Data
Governance
Network
Anchored by IDFC Institute

February 2021

Working Paper 15

Backdoors to Encryption: Analysing an intermediary’s duty to provide “technical assistance”

Rishab Bailey, Vrinda Bhandari and Faiza Rahman

NIPFP

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.

Disclaimer and Terms of Use

The views and opinions expressed in this paper are those of the authors and do not necessarily represent those of the organisation.

Design

Cactus Communications

Suggested Citation:

Bailey, R., Bhandari, V. & Rahman, F., (2021). *Backdoors to Encryption: Analysing an intermediary’s duty to provide “technical assistance”* Data Governance Network Working Paper 15

Supported by a grant from Omidyar Network

Abstract

This paper examines recent proposals in India that seek to place obligations on intermediaries to provide "technical assistance" to LEAs, by either creating backdoors or weakening standards of encryption. While LEAs have genuine concerns arising from the use of certain types of encryption, implementing a general mandate for "technical assistance" can have significant effects on privacy of individuals and network security. Such a mandate may not pass a cost-benefit analysis, and more importantly may be against constitutional norms, being disproportionate. Rather than limiting the use of certain technologies or implementing significant changes in platform and network architecture, the Indian government should focus on implementing detailed, rights-respecting procedures for data access, developing hacking capabilities with sufficient oversight, encouraging research and development, and improving coordination with industry and academia.

Table of Contents

1. Introduction

Ensuring timely access to online communications and digital trails is seen as essential in allowing law enforcement agencies ("LEAs") to perform their security and policing functions. One of the main difficulties faced by LEAs relates to accessing hidden, masked or encrypted communications. The increased usability and popularity of strong encryption techniques, often by default, keeps content safe from virtually any "brute force" attacks. While not novel, this issue has risen to global prominence over the last four to five years, possibly due to the increased usage of privacy enhancing technologies across the digital ecosystem.[1]

The problem for LEAs arises in two contexts - the first relates to the inability to access encrypted data at rest, as was the case in the Apple-FBI standoff in 2016 (Kahney, 2019). The second is in conducting surveillance over (or monitoring) encrypted data that is in motion, or flowing between nodes on the internet, as in the case of services that utilise end-to-end encryption ("E2E").

A number of laws and mechanisms have been proposed in different jurisdictions to address these issues. There is, however, no uniform policy prescription that is seen as providing an adequate solution to what is often framed as a zero-sum game between privacy and security interests. Numerous suggestions have been proposed to deal with this issue. Invariably, these proposals boil down to the creation of backdoors in technology products (or the weakening of encryption standards) so as to enable "exceptional access" for LEAs.[2] However, as we discuss in this paper, these suggestions appear inadequate both from a civil liberties and a technical perspective.

The Indian government has also increasingly sought to regulate the use of encryption. This is notwithstanding the fact that Indian law currently limits the use of strong standards of encryption by certain intermediaries such as telecom service providers. Further, intermediaries can be required to assist in decrypting content, when they have the ability to do so, subject to certain procedures. Notably, the government released a draft National Encryption Policy in 2015, which sought to reduce standards of encryption used in the country. This was swiftly withdrawn after facing much criticism from industry and civil society. More recently, the issue has come up before courts in the case of *Anthony Clement Rubin v. Union of India (2019)*, where suggestions were made to create key escrow-based mechanisms to enable access to encrypted conversations on WhatsApp. The draft Information Technology (Intermediary Guidelines Amendment) Rules of 2018 also propose to expand the scope of assistance required to be provided by intermediaries to LEAs.[3] This has been viewed as a means to allow the government to demand the creation of backdoors or otherwise weaken encryption used by popular platforms (Bailey, Parsheera & Rahman, 2019). More recently, a parliamentary committee examining the issues of online

[1] This is likely to be prompted by the growing importance of the digital ecosystem, the rising privacy awareness across the world, as well as various regulatory developments such as the implementation of the General Data Protection Regulation in the EU and the California Consumer Privacy Act, 2018.

[2] A backdoor is a covert method of circumventing the encryption or authentication system on a computer or mobile phone, that takes place without the consent of the owner of the computer system. As Coldewey (2017) explains, a backdoor is often at odds with the stated purpose of the system and takes place under the control of undisclosed persons.

[3] The draft rules require intermediaries to provide "such information or assistance as asked for by any government agency or assistance concerning security of the state or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto". Intermediaries are also required to enable tracing the originator of information on their platforms "as may be required" by authorised government agencies.

child abuse related content, has also recommended the creation of exceptional access for LEAs to exercise their functions.

The paper is structured as follows. In *section 2*, we provide an introduction to the concept of encryption, a background to the encryption debate, and delineate the legal framework governing encryption and "technical assistance" in India. In *section 3*, we examine the scope of the duty of "technical assistance" that intermediaries are required to provide to LEAs. We analyse the problems caused to LEAs by the use of encryption, as well as the concerns that are likely to be caused by mandating enhanced "technical assistance" and creation of backdoors by intermediaries. We argue that any general mandate to weaken encryption and create backdoors will likely prove pointless, counterproductive, and violate constitutional norms. We also examine various alternatives that have been proposed - the use of key escrows and ghosting protocols - and conclude that these methods too, may prove unworkable given both constitutional and technical concerns. Consequently, we provide an interpretation for "technical assistance" for both recoverable and unrecoverable encryption that best addresses privacy and law enforcement concerns. Based on the range of problems that affect the ability of LEAs to access data, we argue that seeking to weaken encryption standards would merely provide a short-term solution and that too at a cost (for civil liberties and the digital ecosystem as a whole). Accordingly, the government would be well advised to take a more long-term perspective on the issue of LEA access to data. It should focus on enhancing its capacities, including by ensuring deeper linkages and coordination among LEAs, academia and industry. Putting in place rights respecting processes to formalise methods of data access, and investing in hacking capacities (with sufficient oversight and accountability) must be a priority. Further, creating an enabling environment for development of a local security products market, and investing in research and development of such technologies may provide a more practical way for the government to proceed.

2 Understanding encryption

In this section, we provide an overview of how encryption works and the different types of encryption that are commonly used in the digital ecosystem. We provide a background to the encryption debate, highlighting how the issue of "exceptional access" has been (re)litigated every few years since the early 1990s, but is yet to be satisfactorily resolved. The section concludes by providing an overview of the legal framework governing the use of encryption in India, and the methods LEAs can use to request access to encrypted communications.

2.1 Basics of encryption

Encryption is the process of using a mathematical algorithm to render plain, understandable text into unreadable letters and numbers. Encryption takes place through an encryption key, which is a piece of information that converts the message into an unreadable form. Typically, such unreadable text can only be decoded using a key. Decryption, refers to the process of using the key to transform the unreadable text text back to its original form (Gill, 2018). Depending on the manner of encryption, the same encryption key can be used to encrypt or decrypt information, whereas in other cases, the decryption key is different from the encryption key (EFF, 2018). Encryption thus ensures that the message can only be read by the person who has the key, since it is almost impossible to reverse the encryption. In this process, encryption improves information security.

Encryption secures information against unwarranted access and use through the art of cryptography. Cryptography is a broader field of art and science that involves designing secret codes to ensure confidentiality and secure communication. Cryptography, which means 'secret writing' in Greek, allows users to send and receive messages without third parties being able to understand them, and is also used to ensure user authentication and information integrity (i.e. that a message has not been tampered with during transit) (Krzyzanowski, 2004; Jaikaran, 2016).

Cryptography has been around for millennia as a tool to preserve the sanctity of communications. Julius Caesar wrote to Cicero using a substitution cipher.[4] Hamilton, Jefferson, and Madison also recognised the importance of cryptography in protecting personal and political information (ACLU and EFF, 2015). However, these ciphers embodied certain linguistic and structural properties, which meant that with proper tools and sufficient time, the 'key' could be determined through the "brute force" method (Luciano & Prichett, 1987, 1). For the purpose of this paper, we will be using the term encryption and decryption, rather than focussing on the broader field of cryptography.

