the ability of India's law enforcement agencies will grow commensurately; draft a policy that mandates low encryption standards for devices and products currently available in the market, with a view to intercepting their contents; defer the drafting of an encryption policy with the understanding that such policies cannot keep pace with evolving technologies.

Of the three, having a token policy with low standards of encryption is the least attractive option for the Indian government, businesses and consumers alike. While it may facilitate for LEAs the access that they need for crime investigations/ prosecutions, mandating lower encryption standards will only pull down the overall security of the ICT ecosystem. Not only would such a policy discourage cyber security innovation and the introduction of state-of-the-art devices into the digital economy, it will render Indian users vulnerable to attacks by malicious actors.

In a growing market like India, where a majority of encryption platforms originate internationally, there is some merit in pursuing a hands-off approach towards an encryption policy. As mentioned previously, most providers of popular encryption platforms currently originate from the Silicon Valley and this trend is unlikely to change in the next decade. The attractiveness of such platforms, and the Indian user's unhindered access to them is partly

responsible for the country's rapidly growing rate of internet penetration. Encryption policies should not set the clock back on such growth.

If, however, India seeks to develop a domestic market for encryption products and services, it can ensure that technological development is guided by regulation. This can only be based on an assessment of the overall consumption and trends in use of encryption services by Indian users and businesses. In the United States and United Kingdom, for example, encryption technologies have evolved rapidly with a concurrent enhancement in the interception capabilities of law enforcement agencies. This is not the case in India, and indeed the rest of Asia, Africa and Latin America. Were the government to consider implementing an encryption policy, policymakers should also consider the possibility that these regulations may be emulated by other emerging markets in the future.

This encryption policy must back advancements in technology, and follow international best practices. It must be complemented by strengthening the capacity of law enforcement agencies through the streamlining of processes under Mutual Legal Assistance Treaties and negotiating data-sharing agreements with countries that handle the bulk of Indian data.

What would some of the most important aspects of such a policy look like?

1. Mandating 256-bit (or higher) encryption to secure government-to-government communications.
2. Mandating 256-bit (or higher) encryption to secure government-to-business, business-to-business, and business-to-consumer communications and transactions.
3. Facilitating the adoption of voluntary standards of encryption by the private sector to secure consumer-to-consumer communications.
4. Registration of all vendors and platforms providing encryption technologies in India. The registration process

should be semi-automated (to allow for the verification of supplier credentials), and involve no licensing of products or services.

5. Implementing judicial safeguards to regulate the lawful interception of encrypted data.
6. Where feasible, mandate access to physical devices obtained lawfully by enforcement agencies in pursuance of an investigation.
7. Enabling a discussion on “lawful access”, i.e., clarifying the liability regimes on the consumer and the intermediary as it pertains to electronic data that is sought.
8. Streamline the process of government acquisition of zero day vulnerabilities, with a strict requirement of disclosure once their limited purpose is served.

These recommendations, however, must also keep in mind concerns of the industry with regard to setting limits on key lengths for encryption. It was suggested during the ORF roundtable that from the perspective of an internet business, setting both minimum and maximum key lengths can be counterproductive. The strength of encryption required varies greatly from one industry sector to the next. It was argued that the sheer diversity of considerations ranging from specific security needs, product design, compatibility, performance, and other variables, make it difficult for a one-size-fits-all approach to be effective. For instance, specifying a minimum level of encryption may hinder a business' ability to detect malware or filter spam.

A strong encryption policy can upgrade the overall standard of security in cyberspace, enhance free speech and stimulate e-commerce. It can also encourage domestic research and development in cyber security and cryptographic tools. This will not only address the technology deficit that Indian law enforcement suffers from but also provide them with the much needed human resources to assist with cyber-related crimes. It can also buttress India's data protection norms which not only increases trust within the country but also makes the Indian market a more attractive

destination for international trade. As more companies situate their data in India – not on account of data localisation policies, but because it is financially attractive to set up base in the country – the menu of policy options available to LEAs to investigate and prosecute cyber crimes will also expand simultaneously. But the encryption policy should not be tied down by the complex bilateral and multilateral conversations around electronic data sharing. 

(This multistakeholder consultation was supported by grants from the William and Flora Hewlett Foundation and Google Inc.)

ABOUT THE AUTHORS

Bedavyasa Mohanty is Junior Fellow, and Alexander Spalding is Research Intern, at the Observer Research Foundation's Cyber Initiative.

CHAIRS

- Samir Saran - Vice President, Observer Research Foundation
- Arun Mohan Sukumar - Head, Cyber Initiative, Observer Research Foundation

PANELLISTS

- Gulshan Rai - Coordinator, National Cyber Security, Prime Minister's Office, Government of India
- Ankhi Das - Director of Public Policy for Facebook - India, South and Central Asia
- Bedavyasa Mohanty - Junior Fellow, Observer Research Foundation
- B. Prasanna - Data Security Consultant, GigSky
- Subho Ray - President, Internet and Mobile Association of India
- Karuna Nundy - Lawyer, Supreme Court of India

ENDNOTES

1. Key escrow is the process by which governments have every encryption service or provider retain a decryption key with a third party. That third party can then provide the decryption key to the government for investigation purposes.
2. Harold Abelson, et al. “Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications,” *Communications of the ACM*, 58:10 (2015).
3. 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> (Accessed September 3, 2016)
4. 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)



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



To know more about
ORF scan this code

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.