If India’s encryption policy is to be effective, it must mandate higher standards and enhance trust

2017-1-24

Regardless of which digital jurisdiction an individual finds themselves in, encryption will always be an intensely controversial issue. It is therefore important to have comprehensive dialogues on the management of India’s contemporary digital ecosystem, which engage stakeholders from across the board. Reflecting on a recent Observer Research Foundation initiative to do just this, ***Alexander Spalding*** *writes that as it attempts to assert itself as a global digital hegemon, India needs to realise that its digital economy can only be as robust as the measures that are in place to protect the data and transactions in its networks.*

Societies across the world are experiencing unprecedented rates of digitisation. Indeed, more and more financial, social, and political activity is occurring in cyberspace everyday on account of the secure and reliable transactional platforms that are now available. In order to ensure that the digital ecosystem continues to function as a conducive tool for the advancement of favourable conditions in our changing world, the global effort to manage the evolution of cyberspace needs to take the integrity and protection of end-user data very seriously. This is why regardless of which digital jurisdiction an individual finds themselves in, encryption — on account of the complex legal and logistical technicalities that arise in relation to managing Governmental access to private data circulating in cyberspace — will always be an intensely controversial issue.

As part of its attempt to revolutionise the degree of engagement in the realm of Indian policymaking, the Observer Research Foundation organised a multistakeholder discussion on encryption in Delhi, bringing together representatives from the government, civil society, industry and trade associations, as well as global internet companies. The consultation sought to generate a comprehensive dialogue on the future of encryption India, in the hope that future engagements would prove to be more inclusive of the different actors who play a fundamental role in the management of India’s contemporary digital ecosystem. The need to revolutionise the nature of Indian policymaking debates (particularly in relation to cybersecurity) became apparent after the first National Encryption Policy (henceforth ‘NEP’) had to be swiftly withdrawn by the Government in September 2015 on account of how much fierce backlash the policy faced from leading civil society and industry representatives.

The now-withdrawn initial NEP was composed of two essential parts. Firstly, it stipulated the generation of a hybrid licensing regime requiring suppliers of encryption technologies and platforms providing encrypted communication channels to deposit their decryption keys with the Indian communications regulators. This also meant that every encryption vendor or service provider operating within the Union off India was expected to provide the Government with working copies of the software and hardware that said vendor or service has used for encrypting communications. Secondly, the NEP also required for the storage of encrypted messages in plain text form for 90 days in the event that law enforcement personnel would require access to the contents of said messages during criminal investigations. What was therefore being proposed was a hybrid model combining elements of both key escrows as well as backdoors to encrypted devices that drew heavily from both the US Communications Assistance for Law Enforcement Act and the British Regulation of Investigatory Powers Act .

It became immediately clear that this proposed policy was problematic for three reasons. Firstly, the centralisation of encryption keys within easily identifiable central key escrows leaves encrypted conversations vulnerable to malicious attacks from unwanted third-parties. Mandating the inclusion of backdoor access to these key escrows also jeopardises the integrity of entire encrypted communications systems. Secondly, the conditions outlined in the NEP raised multiple concerns about the prospect for the State abusing its newfound surveillance powers, a concern that is understandable in the context of a digital jurisdiction like India wherein not only does the law not guarantee an individual ‘Right to Privacy’ (as in such leading digital economies as Germany), but also that the legal test for justifying a State-initiated data requisition order (on the grounds of a ‘national security concern’) is currently ambiguous, open-ended, and legally precarious. Finally, concerns were also raised in regards to the lack of judicial oversight within the NEP. It therefore became clear that the stipulations of the NEP were not created in the interest of all major stakeholders, and were therefore simply intended to function as a means through which the Indian state could legitimately expand its already extensive surveillance regime.

One of the most important recommendations that arose from the multistakeholder debate was that any conceivably sustainable encryption policy must ultimately aim to enhance trust in the way that each respective stakeholder conducts themselves in the digital economy. Furthermore, on account of how encrypted platforms ensure end-user privacy and help maintain the fundamental integrity of data, any policy reformulation must mandate stronger and more transparent encryption standards as well as help incubate a more institutionalised domestic cryptography industry. This should be complemented by enabling a discussion on ‘lawful access’, which refers to clarifying the liability regimes on the consumer and the intermediary as it pertains to electronic data that is sought.

Stronger encryption standards reflect the maintenance of encryption as a normative best governance practice (in the interest of privacy and free speech) whilst increasing the transparency of the reasoning behind the advancement of a particular set of encryption thresholds makes it easier for individual stakeholders to understand the Government’s sincere intentions when it comes to accessing encrypted data. Increasing regulatory transparency and the definition of legal access ultimately ensures that encryption regulation respects the concept of regulatory proportionality, which is in turn a consideration that is of paramount important if confidence in individual stakeholder behaviour within the digital economy is to be increased.

For a state whose governance practices have been characterised by intense state-centric, top-down intervention in the lives of its citizens since Independence, the embrace of multistakeholder debate in regards to Indian encryption standards marks an important shift in the way that national governance practices in India are being reformulated by global forms of neoliberal governmentality. In its attempts to assert itself as a global digital hegemon, India needs to realise that its digital economy can only be as robust as the measures that are in place to protect the data and transactions flowing through its networks. In its attempts to advance multistakeholder dialogue on the issue of encryption, therefore, India is signalling to the world that it is ready to establish itself as a pioneer for modelling how all stakeholders can symbiotically contribute towards the successful evolution of both the national and global digital economy.

This article is based on a report co-authored by Bedavyasa Mohanty and Alexander Spalding Framing multistakeholder conversations on encryption*. Read the full report here.*

Alexander also wrote a Student Diary article for South Asia @ LSE about his experience interning at the Observer Research Foundation. Read the post here.

Cover image credit: Blue Coat Photos. CC BY-SA 2.0

This post gives the views of the author, and not the position of the South Asia @ LSE blog, nor of the London School of Economics. Please read ourcomments policy before posting.

About the Author

Alexander Spalding *is a third-year student of Social Anthropology at the London School of Economics and Political Science. He spent his summer working with the Observer Research Foundation as a policy research intern with the think-tank’s cyber-security team in Delhi. While in India he also conducted ethnographic research on the way that former street children use the Delhi ‘street theatre’ scene as a therapeutic domain, and travelled extensively in Rajasthan and the Indian Punjab.*