DGN Policy Brief 10
March 2021

Backdoors to Encryption: Analysing an Intermediary's Duty to Provide "Technical Assistance"

Rishab Bailey, Vrinda Bhandari and Faiza Rahman

- *The government should avoid implementing a general mandate for intermediaries to either weaken encryption standards or create backdoors in their products/platforms because this constitutes a disproportionate intrusion into the right to privacy. Such a mandate will also likely fail a cost-benefit analysis in view of the possible effects on network security, the availability of alternatives with law enforcement agencies (LEAs), the limited impact of such a move on criminal use of the Internet, and geopolitical considerations.*
- *India must instead seek to implement rights-respecting processes to enable law enforcement to access data collected by intermediaries in a timely manner. The government must also take a more long-term perspective by seeking to enhance its capacities, including by developing hacking capabilities, with sufficient regulatory oversight.*

Context

The rising use of encryption is said to be problematic for LEAs, in that it directly impacts their ability to collect data required to prosecute offences. This has led to various proposals to address this perceived impasse, although there is no global consensus on best practices dealing with unrecoverable encryption.[i] In India, the government has proposed adopting new Intermediary Guidelines under the IT Act, 2000, that seek to extend the "technical assistance" mandate of intermediaries to ensure "traceability", although the term has not been clearly defined.[ii] This provision goes beyond existing mandates in the law that require holders of encryption keys to provide decryption assistance, when called upon to do so, in accordance with due process and based on their capability to decrypt the information. Courts have also been called to weigh in on this debate, with the Madras High Court and the Supreme Court hearing petitions that seek to facilitate LEA access to end-to-end encrypted (E2E) content (through backdoors) on platforms such as WhatsApp, although there has been no definitive ruling so far.[iii] A Rajya Sabha Ad-hoc Committee Report released in 2020 has also recommended that LEAs be permitted to break or weaken E2E to trace distributors of illegal content.[iv]

- Against this background, the paper examines the scope of the obligations that ought to be imposed on intermediaries to provide "technical assistance" to LEAs, and whether that should extend to weakening standards of encryption, such as through the creation of backdoors. The paper also examines, in brief, proposals for alternatives, such as the use of escrow mechanisms and ghost protocols.
- The paper begins with an introduction to the concept of encryption, provides a background to the global encryption debate, and outlines the legal framework governing encryption in India. The paper then examines the problems caused to LEAs by the use of encryption – both recoverable and unrecoverable - and contrasts these with the concerns that are likely to arise due to an enhanced "technical assistance" mandate. The paper concludes with an examination of the constitutionality of a general mandate to create backdoors in encryption products, while also pointing to various factors that must be considered before implementing such a policy such as the effects on privacy, network security, geopolitical implications, etc.

Main arguments

- Encryption secures against unwanted access to communications. This ensures confidentiality and integrity of data and creates trust in electronic systems.
- However, the use of encryption can enable bad actors to "go dark", thereby making it difficult for LEAs to carry out their functions.
- The concerns with the use of encryption are driven by a number of factors, namely growing instances of cybercrime, the growing use of strong encryption being embedded by default into technology products (such as WhatsApp

and Signal), the increased use of authentication features in devices such as the passcode to unlock an iPhone, and the use of data minimisation practices such as transient messaging or 'disappearing messages'.

• These concerns have led to calls for intermediaries to weaken encryption standards or create backdoors in their products/platforms.

• However, the creation of backdoors is problematic for the following reasons:

- Privacy: Private thoughts and communications, being an expression of a person's identity, deserve protection from unwarranted government intrusion. Surveillance can also lead to unwanted behavioural change at social and individual levels and create a chilling effect.
- Security: Creating backdoors can weaken network security as anyone can exploit them, not just the government.[v] Backdoors create single points of failure – which is bad system design. They can also lead to greater complexity in system design, which can make networks more vulnerable to attack.[vi]
- Mandating decryption can be seen as violating an individual's right against self-incrimination.[vii]
- Surveillance itself is not meant to be a frictionless process. It has been argued: (a) that introducing inefficiencies in the functioning of LEAs is what separates a police state from a democracy,[viii] and (b) India has seen a shift towards a "due process" model from a "crime control model".[ix] Encryption creates procedural hurdles, ensuring some checks and balances over the functioning of LEAs, and the possibility of mass surveillance, thereby re-balancing the asymmetric power distribution between the State and citizen

• Given these concerns, should the duty of "technical assistance" extend to the creation of backdoors?