Strong encryption systems help ensure the confidentiality of data, and thus foster trust in electronic systems, which form the bedrock of our current economic and information infrastructure. Encryption is thus useful for ordinary citizens to protect the privacy of their digital data and their anonymity. Businesses use encryption to secure their trade secrets and ensure that their dealings with suppliers and customers are genuine and authentic. Governments use encryption to protect national secrets from bad actors and cyber criminals (Jaikaran, 2016). Encryption works best when it is used by everyone and is automatic - if it were to be used only for information deemed important, it would automatically signal the value of the data. As Bruce Schneier (2015) explains, if only dissidents in a country were to use encryption, it would be easier for an autocratic government to identify them. However, when everyone uses encryption all the time, and when it is built into communication systems, it becomes difficult for the government to distinguish between the use of encryption in a regular private conversation and in a sensitive context.

Over time, methods of encryption have become easier to use and tougher to crack, thus improving their functionality as privacy preserving technology. However, as we shall discuss further on in this paper, the ubiquity and complexity of encryption systems have begun worrying governments and LEAs.

One way of thinking about encryption is using the analogy of a door and a lock. Just as putting a lock on a door does not prevent someone from breaking the lock and entering the house, encryption does not prevent LEAs from accessing information stored on a particular device. It only makes it harder for them to do so (Selinger, 2015). LEAs may try and break the encryption through the use of computational power.[5] They also have other methods to decode encrypted files, such as by deciphering passwords or other information used for securing data. This can be done through the use of cameras, keyloggers or exploiting software bugs in the encryption technology (ACLU and EFF, 2015). However, modern cryptographic tools use vastly sophisticated encryption algorithms in order to reduce the risk of brute force decryption, to increase the number of possible keys, and to ensure that the encrypted message does not reveal the linguistic and structural properties of the original plaintext message. This has made decryption more time intensive, difficult, and 'computationally demanding' for LEAs (Gill, 2018).

[4] The 'Caesar Cipher' "shifts the alphabet three places to the right and wraps the last three letters X, Y, Z back onto the first three letters" (EFF, 2018).

[5] This can be done for instance by attempting every possible key combination to decrypt a particular message. This method is commonly referred to as a brute force decryption.

2.2 Types of encryption

Encryption can be understood in a number of different ways, and applied at different times. Data can be encrypted in transit, when it is sent from one location to another; and at rest, when it is received and stored.[6]

A broad distinction can also be made between symmetric and asymmetric encryption. Symmetric encryption refers to cryptosystems where the encryption and decryption key is the same. Imagine a key where every alphabet is represented by a number. Thus, A = 1, B =2, C= 3 etc. If a person X has to send the message "Come here" to person Y, then she will use this key to encrypt the message as "313155 85185". Person Y can simply decrypt the message using this key. However, a third person, Z, may also be able to crack this encryption through brute force, by trying different combinations. This is an example of weak symmetric cryptography (EFF, 2018). AES, or Advanced Encryption Standard is a form of symmetric cryptography that is used in database or storage encryption for protecting data at rest (Townsend, 2019).

In contrast, in asymmetric encryption systems, or public key cryptography, the encrypting and decrypting keys are different, which makes for a stronger encryption system. Encryption, through a public key cryptography system, uses the idea of a public key (that is known or available with everyone) and a private key (that is only available to the specific individual). Thus, a stranger can encrypt a message using a public key, but only the intended recipient, who is the holder of the private key, will be able to decrypt and make sense of the message (Krzyzanowski, 2004). The reverse is also possible; namely, an individual X can encrypt using a private key, which can be decrypted by another individual Y, using a public key. The commonly used RSA encryption is a form of asymmetric encryption.

Lewis, Zheng and Carter (2017) distinguish between different types of encryption based on the ease of decrypting the information. "Recoverable encryption" involves the use of encryption products and services where third parties can access and decrypt the encrypted communication without the cooperation of either the sender or recipient of the message, or the owner of the device on which the encrypted data is stored. This is because even if the data is encrypted, the service provider has access to the private key implying that it can decrypt the information. Email encryption, using secure socket layer (SSL) or transport layer security (TLS) encryption is mostly recoverable.[7] This makes it easier to regain access to our email accounts using a forgot password feature. For instance, Gmail uses the TLS layer to automatically encrypt data in transit. However, this encryption is recoverable, which means that LEAs can decrypt the contents of our emails, with the assistance of the service provider (such as Google for Gmail accounts).[8]

[6] Encryption can also be applied at different layers of the internet, for instance, to an entire telecom service provider's data stream or to data streams from individual applications or individuals.

[7] There are now some e-mail services, such as ProtonMail, that provide end to end (or unrecoverable) encryption services, which means that if a user forgets their password, there is no way to recover the data linked with the account. On its website, ProtonMail states, *"ProtonMail's zero access architecture means that your data is encrypted in a way that makes it inaccessible to us. Data is encrypted on the client side using an encryption key that we do not have access to. This means we don't have the technical ability to decrypt your messages, and as a result, we are unable to hand your data over to third parties. With ProtonMail, privacy isn't just a promise, it is mathematically ensured. For this reason, we are also unable to do data recovery. If you forget your password, we cannot recover your data."* See ProtonMail, End-to-End Encryption, available at <https://protonmail.com/security-details>.

[8] For further information on the encryption practices followed by Google for Gmail, see Google, Email Encryption FAQs, <https://tinyurl.com/y6mcfrbr>

In contrast, "unrecoverable encryption" involves the use of cryptographic techniques that prevent any third party, including the service provider, from decrypting the contents of the encrypted communication, even if it wants to. Unrecoverable encryption is slowly gaining popularity, and is most commonly found in two places (Lewis et al., 2017). The first is E2E in instant messaging services such as WhatsApp and Signal, where the private key remains with the user on their device. Thus, if X sends a WhatsApp message to Y, the message is encrypted for Y on X's phone and can *only* be decrypted by Y on her phone. The intermediary, namely WhatsApp and hence, by extension, LEAs, have no power or ability to decrypt the message and become aware of its contents without the cooperation of the sender or recipient (Gill, 2018).[9]

The second form of unrecoverable encryption is full disk encryption, as deployed on the iPhone, where the data stored on the device is encrypted and can only be accessed by the user through a passcode/password. As is the case with E2E, service providers such as Apple cannot access the encrypted content on the mobile phone without access to the passcode/password. Hence, Apple cannot provide decrypted information to LEAs, even if required to by court order. Apple (2016) in its Legal Process Guidelines for law enforcement in the United States has clearly stated that *"for all devices running iOS 8.0 and later versions, Apple is unable to perform an iOS device data extraction as the data typically sought by law enforcement is encrypted, and Apple does not possess the encryption key."* In its FAQ section, Apple further states that it "does not have access to a user's passcode" and hence, cannot provide any individual or law enforcement with a passcode to an iOS device that is currently locked. It is thus clear that building a backdoor in a full disc encrypted service/product will fundamentally change the nature of the protection offered by unrecoverable encryption. Full disc encryption services that have a backdoor cannot be classified as truly unrecoverable encryption services anymore.

The categorisation of encryption products based on ease of access to the decrypted content is particularly relevant from a legal and policy perspective. Whether content can be decrypted by a third party (service provider) significantly changes the means available to LEAs to access data. Accordingly, this paper will adopt the terminology of recoverable and unrecoverable encryption.

2.3 Background to the encryption debate

The origins of the modern encryption debate can be traced to the 'crypto wars' of the 1990s, when the U.S. Communications Assistance for Law Enforcement Act, 1994, was being enacted. This period saw the government on one side and technology, privacy, and security researchers on the opposite side, with respect to proposals to build backdoors to communication systems or to reduce encryption standards (Finklea, 2016). This is best exemplified through the Clinton administration's push for a key escrow encryption system, known as the "Clipper Chip". As explained by a Clinton administration aide, the focus of the government was on developing strong cryptography that would protect people, but would also not undermine the ability of LEAs to their job. The government felt that it had three options. The first was to adopt relatively weak cryptography, which would make it easier for LEAs to monitor communications, but would not provide sufficiently high standards of security and privacy. The second option was to adopt very strong cryptography that would ensure privacy, but preclude LEAs from monitoring conversations. The third, and preferred option, was for the government to use the Clipper Chip, which involved the use of strong encryption systems, but with backdoors (Peterson, 2015). The Clipper Chip would be inserted into a communication device; it would copy the encryption key and send it to a secure escrow. Thus, a copy of the keys would be retained by a trusted third party, who would hand this over to an LEA upon proper legal authorisation, thereby enabling the LEAs to decode the encrypted

[9] To understand further how encryption works in group chats, see (Fisher, 2017; Shafi, 2018).

conversation. However, as security researchers found vulnerabilities in the system design, the proposal was eventually abandoned (Harold Abelson et al., 2015).

