35

ORF SPECIAL REPORT

MAY 2017

Encryption Policy 2.0: Securing India's Digital Economy

BEDAVYASA MOHANTY

Source: brewbooks/Flickr

INTRODUCTION

The Observer Research Foundation, in collaboration with the Centre for Internet & Society and the Takshashila Institution, convened a multistakeholder consultation on encryption at the TERI campus in Bengaluru on 17 December 2016. Representatives from government, industry, the technical community and civil society participated in the discussion. The roundtable was the second in a series of multistakeholder consultations on encryption organised by ORF. The first, held in New Delhi on 12 August 2016[1] with law enforcement agencies, businesses and regulators, provided context for the conversation in Bengaluru. The second roundtable was convened in Bengaluru to engage the city's vibrant technical community– comprising individuals from the IT sector, and representatives from internet companies, the government, and academe.

Over the past year, encryption has been at the forefront of conversations on cyber regulation and human rights. The development of full disk encryption, which renders data stored on hard drives unrecoverable, and the easy availability of end-to-end encrypted communication services has become a major concern for law enforcement agencies seeking data for investigation and prosecution. Encryption, however, involves a multitude of actors and manifold, complex issues. While some of these issues have attained relative clarity over time, many others remain unresolved.

When the Department of Electronics and Information Technology (now Ministry of Electronics and Information Technology) invited comments from industry associations and civil society on encryption, it stated that a questionnaire for comments and suggestions would also be circulated among them. No such questionnaire was released, however.

The government's attempts at drafting a multistakeholder policy will bear fruit if it clarifies its stance on the various aspects of encryption so that stakeholders can provide constructive inputs. Meanwhile, stakeholders need to engage in consensus-building exercises to make their inputs targeted. ORF's Bengaluru roundtable highlighted many issues that were central to the encryption policy – all of which need closer consideration. This paper, through multistakeholder inputs, tackles some of the issues that were highlighted in the Draft Encryption Policy of 2015 and suggests policy priorities for the next iteration of the policy.

KEY QUESTIONS

Bulk Encryption

In 2012 when the Department of Telecommunications sought to converge internet and telephony services, it introduced the Unified License (UL) to phase out the Internet Service Provider (ISP) License. The UL dropped the ISP license's provision[2] that barred encryption by service providers over a 40-bit key length. The UL, however, retained the ISP license's ban on 'bulk encryption'[3]—thus leaving his ban in policy purgatory for many years now. As most internet services today use encryption in one form or another, this provision has become more relevant than ever.

The sectoral regulations on encryption have far surpassed the 40-bit restriction on encryption. The Information Technology (Certifying Authorities) Rules 2000, for instance, mandate that authentication of digital signatures is to be undertaken via public key cryptography.[4] The level of security prescribed for this purpose is the RSA Encryption Standard which uses 512, 1024 or 2048 bit encryption.[5] Similarly, The Reserve Bank of India[6] and Securities and Exchange Board of India[7] have recommended that for financial transactions, 256-bit encryption should be made the default standard.

There is now a growing agreement between service providers and consumers that the ban on bulk encryption must be revisited. Globally, law enforcement officials too are beginning to realise that encryption is critical for security and are only requesting the ability to access communications when lawfully authorised.[8] A ban on bulk encryption, therefore, is undesirable for all the actors involved. One of the most significant contributions of the new encryption policy will be clarifying this regulatory confusion and possibly, overriding the ban on bulk encryption.

Key Lengths

Attempts to regulate the strength of encryption were among the most criticised aspects of the draft encryption policy. The policy stated that the government would prescribe encryption algorithms and key sizes for all forms of communications, be it businesses, citizens or government employees. This was considered problematic. If the government sets a low standard like the 40-bit ceiling prescribed in the ISP license, then most internet companies would have to slide back on the level of security over their networks to comply with the policy. If, on the other hand, the government prescribes too high a standard for encryption, it may prove burdensome for businesses to upgrade their networks to remain compliant with the policy.

Most stakeholders share a fundamental concern that the policy seems to be leaning towards denying the user a choice in key length. During the Bengaluru consultations, many stakeholders supported the view that citizen-to-citizen communications (C2C) should not be regulated by the government through the prescription of either maximum or minimum key lengths. Rather, citizens should be free to adopt services based on the level of security they require.