- As far as recoverable encryption is concerned, there is no need for creation of backdoors as the intermediary already has the decryption key. The focus in such cases should be to implement proper oversight and other procedural frameworks to ensure that LEAs exercise their powers of surveillance or decryption appropriately. The Indian statutory framework is lacking in this regard. There is no judicial oversight, no proportionality requirements in the law, and no meaningful checks and balances over decryption processes. We have proposed changes along these lines in order to improve the transparency and accountability of the system.
- The situation with regard to unrecoverable encryption is more complex since only the user can decrypt the content. However, even in this case, mandating backdoors is not an appropriate policy answer, as:
  (i) LEAs have multiple alternatives to collect information, including by accessing metadata and unencrypted backups of encrypted communications. They can also use targeted surveillance methods to conduct investigations.[x]
  (ii) India is already using spying technology, as we saw in the Pegasus case, although we recommend that such a procedure should be institutionalised only after introducing regulatory oversight. LEAs also have other methods they can use - from key-stroke logging programs to exploiting weaknesses in implementation of encryption systems.[xii]
- Accordingly, there may be a need to carry out a more detailed cost-benefit analysis in such cases. This exercise should consider, *inter alia*:
  (i) The number of cases where unrecoverable encryption has proved to be a hurdle for LEAs in collecting relevant information.
  (ii) The cost to intermediaries in changing their platform architecture.
  (iii) The risk of such laws getting caught up in global geopolitics.[xiii]
  (iv) Whether such laws will be effective, considering that many criminals may use open source encryption or encryption from platforms that are not located within Indian jurisdiction.[xiv]
- Finally, while a mandate for targeted decryption or assistance may be constitutional if it is backed by a law with sufficient safeguards, a general mandate for creation of backdoors is unlikely to pass constitutional muster, assuming a high intensity of proportionality review is applied. A higher intensity of judicial review will have to look not just at whether the proposed intervention would substantially improve national security,

but would also need to engage with the fact that it would (a) compromise the privacy and security of individuals at all times, regardless of whether there was any evidence of illegal activity on their part, and (b) that LEAs have other alternative means available to them to carry out investigations. Thus, the paper highlights how a general mandate for backdoors is not the least restrictive measure available.

Conclusion/Policy recommendations

• A general backdoor to 'break' unrecoverable encryption is not proportionate, given the significant privacy and security concerns, and the alternatives available with LEAs to aid their investigation processes.
• The Indian government should support the development and use of strong encryption systems.
• Rather than limiting the use of certain technologies, or mandating significant changes in platform/network architecture, the government should take a more rights-preserving and long-term view of the issue. This will enable a more holistic consideration of the interests involved, avoid unintended consequences, and limit the costs that come with excessive government interference in the technology space. The focus of the government must be on achieving optimal policy results, while reducing costs to the ecosystem as a whole (including privacy and security costs). A substantive mandate to limit the use of strong encryption would increase costs for the entire ecosystem, without commensurate benefits as far as state security is concerned.
• The tussle between LEAs and criminals has always been an arms race. Rather than adopting steps that may have significant negative effects on the digital ecosystem, the government could learn from the policies adopted by countries such as Germany, Israel and the USA. This would involve interventions along two axes – legal changes and measures to enhance state capacity.
• The legal changes that can be implemented, include:

- Reform of surveillance and decryption related processes to clarify the powers of LEAs, and ensure appropriate review and oversight. It is also essential to standardise and improve current methods of information access by LEAs at both domestic and international levels. There must be greater transparency in the entire surveillance and information access apparatus, including by casting obligations on intermediaries and the State to make relevant disclosures to the public.
- Adoption of a Vulnerabilities Equities Process, which could enable reasoned decisions to be made by the government about the disclosure of software/network vulnerabilities (thereby allowing these to be patched, in circumstances where this would not significantly affect security interests). Such a process is used today in the US, and while not without critics, does enable a better balancing of privacy, security and other interests.[xv]
- Amendment of telecom licenses, which currently give excessive leeway for exercise of executive authority, without sufficient safeguards.