The debate arose again in 2014, when Apple and Google added full disk encryption to their mobile operating systems; and in 2016, when WhatsApp added default E2E on its messaging platform. Such built-in, unrecoverable encryption hastened the spread and ubiquity of encryption, and deepened the tensions between LEAs and privacy advocates and tech companies. This caught the public's attention in 2016 when Apple refused to create a backdoor to the iPhone of the San Bernardino shooter. The FBI sought a judicial order to compel Apple to create a "unique version of iOS that would bypass security provisions" on the iPhone lock screen, allowing the unlock passcodes to be entered electronically. Apple resisted this demand, stating that while it was technically possible to comply with the FBI's request and create an entirely new OS, there were three main problems. First, allowing passcodes to be entered electronically would make it easier to unlock the iPhone through brute force, by using modern computing power, thereby undermining the security and privacy of its users. Second, any judicial order would set a precedent for other LEAs to seek similar actions, thus expanding the government's powers. Finally, building a separate OS to be used exclusively by the government would be akin to a master key that could open millions of locks. This could easily be misused by bad actors (Apple, 2018).

Similar debates have taken, and continue to take place, in India as well. When terrorists were found to have used Blackberry devices in the course of the Mumbai terror attacks in 2008, the Indian government intensified its earlier demand for Research in Motion (RIM) to provide LEAs access to encrypted data, relocate its servers to India, and hand over encryption keys to the government. Despite the Indian government claiming that it had cracked the encryption used by RIM, the political tug of war eventually resulted in the company relocating its servers to India in 2010, and agreeing to hand over the plaintext of communications sent over its Blackberry messenger service to Indian LEAs (Agencies, 2010; Bharati, 2008).

In 2015, the Central Government circulated a draft National Encryption Policy for comments. The policy was controversial because it sought to impose various onerous obligations on companies and individuals alike. The policy required vendors of encryption products to register with the government and provide working copies of their hardware and software used for encryption. Similarly, companies or users in a B2B sector were required to store plain text of information that had been encrypted and hand it over to LEAs when necessary (Mohanty, 2019). Given the widespread backlash against the draft policy, the government swiftly withdrew it, clarifying that the policy was "just a draft and not a view of the government" (Sharma, 2015). No new national encryption policy has been proposed since, nor has India updated its cyber security policy since 2013 (though a new cyber security policy is due to be released shortly).

In the same vein, the government released the draft IT [Intermediaries Guidelines (Amendment) Rules], 2018 for public comments. These proposed amendments require intermediaries to, *inter alia*, enable "traceability" of users and provide LEAs with all information and assistance requested by them.[10]

[10] Under the controversial Rule 3(5) of the draft Intermediary Guidelines, 2018, the government has proposed to empower LEAs by requiring intermediaries to trace an 'originator of information' on their platforms. For the purpose of this paper, this requirement is how we understand 'traceability'. This change was introduced partly in response to security concerns, and partly in relation to fake WhatsApp forward messages leading to lynchings across India. The Draft was put forth in the public following a Parliamentary motion on "Misuse of social media platforms and spreading of fake news", which led to the government deciding to strengthen the legal framework to make social media platforms more accountable. (MeiTY, 2018).

Similarly, in February 2020, an ad-hoc committee of the Rajya Sabha led by Mr. Jairam Ramesh, concerned with the "alarming issue of pornography on social media and its effect on children and society as a whole", recommended that LEAs should be allowed to break E2E to trace distributors of child pornography and that applications that track children's access to pornographic material should be made mandatory on all devices sold in India (PIB, 2020).

The Indian government has also articulated its concerns regarding the use of encryption before various courts. In 2019, during a hearing in the Supreme Court, the Attorney General of India argued that social media companies such as WhatsApp and Facebook have a "responsibility" to share data with LEAs in cases involving threats to national security; and they cannot claim an inability to decrypt data (Reuters, 2019).

Most recently, the Indian government, along with Japan and the Five-Eyes Alliance (USA, UK, Australia, New Zealand, and Canada) issued a statement in October 2020, calling on companies to build backdoors to E2E platforms so as to facilitate access to LEAs. Interestingly, the statement selectively quotes from the US-EU Joint Statement of 2019, which while recognising that encryption was (mis)used by terrorists and could impede investigations, also recognised that "encryption is an important technical measure to ensure cybersecurity and the exercise of fundamental rights, including privacy, which requires that any access to encrypted data be via legal procedures that protect privacy and security." (Agrawal, 2020b) A draft resolution by the Council of the European Union has also acknowledged the problems posed by encrypted communications to LEAs, but reiterated support for strong encryption policies, noting that the increased adoption of E2E is a "positive reflection" (Agrawal, 2020a).

While the above mentioned developments are still mostly proposals or policy statements, they help provide a context within which the encryption debate is currently taking place in India. The only contrary signal has been sent by the Telecom Regulatory Authority of India (TRAI), which in its recommendations on regulation of Over-the-Top (OTT) Platforms, recognised the importance of encryption in maintaining privacy and security of data. Accordingly, TRAI has suggested that the government should avoid any regulation that requires changes in platform architecture, or would otherwise lead to vulnerabilities being introduced in communication systems (TRAI, 2020).

2.4 The law in India

A combination of laws, rules, and provisions in telecom licenses, require intermediaries to provide technical assistance and information to authorised government agencies/LEAs when called upon to do so. While the obligation to provide technical assistance is clear, the nature and extent of such assistance, and whether it can and/or should extend to enabling backdoors, especially in the context of information protected by unrecoverable encryption, is unclear. In this section, we detail the various provisions and rules under the Information Technology Act, 2000 ("IT Act") and telecom licenses that require intermediaries to provide such assistance to LEAs.

2.4.1 Electronic surveillance under Section 69 of the IT Act

Under the IT Act, intermediaries must facilitate the surveillance of individuals and enable the decryption of data. Under Section 69(1), the government can direct any LEA (such as the Central Bureau of Investigation or the Intelligence Bureau) to intercept, monitor, decrypt (collectively termed as "electronic surveillance") or cause the same to be carried out on various grounds specified in the provision.[11] Section 69(3) requires intermediaries to extend "all facilities and technical assistance" to provide or secure access to the relevant computer resource; intercept, monitor or decrypt such information; or provide information stored in a computer resource. Failure to do so, results in criminal sanction.[12]

The government notified the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (the "Surveillance Rules") to provide procedures and safeguards to facilitate electronic surveillance. Rule 13 imposes a specific obligation on intermediaries to provide "all facilities, cooperation and assistance" for electronic surveillance, as may be required by the government. Intermediaries must also provide "technical assistance and the equipment including hardware, software, firmware, storage, interface, and access to the equipment" wherever required by the authorised government agency.[13] Notably, such cooperation and assistance extends to permitting the intermediary to install software at the subscriber's end to enable electronic surveillance as well as to access and analyse information from a computer resource.[14] The intermediary is expected to retain the confidentiality of the intercepted, monitored, or decrypted information.[15] Importantly, Rule 8 makes it clear that LEAs are supposed to exercise these powers only in cases it is not possible to acquire the necessary information through alternative reasonable means.[16]

In respect of decryption, the Surveillance Rules provide that decryption key holders are required to disclose the decryption key or provide decryption assistance when called upon to do so. However, a request for decryption is limited to the extent the information is encrypted by the intermediary or "the intermediary has control over the decryption key." [17]

It is clear that under the Surveillance Rules, intermediaries are obliged to provide co-operation and technical assistance in fulfilling LEA requests for electronic surveillance to the extent they are capable of. The manner of such technical assistance, and how it plays out in cases of E2E services such as WhatsApp has been a subject of much debate in India recently, as seen in *Anthony Clement Rubin v. Union of India (2019)*. Courts may have to eventually decide whether "technical assistance" obliges an intermediary to create a backdoor or modify the platform architecture. Similar "technical assistance" obligations are placed on intermediaries in the context of collection and monitoring of metadata under Section 69B of the IT Act.[18]

[11] Section 69(1) of the IT Act, 2000 provides that the central or state government can direct interception/monitoring /decryption where necessary or expedient to do so in the interests of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign states, public order, prevent commission of a cognisable offence relating to the above, or for investigation of any offence.