The question that arises then is whether or not relaxations on the strength of encryption should be extended to business entities as well. This is a complex question. Whereas citizens need protection of their information against unauthorised surveillance by the state, businesses need to protect their data from malicious actors that would commercially exploit them. Indeed, the number and complexity of such exploits has increased in recent years. These looming threats make setting minimum key lengths for encryption a sensible decision for B2B and B2C communications. There are concerns, however, from the email providers that high encryption—especially end-to-end encryption—makes spam filtering and targeted advertising difficult. This, in turn, makes their services less efficient and less profitable. Some companies, such as the Switzerland-based secure email service Protonmail, are testing mechanisms to effectively filter spam despite strong encryption. However, stakeholders in Bengaluru were of the opinion that until such time that most service providers have tested and adopted these mechanisms, it may be prudent to avoid setting any minimum or maximum key length for encryption. The policy should then set minimum key lengths only for government communications and the sectors such as banking and energy, identified as Critical Information Infrastructure because these need immediate protection.

Registration v. Licensing

In order to access data, governments often enter into agreements with companies collecting electronic information. This can even take the form of a licensing regime where only licensed providers of encryption services would be allowed to operate in a certain market. Naturally, both industry and consumers are wary of a licensing regime as it gives the government discretionary power to allow or disallow services. Governments may favour only those services that allow them unhindered access to data and thus make communications unsecured. However, while dealing with encrypted data, law enforcement agencies need technical assistance that can only be provided by the company.

Some countries like Israel regulate "Engagement in Encryption"[9] through a licensing regime. The stated objective of the regime is control over dual-use encryption technologies.[10] However, in practice, the licensing mechanism is leniently enforced and is instead used to foster a relationship between the private sector and Israeli authorities.[11] This helps keep the authorities abreast of technical developments in the field of cryptography and, in exigent circumstances, enables information exchange. Indian policymakers too would be well advised to adopt a mechanism that allows them to cooperatively exchange information with the private sector rather than compel companies to retard encryption in their products.

An alternative to a licensing arrangement is a voluntary registration mechanism where encryption providers voluntarily register with the government. The companies can also provide information such as the strength of encryption in their software, or a point of contact for law enforcement decryption requests. As this registration process is voluntary, no penalty can be attached with not registering. Instead, the government can devise ways to incentivise registration.

Enforcement of the policy

One aspect of the policy that has not yet been addressed is the enforcement of its prescriptions. The Draft Policy of 2015 offered no indication about the specific ways in which the policy would be enforced. One of the greatest roadblocks to enforcement is the sheer number of encryption products and technologies that are available online. Users, including those who seek to use encryption for illegal purposes, will always find a way to make their communications anonymous through either one of various over-the-counter products or the Dark Web. For instance, the last Yahoo email hack affecting 500 million users saw a complementary migration of users to Proton mail, a Switzerland-based, end-to-end encrypted email service that does not cooperate with law enforcement data requests.[12] No umbrella policy will, therefore, be able to cover or curtail the proliferation of all encryption products.

This then begs the question, what products does the encryption policy seek to regulate? One explanation is that the policy will only regulate those encryption services and products that are used by a substantial number of users, such as email and chat clients, among others. If this is the case, then the policy would be well-served to clarify this for two reasons. First, by limiting its scope, the policy is less likely to fail in the enforcement of its guidelines. Second, if the policy ultimately prescribes necessary changes to technology and protocols, then bigger companies with large amounts of capital at their disposal would be better placed to incorporate these changes than smaller fledgling startups.

ZERO DAY VULNERABILITIES

While stronger encryption is better both for the overall standard of security as well as the digital economy, the policy must also seek to balance law enforcement's need for data in certain exigent circumstances where significant threats to national security exist. Retaining access to data is increasingly becoming possible through the acquisition of zero day vulnerabilities in software. 'Zero days' are thus named for that fact that once discovered, both developer and exploiter have zero days left to either patch the vulnerability or exploit it. Governments are now becoming the biggest investors in the underground zero day market as they build a stockpile in anticipation of a cyber-attack on their systems. The United States government is one of the largest investors in zero day[13] with an annual budget of $25.1 million dedicated for this purpose.[14] The Indian government's intrusive capability is in all likelihood built on a stockpile of zero days[15] whose utility is limited by a constant tussle with the software developer's attempts to patch the vulnerability. The encryption policy should then be complemented by a zero day acquisition policy that can prescribe time limits within which law enforcement can be compelled to disclose the existence of the vulnerability to the software developers. The US Vulnerabilities Acquisition Process is one of the few institutionalised systems that allows for cooperation among various law enforcement agencies and sets disclosure mandates. There are many, however, who argue that such a policy is likely to be outside the ambit of the encryption policy and must be created as a complementary policy.

Bifurcation of Policy

There are also increasing concerns that the encryption policy that was primarily meant to strengthen India's cyber systems is getting unnecessarily securitised. Some experts have even referred to the 2015 Draft Policy as the 'decryption policy.' The encryption policy, the argument goes, can only have one priority: to enhance the level of security by setting higher standards of encryption or mandate data retention and data disclosure by setting lower standards of encryption. Both imperatives are compelling but competing. There were stakeholders in the Bengaluru roundtable who were of the view that security and privacy can only be achieved if the policy is bifurcated into two parts—one dealing with high standards and the other dealing with decryption mandates. From a policy coherence standpoint, however, this may appear to be another step that will lead to the creation of a set of contradictory guidelines no different from the status quo. This suggestion, therefore, is unlikely to hold much water with New Delhi's policymakers.