• The government must also focus on enhancing its own capacities. This can include measures such as:

- Developing and enhancing covert hacking capacities (though these must be implemented only subject to appropriate oversight and review processes). To this end, there must be appropriate funding of LEAs, including by hiring security and technical researchers.
- Investing in academic and industry research into cryptography and allied areas. The government should also aid the development of domestic entities, which can participate in the global market for data security related products. Enhancing coordination between industry, academia, and the State is essential.
- Increasing participation in international standard setting and technical development processes.

References

[i] Unrecoverable encryption refers to encryption systems where only the participants in a communication have the ability to decrypt the message, i.e. the decryption key is available only with the individual concerned and not a third party such as an intermediary. Recoverable encryption on the other hand refers to the use of encryption, where a third party retains a decryption key and therefore has the ability to access the communications without the specific consent of the individuals concerned. J Lewis, D Zheng, W Carter, *The Effect of Encryption on Lawful Access to Communications and Data*, Centre for Strategic and International Studies (CSIS), February 2017, available at https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/encryption/csis_study_en.pdf

[ii] See Rule 3(5) of the proposed Intermediaries Guidelines (Amendment) Rules, 2018.

[iii] See for instance, *Anthony Clement Rubin v. Union of India,* 2019 SCC Online Mad 11785.

[iv] Press Information Bureau, *Rajya Sabha Committee calls for mandatory apps on all devices and filters to regulate children's access to pornography content,* Government of India, January 25, 2020, available at https://pib.gov.in/PressReleseDetail.aspx?PRID=1600505

[v] Harold Abelson et al., *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications,* MIT Computer Science and Artificial Intelligence Laboratory Technical Report, July 2015, available at http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf

[vi] *Id.*

[vii] D Gripman, *Electronic Document Certification: A Primer on the Technology Behind Digital Signatures,* 17 J. Marshall J. of Computer and Info. L. 769, 1999, available at https://repository.jmls.edu/jitpl/vol17/iss3/3/ (1999); ACLU and EFF, *Brief for Amicus Curiae The American Civil Liberties Union Foundation of Massachusetts, The American Civil Liberties Union Foundation, and the Electronic Frontier Foundation in Support of the Defendant-Appellee in Commonwealth of Massachussets v. Leon Gelfgatt,* Supreme Court of Massachussets, SJC 11358, 2015, available at https://www.aclum.org/sites/default/files/wp-content/uploads/2015/06/gelfgatt-brief_of_amici_curiae_ACLUM_ACLU_EFF.pdf.

[viii] N Richards, *Don't Let US Government Read Your Email,* CNN, August 2013, available at https://edition.cnn.com/2013/08/18/opinion/richards-lavabit-surveillance/index.html; W Hartzog and E Selinger, *Surveillance as Loss of Obscurity, Washington and Lee LR (3) 1343-1387, 2015; S Pell Jonesing for a Privacy Mandate, Getting a Technology Fix – Doctrine to Follow,* North Carolina Journal of Law and Tech., 489-555, 2013.

[ix] G Bhatia, *Privacy and the Criminal Process: Selvi v. State of Karnataka,* SSRN, April 2018, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3166849#:~:text=In%20Selvi%20v%20State%20of,and%20personal%20liberty%20under%20Article

[x] National Academy of Science, Engineering and Medicine, *Decrypting the Encryption Debate: A Framework for Decision Makers,* National Academies Press, 2018.