[12] A failure to assist the relevant government agency in terms of the above may be punished with imprisonment for a term extending to 7 years and a fine.

[13] Rule 19, Surveillance Rules.

[14] Rule 24(2)(iii), (iv), and (vi), Surveillance Rules.

[15] Rule 25, Surveillance Rules.

[16] In addition, every intermediary is required to designate an officer to receive authorised directions from the designated government agencies. This designated officer must maintain records pertaining to the directions received, including the particulars of the person whose information is sought to be electronically surveilled; agencies to whom information is disclosed; and details of the intercepted, monitored, or decrypted information. See Rules 14-16, Surveillance Rules.

[17] Rules 17 and 13(3), Surveillance Rules.

[18] Section 69B of the IT Act read with the Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 deal with the power to authorise to monitor and collect traffic data or information through any computer resource for cyber security. Traffic data is defined in Section 69B(4)(ii) to mean *"any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, data, size, duration or type of underlying service or any other information."* It thus includes metadata.

In reaching their conclusion, courts in India may take some guidance from the Australian experience. Australia enacted the Telecommunications and Other Legislation Amendment (Assistance & Access) Act, 2018 (the "TOLA Act") that empowers LEAs to require technical assistance from "designated communications providers". Requests for "technical assistance" can be in the form of Technical Assistance Requests (TARs), Technical Assistance Notices (TANs), and Technical Capability Notices (TCNs), and can be employed as long as they do not create a "systemic weakness" or "systematic vulnerability".[19] In view of the significant criticism of the law, the Independent National Security Legislation Monitor issued a report in 2020, where they recommended that the power to exercise such exceptional powers should be shifted from the executive branch to an independent authority, the Administrative Appeals Tribunal, which could exercise judicial oversight (INSLM, 2019). The criticisms and concerns raised with the TOLA Act, as expressed for instance by Hardy (2020), Tillett (2019), Jjemba and Ben-Avie (2020), are a signpost for some of the concerns with the proposed Intermediary Guidelines Amendment Rules, 2018.[20]

2.4.2 Intermediary Guidelines under the IT Act

Under the IT Act, as part of their privilege of enjoying safe harbour status within India, certain "due diligence" obligations are placed on intermediaries. These require, among other things, for them to disable access to any unlawful content upon receiving a court order or a request from a government agency.[21] These obligations are further elaborated upon in the Information Technology (Intermediaries Guidelines) Rules, 2011 (the "Intermediaries Guidelines"). Per the Intermediary Guidelines, intermediaries must provide information "or any such assistance" to lawfully authorised government agencies, when required to do so by lawful order.[22] Any request from an LEA must must clearly state the purpose of seeking information or assistance from an intermediary, which is limited to information or assistance required for the purpose of verification of identity, or to prevent/detect/investigate /prosecute/punish, any cyber security incident or any other law in force.[23]

So far, the Intermediary Guidelines have mostly been used to take down access to unlawful content. However, in December 2018, the government circulated the IT (Intermediary Guidelines (Amendment) Rules), 2018 which imposed various new obligations on intermediaries. One of the most controversial provisions was the proposed amendment to Rule 3(5) which requires intermediaries to provide "such assistance or information as asked for by any government agency" within 72 hours of a request being made. Importantly, the proposed amendment also requires intermediaries to trace any "originator of information" on their platforms, as may be required by authorised government agencies. The proposed amendment is unclear about the scope of the traceability requirement, and whether it extends to

[19] TARs are voluntary requests to designated communication providers to voluntarily provide data or assistance in respect of criminal investigations or national security matters. TANs are similar to TARs, but they are in the nature of an 'order', and not a request. TANs are used where the provider already has technical means to provide access to law enforcement. TCNs, which are used in the most serious cases, are directions to implement a new capability in a product or service to intercept and decrypt communications that would otherwise be encrypted. See Sections 317A till 317ZT of the Telecommunications Act, 2017 as amended by TOLA

[20] The TOLA Act has been criticised for being anti-privacy, facilitating mission creep, and for lacking adequate date retention related safeguards. See also Krahulkova (2020).

[21] Section 79(2)(c) and 79(3)(b) of the IT Act, 2000 read with Rule 3 of the IT (Intermediary Guidelines) Rules, 2011. See also Shreya Singhal v Union of India, (2015) 5 SCC 1.

[22] Rule 3(7), Intermediary Guidelines. The agency must be authorised to deal with investigative, protective or cyber security activities.

[23] Further, intermediaries are also required to report cyber security incidents and share relevant information with the Indian Computer Emergency Response Team Refer Rule 3(9), Intermediaries Guidelines.

mandating a platform architecture change or creating a backdoor. The information or assistance sought by the government must relate to a matter concerning security of the state, cyber security, investigation, detection, prosecution, prevention of an offence, protective or cyber security or other connected matters.[24]

Rule 3(9) of the proposed amended rules requires intermediaries to deploy "technology based automated tools or appropriate mechanisms, with appropriate controls" to proactively identify and remove or disable access to unlawful content. As with the current rules, intermediaries are also required to report cyber security incidents and share information related to such incidents with the Indian Computer Emergency Response Team.[25]

These provisions (together with various other changes proposed in the draft guidelines) have come in for a significant amount of criticism by various stakeholders. This has primarily been on the grounds that the proposed changes may adversely affect fundamental rights of individuals by incentivising over-censorship by intermediaries.

This may lead to a chilling effect on expression rights (Arun, 2019). The traceability requirement has also been criticised for being vague, overly restrictive, and circumventing procedural safeguards (Bailey et al., 2019).

2.4.3 Telecom Licenses

Telecom service providers and internet service providers (jointly referred to as "TSPs") are required to execute a contract, the Unified Access Services License ("UASL") with the Department of Telecommunications of the Government of India (the "DoT"). The UASL provides fairly wide-ranging conditions pertaining to the technical and other facilities and assistance required to be provided by the licensee to the government/LEAs.[26] TSPs are required to implement mechanisms and provide adequate means to enable monitoring and interception of communications as may be required by the government.[27] They must also ensure that they make necessary provisions, in terms of hardware and software, to enable lawful interception from a centralised location.[28] Licensees must also install suitable monitoring equipment, based on the requirements of the government or designated security agencies.[29]

The licensee is obliged to provide, without any delay, facilities to enable tracing of "nuisance, obnoxious, or malicious" communications flowing through its network, where required for investigations, detection of crime or in the interests of national security.[30] Licensees must also make available access to their entire networks including equipment installed in subscriber premises, for technical scrutiny and inspection.[31] The government also reserves the right to "evaluate" any encryption equipment used in

[24] A request can be made in writing or through electronic means, but it must state the purpose of seeking such information or assistance.

[25] Rule 3(10), Intermediary Guidelines, 2011

[26] The UASL itself consists of multiple parts. Part I contains general conditions applicable to all service providers. Part II contains different conditions based on the type of service being provided. The entire UASL is available at <https://tinyurl.com/y35r5p43>.

[27] Refer Clauses 23.2, 40.2, Chapter I, UASL

[28] Clause 39.23(xvi), Chapter I, UASL.

[29] Clause 39.12, Chapter I, UASL.

[30] Refer Clause 38.2, Chapter I, UASL.

[31] Clause 39.2, Chapter I, UASL

the licensees network.[32] While the licensee is solely responsible for ensuring the privacy of communications and security of their network, they are barred from using “bulk encryption.”[33] Interestingly, Clause 39.11(ii) provides for fines to be levied on the licensee in case any vulnerability is deliberately created in the telecom equipment used.

The UASL confers excessively broad powers to the Government and curiously have not been subject to much scrutiny or discussion. We believe that the terms of the UASL should be amended to narrow the scope of powers exercised by the government over TSPs.