CONCLUSION

Whatever form the final encryption policy takes, the primary objective of the policy must be to secure the information security architecture of the Indian digital economy. Multiple analyses of law enforcement access for data have concluded that the decryption of data alone is no guarantor of national security. Moreover, little data is available about the extent to which access to encrypted data will actually assist in the pursuit of criminal investigations. In the United States, for instance, of the 14,500 wiretap requests made between 2012 and 2015, only 0.2 percent encountered unrecoverable encryption.[16] If the number of encrypted devices in the US (47 percent of all devices) is compared with that of India (10 percent),[17] then the percentage of law enforcement requests in India encountering indecipherable encryption is likely to be even lower. This is not to dismiss the reality that the prevalence of end-to-end encryption platforms does pose a concern for Indian law enforcement agencies, especially as it relates to counter-terrorism efforts. But policy solutions—as distinct from technology-driven solutions—that seek to restrict encryption are only likely to work for a short while, if at all. Knowledge that a particular platform's data is accessible to the government will only cause criminals to migrate to more obscure services. The encryption policy must set out a forward-looking agenda for the Indian digital economy, affirming the basic tenet that strongly encrypted devices and platforms are needed and recommended to secure the data of Indian institutions, businesses and users.

ABOUT THE AUTHOR

Bedavyasa Mohanty is Junior Fellow at the Observer Research Foundation's Cyber Initiative.

ENDNOTES:

1. Bedavyasa Mohanty and Alexander Spalding, “Framing Multistake holder Conversations on Encryption”, ORF Special Report No. 29, December 6, 2016, http://www.orfonline.org/research/framing-multistakeholder-conversations-on-encryption/

2. Condition 2.2(vii), “License Agreement for Provision of Internet Services”, Department of Telecommunications, Ministry of Communications and Information Technology, January 2010, http://www.dot.gov.in/sites/default/files/L%20A%20after%2025.01.10(1)_0.doc?download=1.

3. Condition 37.1, “License Agreement for Unified License”, Department of Telecommunications, Ministry of Communications and Information Technology, March 29, 2016, http://www.dot.gov.in/sites/default/files/2016_03_30%20UL-AS-I.pdf?download=1.

4. Rule 3, The Information Technology (Certifying Authorities) Rules 2000

5. Rule 6, The Information Technology (Certifying Authorities) Rules 2000

6. 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

7. 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

8. James Lewis et al, “The Effect of Encryption on Lawful Access to Communications and Data”, *Centre for Strategic and International Studies*, February 2017, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170221_Lewis_EncryptionsEffect_Web.pdf?HQT76OwM4itFrLEIok6kZajkd5a.r.rE.

9. Law Governing the Control of Commodities and Services - 1957 (5717) Order Regarding the Engagement in Encryption Items - 1974 (5734), http://www.mod.gov.il/English/Encryption_Controls/Pages/order.aspx.

10. Encryption Controls in Israel, Ministry of Defence, Israel http://www.mod.gov.il/English/Encryption_Controls/Pages/default.aspx.

11. Matthew Waxman and Doron Hindin, “How Does Israel Regulate Encryption”, *Lawfare*, November 30, 2015, https://www.lawfareblog.com/how-does-israel-regulate-encryption.

12. Paul Sawers, “Encrypted email app ProtonMail reports surge in users after latest Yahoo hack revealed,” *Venture Beat*, December 22, 2016, https://venturebeat.com/2016/12/22/encrypted-email-app-protonmail-reports-surge-in-users-after-latest-yahoo-hack-revealed/.

13. Jospeh Menn, “SPECIAL REPORT - U.S. cyberwar strategy stokes fear of blowback”, *Reuters*, May 10, 2013,http://in.reuters.com/article/usa-cyberweapons-idINDEE9490AX20130510.

14. Brian Fung, “The NSA hacks other countries by buying millions of dollars' worth of computer vulnerabilities”, *The Washington Post*, August 31, 2013 https://www.washingtonpost.com/news/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities/?utm_term=.6d5a51ce08f3.

15. Nicole Perlroth & David E. Sanger, “Nations Buying as Hackers Sell Flaws in Computer Code”, *The New York Times*, July 13, 2013, http://www.nytimes.com/ 2013/07/14/ world/europe/nations-buying-as-hackers-sell-computer-flaws.html.

16. US Courts, “Wiretap Reports,” http://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports.

17. Supra Lewis et al.

ORF OBSERVER RESEARCH FOUNDATION

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