[xi] S Shantha, *Indian Activists, Lawyers, Were Targeted Using Israeli Spyware Pegasus,* The Wire, October 2019, available at https://thewire.in/tech/pegasus-spyware-bhima-koregaon-activists-warning-whatsapp; T Rajalakshmi, *The Pegasus Fiasco: Privacy in Peril,* Frontline, December 2019, available at https://frontline.thehindu.com/science-and technology/article30148934.ece#:~:text=Even%20this%20surveillance%20covers%20only,on%20his%20or%20her%20device.

[xii] V Mohan, *New E-Tools Being Developed to Trace Sources of Fake News,* The Tribune, May 2020, available at https://www.tribuneindia.com/news/sciencetechnology/new-e-tools-being-developed-to-trace-sources-of-fake-news-88886

[xiii] This has been the case, for example, with Huawei and ZTE, who have faced significant international pressure in view of the Chinese government's purported ability to access data flowing through their networks. S Dickinson, *China's New Cryptography Law: Still No Place to Hide,* HarrisBricken, November 2019, available at https://www.chinalawblog.com/2019/11/chinas-new-cryptography-law-still-no-place-to-hide.html; N Lindsey, *China's New Encryption Law Highlights Cryptography as a Strategic Priority,* CPO Magazine, November 2019, available at https://www.cpomagazine.com/data-protection/chinas-new-encryption-law-highlights-cryptography-as-a-strategic-priority/.

[xiv] For instance, Europol and Interpol have been increasingly concerned about the use of steganography and open source encryption solutions by international criminal groups. Therefore, even if there is a bar on using strong encryption, those who want to break this law, will continue to have ways available to them to do so. See R Callimachi, *How ISIS Built the Machinery of Terror Under Europe's Gaze,* The New York Times, March 2016, available at https://www.nytimes.com/2016/03/29/world/europe/isis-attacks-paris-brussels.html?_r=0; S Murphy, *Steganography: The New Intelligence Threat,* Marine Corps War College, Marine Corps University, 2004, available at https://bit.ly/3lQrgQF; Europol and Eurojust, *Second Report of the Observatory Function on Encryption,* January 2020, available at https://www.eurojust.europa.eu/second-report-observatory-function-encryption; Cabaj et. al, *The New Threats of Information Hiding: The Road Ahead,* 2018, available at https://arxiv.org/pdf/1801.00694.pdf.

[xv] Government of the US, *Vulnerabilities Equities Policy and Process for the United States Government,* 2017, available at https://www.eff.org/document/vulnerabilities-equities-process-january-2016; D Zhang, *Vulnerabilities Equities Process Revisited,* Georgetown Securities Studies Review, May 2019, available at https://georgetownsecuritystudiesreview.org/2019/05/28/vulnerabilities-equities-process-revisited/

Data Governance Network

The Data Governance Network is developing a multi-disciplinary community of researchers tackling India's next policy frontiers: data-enabled policymaking and the digital economy. At DGN, we work to cultivate and communicate research stemming from diverse viewpoints on market regulation, information privacy and digital rights. Our hope is to generate balanced and networked perspectives on data governance - thereby helping governments make smart policy choices which advance the empowerment and protection of individuals in today's data-rich environment.

About Us

The National Institute of Public Finance and Policy (NIPFP) is a centre for research in public economics and policies. Founded in 1976, the institute undertakes research, policy advocacy and capacity building in a number of areas, including technology policy. Our work in this space has involved providing research and policy support to government agencies and contributing to the creation and dissemination of public knowledge in this field. Our current topics of interest include privacy and surveillance reform; digital identity; Internet governance and rights, and regulation of emerging technologies. We also focus on research that lies at the intersection of technology policy, regulatory governance and competition policy.

About the Author

Rishab Bailey and Faiza Rahman are technology policy researchers at the National Institute of Public Finance and Policy (NIPFP), New Delhi. Vrinda Bhandari is a practising advocate.

Disclaimer and Terms of Use

IDFC Institute

301, 3rd Floor, Construction House 'A', 24th Road, Off Linking Road,
Khar West, Mumbai 400052

/idfcinstitute @idfcinstitute /IDFCInstitute