2.4.4 Section 91, Code of Criminal Procedure

In addition to the laws under the IT Act, LEAs can also rely on pre-digital era procedural powers under Section 91 of the Code of Criminal Procedure, 1973 to ask companies to produce a “document or other thing” for the purpose of investigation, inquiry, or trial. In practice, LEAs use this provision to seek the production of data, such as metadata, stored data or data at rest (including emails sent and received), communication data, and other forms of electronic evidence that may be in the possession of intermediaries (Abraham & Hickok, 2012; Krishnakumar, 2019). Before the Madras High Court, WhatsApp stated that in response to Section 91 requests, it would provide *“Basic Subscriber Information (BSI) includes phone number, name, device info, App version, Start date/time, connection status, last connection date/time/IP, E-mail address, Web client data.”* (Anthony Clement Rubin v. Union of India, 2019).

From the above, it is clear that Indian laws vests broads powers with the government and LEAs to seek assistance from intermediaries in carrying out their functions. This may range from providing detailed information on users, to enabling surveillance over them or requiring intermediaries to decrypt data, where practical.

Having studied the historic and legal genesis of the debate around encryption, the next section will examine the main arguments raised for and against requiring intermediaries to create backdoors to facilitate decryption. This will help assess the scope of the obligation of ‘technical assistance’ on intermediaries, both in relation to recoverable and unrecoverable encryption.

3 Analysing the scope of ‘technical assistance’

This section of the paper examines the arguments advanced by LEAs, civil society, academia, and the cyber security community for and against the legal restriction of encryption. Based on an analysis of these arguments, we try and determine the scope of the duty of technical assistance imposed on intermediaries with respect to recoverable and unrecoverable encryption deployed on their platforms. We argue that the government should not implement a mandate for intermediaries to weaken encryption by building backdoors into products/services. We therefore examine what could be the possible way forward. What steps can the government take to ensure that it is able to carry out its

[32] Service providers must adhere to the IT Act and regulations thereunder insofar as encryption is concerned. Refer Clauses 37, 37.5, Chapter I, UASL.

[33] Clause 37.1, UASL. Bulk encryption has not been defined in the UASL, but likely refers to encrypting a large number of units at the same time / implementing encryption on the entire data stream of the TSP. Note also that TRAI has suggested that the Department of Telecommunications re-examine the encryption standards in TSP licenses (TRAI, 2018).

security functions, while at the same time respecting civil liberties and not hampering development of the digital ecosystem?

3.1 Should the government restrict the use of strong encryption?

As described previously, calls for limiting the deployment of strong encryption by intermediaries have largely been based on the need for LEAs to have access to information necessary for pursuing their law enforcement duties. LEAs point to the need to ensure accountability for online harms, and therefore argue that intermediaries must provide them with all data relevant to an investigation. This demand is complicated by the deployment of virtually uncrackable encryption systems by intermediaries. This section of the paper unpacks these arguments.

3.1.1 The problems posed by unrecoverable encryption to law enforcement

The choice of encryption system by an intermediary has direct consequences for the ability of LEAs to access and read information required for the performance of their functions. It is no surprise then, that demands by LEAs to restrict encryption have been around since 1997, when the FBI Director Freeh (1997) deposed before the Senate Judiciary Committee that

> "Law enforcement is in unanimous agreement that the widespread use of robust non-key recovery encryption ultimately will devastate our ability to fight crime and prevent terrorism. Uncrackable encryption will allow drug lords, spies, terrorists and even violent gangs to communicate about their crimes and their conspiracies with impunity. We will lose one of the few remaining vulnerabilities of the worst criminals and terrorists upon which law enforcement depends to successfully investigate and often prevent the worst crimes."

The FBI suggested a key recovery encryption, or the Clipper Chip, as a "balanced" solution to the problem, where a decryption key for a particular encryption product would be deposited with a "trustworthy key recovery agent for safekeeping" (Freeh, 1997).

The demands of LEAs have not changed much since then. In 2014, the FBI Director, James Comey observed that while they had legal authority to access and intercept conversations, they often lacked the technical ability to do so. In the context of the rise of default encryption settings on platforms and encrypted devices and networks, Comey voiced his fears about criminals and terrorists "going dark" and how with "sophisticated encryption, there might be no solution, leaving the government at a dead end—all in the name of privacy and network security" (Comey, 2014). As elaborated in the previous section, similar debates have been taking place across India as well.

What explains this LEA opposition to new methods of encrypted communication?

First, the growing popularity of stronger encryption architecture, manifesting itself in an increase in the number of E2E messaging services with perfect forward secrecy. It is estimated that 22% of global communication traffic today utilises end-to-end encryption, putting it out of reach for LEAs. A major part of this traffic is processed through WhatsApp, Viber, and Facebook Messenger (where E2E is not the default setting and is only available for one-to-one messaging) (Lewis et al., 2017). Historically, ciphers could easily be uncoded through a brute force attack. Encryption systems have made such advancements in improving the security of platforms, by increasing the number of possible key combinations, that it is almost computationally impossible to guess them. Current Advanced Encryption Systems ("AES") have key lengths of 128, 192, and 256 bits. A brute force attack would require testing all possible key combinations to identify the private key, which means that the use of AES in device software has virtually eliminated the possibility of a brute force attack of data at rest.[34] Perfect forward secrecy further complicates the issue, since the encryption system automatically and periodically changes the keys that are used to encrypt and decrypt communication. This means that even if LEAs are able to access/decrypt the latest key, it will only provide them with a small snippet of the user's communications (Greenberg, 2018).

Second, companies have begun installing features to authenticate encryption to ensure that users are who they claim they are. To avoid intruders taking over a person's phone and to maintain the integrity of communication, companies have begun introducing features such as forced time delays between passcode attempts; and auto-erase, in case of a specified number of failed passcode attempts (Lewis et al., 2017). In fact, the genesis of the Apple-FBI dispute in 2016 lay in the fact that the FBI could not attempt a brute force attack (even assuming there was a chance of success) since the content on the iPhone would be deleted after 10 incorrect passcode attempts. In response to requests by LEAs for creating backdoors to provide assistance to unlock the iPhone (Brewster, 2020), Apple has clarified that *"..there is no such thing as a backdoor just for the good guys"* since backdoors can be exploited by bad actors who threaten national security as well as the data security of its customers (Wong, 2020). Apple claims that while it complies with LEA requests to turn over data stored on its cloud server, iCloud, it does not have access to the data stored on a locked and encrypted iPhone.

Third, the content of communication is secured not only through stronger encryption, but also through data minimisation practices such as transient content (Lewis et al., 2017). Various intermediary platforms such as Telegram, Signal, WhatsApp, Snapchat, and Wickr provide the option for disappearing messages, where the message gets automatically deleted after a pre-set time. Other data minimisation practices followed by Signal include having no data back ups and storing encryption keys in different jurisdictions, making it more difficult for LEAs to decrypt the content (Doffman, 2020). Kik, a messaging platform popular with teenagers (and therefore, child sexual predators) does not store, and cannot access, the phone number associated with the device (Department of Homeland Security, 2015). An increase in the use of these technologies has led to the Rajya Sabha Ad Hoc Committee in India recommending "permitting breaking of end to end encryption", at least within the limited context of child sexual abuse content (PIB, 2020).

Fourth, companies provide a combination of these features – E2E, robust authentication, and ephemeral messaging – by default, without the users having to opt-in; thereby increasing the uptake of these features. It is thus not surprising that LEAs across the world have asked companies such as Facebook to create backdoors in their product designs, so as to enable access to communications of suspects (Alford, 2020).

While these concerns are legitimate, the government's favoured solutions of creating a backdoor or mandating traceability can have a significant impact on civil liberties and data security. The key concerns in this respect are detailed below.

[34] The number of key combinations for AES is so large, that there is near consensus on the virtual impossibility of even supercomputers being able to break the code. For instance, while a 56 bit key size has 7.2 x 1016 combinations, a 256 bit AES has 1.1 x 1077 combinations. While the 56 bit key can be cracked in 399 s, the 256 bit key will take 3.31 x 1056 years to crack by brute force (Haunts, 2019).

3.1.2 Problems with mandating backdoors

In this part of the paper, we highlight the three main concerns that stem from mandating the lowering of encryption standards deployed by online services or requiring intermediaries to create backdoors to enable exceptional access for LEAs. Specifically, we examine privacy, security and other constitutional concerns emerging in this context.

Privacy concerns

There are a variety of privacy related concerns that arise from mandating decryption or backdoors in order to enable easier surveillance. Primary amongst these is intellectual privacy, which is the ability to use the protection of law or social circumstances to read, engage, develop ideas and beliefs, *"away from the unwanted gaze or interference of others"* (Richards, 2015). Security of communication or the trust that one's private communication is secure from interference by third parties is critical for intellectual privacy of individuals to flourish, and encryption imparts the requisite safeguards by protecting our thoughts, until we are ready to enter the public debate (Selinger, 2015).

Private thoughts, expressed in confidence over email or chat applications are an *extension* of one's identity, and therefore deserve protection from unwarranted government access. The argument that only criminals have "something to hide" and hence, there is no threat to privacy through the government's surveillance fails to take into account a pluralistic conception of privacy. This argument limits the understanding of privacy to merely secrecy, or understands that its only purpose can be to hide bad things (Solove, 2007).

This idea can also be viewed from a sociological perspective. As Goffman (1959) explains, our individual identities are *constructs* that are a product of our social interactions and that we display in front of others. Identities are not innate and are chosen based on our 'definition of the situation' (van den Berg, 2010). Goffman (1959) uses a theatre analogy to advance his argument. As part of our social interactions, we assume specific roles and conduct performances for the 'audience' present – this is our performance at the front of the stage, and our 'public behaviour'. However, backstage, when no one is watching and we have privacy, it allows us to relax and let our masks down – this is our 'private behaviour'.

Goffman's analogy can be extended to the current encryption debate. For instance, our private backstage behaviour allows us to remain anonymous, away from the audience. Traceability or decryption, however, removes this mask of anonymity and dissolves the distinction between frontstage and backstage. Knowing that the government may require an intermediary to track the originator of content, will encourage putting back on a mask, and moderating our ideas and expressions. Essentially, an absence of privacy can force unwanted behavioural change, which could be seen as a violation of Articles 14, 19 and 21 of the Constitution.

These privacy and surveillance concerns emanating from the threat of mandating backdoors are only heightened when one closely examines the Indian government's simultaneous move to enact laws that restrict companies from transferring certain types of personal data outside India.[35] Mandatory storage

[35] The government is in the process of enacting the Personal Data Protection Bill, 2019 which requires companies to store a copy of sensitive personal data (which includes financial data, health data, sexual orientation data, biometric data, etc.) in India. In addition, the draft law proposes that a second undefined sub-category known as "critical personal data", can only be stored in India. See Clause 33, Personal Data Protection Bill, 2019. For a detailed proportionality analysis of the provisions seeking to restrict cross-border transfer of certain types of data see (Bailey, Bhandari, Parsheera & Rahman, 2020)

(or mirroring) of personal data within the territory of India coupled with a legal requirement for companies to create backdoors or remove encryption could give rise to significant privacy and surveillance concerns for Indian citizens. It will "chill" public and private expression of individuals over the Internet and ensure that the Indian government has unprecedented access to personal data of citizens.

Security concerns

Encryption is critical for ensuring the security of an individual's data against intrusion from States and private actors. It is primarily used as a security tool to preserve message confidentiality (by ensuring that the message is only read by the intended recipient), to authenticate the identity of the sender (so that no one can mask their identity), and to maintain the integrity of the message (by ensuring that it is not altered in transit) (Gill, 2018). There is therefore an implicit understanding amongst government officials, security and policy experts and intermediaries that encryption improves the security of the data stored. For instance, Article 32 of the GDPR expressly recognises encryption as an appropriate technical and organisational measure to ensure the secure processing of personal data. Clause 24 of the PDP Bill also references encryption as an adequate security safeguard measure. Similarly, the data protection law in Massachusetts in the U.S. requires each business to implement a written information security program to encrypt, where technically feasible, all files containing personal information stored on laptop, and which are transmitted across public networks or WiFi.[36]

As Apple's position referenced previously indicates, there is widespread apprehension that creating a backdoor to an encrypted service will create a weakness and vulnerability in the entire system, which can then be exploited by bad actors. In fact, the FBI Director, James Comey has tried to correct this 'misconception' by stating that they were not seeking any backdoor – they wanted to use the front door, through the legal process, to gain access to information. Security concerns in such a scenario could be mitigated by *"developing intercept solutions during the design phase, rather than resorting to a patchwork solution when law enforcement comes knocking after the fact"* (Comey, 2014).

However, the debate around backdoors should not be simply seen as a balancing act between national security and privacy. It is also a debate around security versus security, namely the national security interests being balanced against cyber security concerns. In its influential 2015 "Keys Under Doormats" report, some of the top cryptographers of the world explained that providing LEAs with exceptional access to private communications would force a U-turn from the prevalent best practices of the industry that have, in general, made the internet more secure, since it would "open doors through which criminals and malicious nation-states can attack the very individuals law enforcement seeks to defend" (Harold Abelson et al., 2015). This is because providing for exceptional access within devices would result in increasing system complexity, which can result in unanticipated vulnerabilities in the way in which this feature would interact with other features (Harold Abelson et al., 2015).

Over the years, LEAs across the world have come up with alternate approaches, which they claim do not undermine unrecoverable encryption, while simultaneously ensuring a safe online environment. For instance, as mentioned earlier, the FBI has previously suggested the adoption of key escrow arrangements wherein a decryption key would be deposited for a particular encryption product, with a

[36] 201 C.M.R. 17: Standards for the Protection of Personal Information of Residents of the Commonwealth (the "Massachusetts Standards" Similarly, Article 32 of the European Union General Data Protection Regulation mentions the use of encryption as a measure to secure data(Union, 2016).

"trustworthy key recovery agent for safekeeping" (Freeh, 1997). A related suggestion was put forth before the Madras High Court in *Anthony Clement Rubin v Union of India* (2019) which suggested circumvention of encryption by (i) tagging individual messages with the originators identification details; and (ii) encrypting the originator's identification information in the metadata of the message, which can be decrypted only by the intermediary concerned (Kamakoti, 2019). Other technical experts, however, have argued that such a suggestion is untenable and is not supported by protocol design (Venkatanarayanan, 2019).

Key escrows have also drawn significant skepticism from the security community, because they have substantial vulnerabilities.[37] As an example, key escrows require us to repose faith in the integrity of the private or government entity holding the decryption keys in trust. Besides, such key databases would inherently be under a high risk of being attacked, constituting a single-point-of-failure, (Kayel, 2015) and deployment of complex key recovery infrastructures will impose huge costs as well (Abelson et al, 1997).

Another proposal towards exceptional access for LEAs has been the adoption of a technique known as "ghosting", where a service provider can be required to secretly add a law enforcement participant to a private chat or call. In 2018, UK's Government Communications Headquarters (GCHQ) proposed the usage of "ghost protocols" to enable targeted exceptional access for LEAs as an alternative to breaking or lowering strong encryption levels (Levy & Robinson, 2018a). This method does not do away with E2E but adds an extra 'end' to any communication. In practice, this would mean that WhatsApp, upon receiving a lawful order, would be required to convert a private conversation between two individuals into a group chat, with a law enforcement member as a *hidden,* third participant.[38] Critics argue, that this is just another form of creating a backdoor. Deployment will fundamentally erode trust between consumers and service providers and provide for a "dormant wiretap in every user's pocket" that can be activated at request. This would detract from the proportionality approach, which only permits exceptional and targeted access to information (Cardozo, 2019). Accommodating "ghosts" would also require fundamental changes in system architecture, thereby introducing unintentional vulnerabilities that create security threats for *all* users (Access Now et al., 2019). Despite these concerns related to erosion of consumer trust, privacy and security, "ghost protocols" do not do away with E2E as such and may, to that limited extent, be slightly less problematic when compared to legally mandating the weakening of encryption on a systemic scale.

Other Constitutional concerns

Some have argued that the act of decryption amounts to a compelled testimonial act that is protected by the right against self-incrimination (EFF, 2011). It is therefore argued that forcing an individual to decrypt or hand over an unencrypted device may violate the constitutional right against self-incrimination. This is because decryption requires transforming scrambled data into readable data, and compelling someone to decrypt data involves them having to explain the data (Gripman, 1999). In the process, a "new, intelligible version" of the data is created. ACLU and EFF (2015) highlight

[37] While key escrow arrangement have broadly been critiqued by security experts, some researchers have recently favoured the implementation of key escrow arrangements wherein the key physically resides on the mobile phone device over arrangements where decryption keys are stored in a centralised repository (Carnegie Institute, 2019).

[38] Notably, discrete addition of a new 'end' or participant is more feasible in WhatsApp and iMessage where group members can be added by the server, albeit through substantial changes in platform architecture, without the help of an existent chat participant. Signal and some other online services already require the cooperation of at least one chat participant to add new group members. For further details see (Green, 2018)

the testimonial aspect of decryption through an analogy - being compelled to decrypt a computer is similar to being forced to create, for the benefit of someone standing on the steps of a library, an English translations for every single library book written in Braille. This act would not only reveal the person's knowledge and ability to translate, but also, in the process, create an entirely new work by revealing the contents of all the books in the library's Braille collection.

The government's primary concern with encryption is that it hinders efficient law enforcement, by impeding the discovery of key information. However, surveillance or even investigation is not meant to be a frictionless process. As Richards (2013) points out, *introducing inefficiencies in the functioning of LEAs is what separates a police state from a democracy.* All our substantive and procedural due process requirements embedded within criminal law are intended to curb the expansion of police powers and protect civil liberties (Hartzog & Selinger, 2015). Encryption serves a similar process in our current digital age, by increasing the transaction costs so as to force the government to prioritise certain investigations over others and restraining them from conducting mass surveillance (Pell, 2013).

A similar argument has been made in the Indian context. Bhatia (2018), points to how the Supreme Court's decision in *Selvi v. State of Karnataka* (2010),[39] indicates a departure from a "crime control model" to a "due process" model - implying a shift from a philosophy which "views the accurate solving of crime to be the highest goal of the law" to one where "even for the detection of crime, there are lines that the State cannot cross – lines grounded in the belief that certain individual rights are inviolable." This argument could be extended to the issue of backdoors, given the broad effects on the digital ecosystem as well as the significant intrusion into privacy rights of society at large.

3.1.3 Encryption restrictions through the lens of Puttaswamy standards

The Indian Supreme Court in *Justice KS Puttaswamy (Retd.) v. Union of India* (2017) affirmed the fundamental right to privacy as flowing from the rights guaranteed under Part III of the Indian Constitution. The Court held that the validity of any restrictions imposed by the State on the right to privacy have to be tested using the proportionality standard. This entails satisfying tests of legality, legitimate aim, proportionality and procedural safeguards (Bhandari, Kak, Parsheera & Rahman, 2017). In the Aadhaar judgment, *Justice KS Puttaswamy (Retd.) v. Union of India (2019)*, the Supreme Court built upon this foundational framework and formulated the different tests that would form a part of the proportionality analysis (Bhandari & Lahiri, 2020; Parsheera & Bailey, 2018b). Accordingly, any restriction into the right to privacy has to satisfy the following tests:

- Legality: Does the restriction flow from a law?
- Legitimate aim: Does the restriction pursue a legitimate State aim?
- Suitability: Do the means adopted by the restriction have a rational nexus to the objective sought to be achieved by it?
- Necessity test: What alternatives can be identified and are these as effective as the chosen restriction in achieving the stated end? Is there a less intrusive way of achieving the same end?
- Proportionality: Is the interference into privacy rights proportionate to the need for such interference, and does it have sufficient procedural guarantees?

Targeted decryption, as well as mandating the creation of backdoors, will likely satisfy the legality and legitimate aim prongs of the *Puttaswamy* tests, if done through an appropriate legislative amendment aimed at ensuring security of the state. However, depending on the intensity of the review adopted by

[39] In this case, the court barred the use of 'evidence' procured through the use of narco, brain mapping or polygraph tests on individuals.

courts such moves may not pass the suitability test. While a low standard of review may lead a court to conclude that mandating backdoors may enhance the general objective of national security to a certain degree,[40] a higher standard of judicial scrutiny may require courts to assess if creation of backdoors will further the aim of national security to a *substantial level*. Such heightened scrutiny will then require courts to evaluate counterfactual impacts of the measure i.e., the lowering of overall cyber security and privacy of all individuals.

Further, when it comes to the 'least restrictive' measure test, we believe that ordering decryption of a specific communication, when based on evidence of suspicion, may qualify as a 'least restrictive' measure. The fact that access is targeted towards a specific transaction, where there is adequate evidence to indicate an illegal offence may satisfy the proportionality assessment, as long as there are sufficient procedural safeguards such as a requirement for judicial oversight. Requiring the creation of backdoors within all computer systems would not satisfy the necessity and proportionality prongs, given that this would compromise the privacy and security of all individuals at all times, by rendering their computer resources vulnerable, and despite the absence of any evidence of illegal activity. Given that LEAs already have other less intrusive alternatives such as legally accessing unencrypted stored data and metadata, etc., the mandate to create backdoors will not qualify as a least restrictive measure. Some alternate avenues available to LEAs for accessing data for purposes of investigation are detailed further on in the paper.

3.2 Scope of duty to provide technical assistance: What does it mean?

As discussed earlier, intermediaries are obliged to provide 'technical assistance' to LEAs under Indian law, although the scope of such assistance is unclear. In this section, we unpack the meaning of 'technical assistance' in the context of recoverable and unrecoverable encryption and conclude that the term should not be interpreted to include creating a backdoor to the encrypted service.

3.2.1 Recoverable encryption

Indian law currently requires intermediaries to provide assistance to LEAs to decrypt information if it is necessary or expedient to do so in the interest of sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence.[41] Unlike E2E, recoverable encryption deals with cases where the intermediaries have the technical ability to decrypt communications, if called upon to do so. These are not cases, therefore, where LEAs have any basis to demand the creation of backdoors in encryption products and services.

However, the current statutory framework surrounding technical assistance by intermediaries is problematic, and is in fact, under challenge before the Supreme Court.[42] The Indian statutory regime continues to be an outlier among constitutional democracies (Bhandari & Lahiri, 2020). The IT Act does not envisage any judicial oversight over the actions of the LEAs, nor does it require LEAs to apply a proportionality test before requesting for decryption from intermediaries, as required by the

[40] See discussion around intensity of suitability review in Chandra (2020) and Pirker (2013). For a detailed analysis of variable intensity of review adopted during the different stages of proportionality analysis by courts across jurisdictions see Rivers (2006).

[41] See Sections 69(1) and 69(3) of the Information Technology Act, 2000

[42] *Internet Freedom Foundation v Union of India*, W.P. (C) No. 44/2019.

Puttaswamy verdicts. As the Justice Srikrishna Committee (2018) noted, after comparing the law in UK (where judicial oversight exists), Germany (where parliamentary oversight exists), and South Africa (which has a combination of parliamentary and judicial oversight over surveillance action), *"executive review alone is not in tandem with comparative models in democratic nations which either provide for legislative oversight, judicial approval or both".* Officials within the GCHQ have also publicly commented on the importance of ensuring independent judicial oversight over actions of law enforcement, and the importance of factoring in the principles of necessity and proportionality in such decisions (Levy & Robinson, 2018b). Even the Independent National Security Legislation Monitor report in Australia recommended judicial oversight for the three tiers of 'technical assistance' in Australia (INSLM, 2019).

The Surveillance Rules notified under Section 69 of the IT Act set in place a process by which decryption requests by LEAs are authorised by the Home Secretary in the Central and State Governments, and the review of the authorisation orders is done by a Review Committee, consisting of members of the executive. Consequently an order of decryption can be obtained very easily by LEAs. Given that every instance of ordering decryption will lead to identification of users and disclosure of private information, it will involve a careful balancing of a number of rights and interests. For instance, such a decision will invariably involve the right to privacy and the right to free speech on one hand, and may also involve a countervailing right of the victim (such as the right of privacy or right to life of the person against whom the offence has been committed) as well the right of the state to investigate a particular offence. In Bailey, Bhandari, Parsheera and Rahman (2018), we argue that these determinations being discretionary in nature, require application of mind to the specific circumstances of each case. Such determinations are transaction-intensive in nature also in terms of the volume of requests made by LEAs. A purely executive oversight process is opaque and non-adversarial. In contrast, judicial proceedings are usually transparent and require judges to enunciate reasons for their decisions, even in the absence of adversarial proceedings. Importantly, decision making in such cases is by a trained, independent entity.

We therefore believe that courts are best placed to engage in the complex balancing exercise that calibrates the right to expression and privacy with other interests. Section 69(1) of the IT Act should therefore be amended to ensure that decryption orders are subject to prior judicial review and that law enforcement or intelligence agencies, or other government officials are not directly authorised to seek decryption of computer resources from intermediaries. Further, the order for decryption should be open to appeal (Bailey et al., 2018).

In addition, there is a need to implement a clear procedural framework that outlines various factors/requirements that ought to be considered before an order of decryption is issued to an intermediary. While the current Surveillance Rules do require the competent authority to consider whether alternative means have been exhausted prior to ordering decryption or surveillance, the process is both opaque and lacks appropriate fetters on executive discretion. The law should contain clear requirements to ensure the necessity and proportionality of any interventions. Reasons must be recorded, and must be subject to review. Further, appropriate time should be given to the intermediary to decrypt the information to ensure that disproportionate costs are not imposed (subject to emergency requests); and wherever possible, the user should be allowed to object to a disclosure request.[43] If prior notice is not feasible due to the nature of the case, the courts should consider providing the individual with a post-facto notification of decryption (Bailey et al., 2018).

[43] Implying that notice should be given to the relevant user whose information is sought to be decrypted. A similar requirement is set out under Section 11 of the Right to Information Act, 2000 which mandates that the party whose information is being disclosed is given notice and an opportunity to object.

3.2.2 Unrecoverable encryption

By definition, unrecoverable encryption covers those cases of encryption where it is not possible for intermediaries to access user data in response to a government request. LEAs are not necessarily demanding that companies stop using encryption altogether; rather their preference is for the use of recoverable encryption that will allow intermediaries to decrypt information when required. In deciding whether intermediaries, as part of their duty of technical assistance, should be required to ensure backdoors, and thus, effectively end unrecoverable encryption (and E2E), various considerations need to be taken into account.

First, even with the use of unrecoverable encryption, law enforcement is not out of options. LEAs can still continue to access unencrypted stored data as well as metadata (National Academies of Sciences, Engineering, and Medicine, 2018). For instance, while E2E services such as WhatsApp do not ordinarily store contents or transaction logs of delivered messages, they do retain metadata and other information about users, including account information, device information, usage and log information, transactional information, status information, connections, and cookies.[44] The retained data includes device-specific information such as hardware model, operating system information, browser information, IP address, mobile network information, device identifiers, and device location information (in some cases) (WhatsApp, 2019). All this information can be shared with law enforcement, if required.[45]

Access to metadata gives LEAs detailed information about a particular user or transaction, which can be significant for investigative purposes.[46] Additionally, various digital forensic tools are already being deployed by LEAs in India for instance in the context of tracking sources of misinformation and fake news (Mohan, 2020). Investigations relying on metadata and the use of advanced data analytics can reveal patterns of behaviour and conversations of a particular suspect, even if the content of the conversation is encrypted. Certain new implementations of homomorphic encryption (HE) could also be used by LEAs to enable the detection of illegal content in transit over networks.[47]

[44] This includes the mobile phone number of the user; the phone numbers in her mobile address book; profile name, profile picture, and status message if available; a favourite list of contacts, and groups and lists associated with the account information.

[45] It is worth reiterating that the manner and method of accessing such data must be proportionate and subject to appropriate safeguards, review etc. (Bailey et al., 2018). The government should not have indiscriminate access to even such data.

[46] To this end, note for instance that Facebook has informed the US Senate Judiciary Committee that it is seeking to build tools that would enable it to provide critical metadata to LEAs, which could be used to *"...look for signals and patterns of suspicious activity"'* (Alford, 2020).

[47] Presently LEAs use hashed values of "known illicit content" to compare against suspicious data in order to determine whether illegal content such as child pornography is being distributed. The hashing process involves using an algorithm to generate a numeric identifier for known illegal content (Branham, 2019). This identifier can then be matched against hashes of relevant data sets to search for copies of the illegal content (Branham, 2019). This process can however require LEAs to access data sets of suspects. When looking for illegal content on a network, this may need them to access the entire data stream, which can affect privacy rights. Alternatively, service providers can screen content on their networks based on the hash values provided by LEAs. However, this can render the hash values insecure and enable gaming of the system. By using HE - which enables processing to be carried out on encrypted data, with an encrypted output - LEAs would be able to encrypt their database of hash values and then allow service providers to use this to run a check against their data streams. The service provider would learn nothing of the LEAs encrypted database but would still be able to screen content. This could therefore also reduce the need for centralised monitoring of entire data streams by government agencies. Refer (iamtrask, 2017; Armknecht et al., 2015; Buterin, 2020).

Also, it must be kept in mind that despite the fact that new technologies have indeed enabled new types of offences to be committed, the growth of the digital ecosystem (and the consequent collection of large quantities of data about individuals) has actually made policing much easier in many contexts. Indeed, one could argue that the vast quantities of unencrypted data available to LEAs can and has enhanced the capacity of LEAs to perform their functions, particularly in the Indian context, where the police force is significantly understaffed (Srikanth RP, 2019; Baxi, 2018). This is in fact why there are very real global concerns about the emergence of new forms of surveillance and the need to limit the State's powers in this respect.[48]

Second, incidents such as the FBI breaking Apple's encryption (Welch, 2020) or the installation of Pegasus software on the devices of politicians, activists, lawyers and journalists also show that governments are in fact more than capable of devising methods that circumvent unrecoverable encryption (Shantha, 2019). While the Indian government has not explicitly admitted or denied using Pegasus to surveil dissenters (Rajalakshmi, 2019), this incident definitely demonstrates the ability of governments to find their own methods to break unrecoverable encryption, and hence, the need for evolving mechanisms to regulate such instances of 'illegal surveillance' by governments using such invasive technologies. For instance, in Germany, the government encourages strong encryption and there is no ban or limitation on encryption techniques. However the legal framework also empowers LEAs to engage in hacking of devices for investigative purposes, provided it is approved by a judge and subject to satisfaction of certain substantive and procedural requirements (Acharya and Bankston and Schulman and Wilson, 2017).

Similarly, the United States has instituted a vulnerabilities equities process (VEP) which lays down a clear inter-agency procedural framework for US agencies to follow when they find a publicly unknown software/hardware vulnerability in information systems. The VEP seeks to balance the various risks and benefits before the concerned government agency to either disclose details regarding the vulnerability (so that it can be patched) or exploit it for law enforcement purposes.[49] Although the vulnerable equities process is not without its skeptics (Zhang, 2019), it indicates a route of progress. Given that *Puttaswamy* lays down that any restriction on the right to privacy must satisfy the proportionality test and have sufficient safeguards to prevent against misuse, exploitation of vulnerabilities within information systems should also be done in accordance with a lawful and proportionate legal framework. In addition to formulating a framework for oversight over surveillance processes themselves, there is therefore also a case to institute a VEP like framework in India. This can ensure appropriate balancing of interests and adherence to due process, even when the government resorts to exploitation of vulnerabilities for national security and law enforcement purposes.

Third, it must also be kept in mind that intermediaries, particularly large platforms, face significant pressure to enable investigation of online offences. Companies are often unwilling to incur the displeasure of the security establishment or indeed the adverse publicity that may result from cases where it appears that they are not doing all they can to reduce online criminal activity. As a result, companies often take decisions to build "weakness by design" into their products and services. For

[48] To illustrate, rather than having to secure a warrant and having to physically install a tracking device on a suspect's vehicle, LEAs can now merely request location data from a relevant intermediary (say the car manufacturer, a telecom company or a digital intermediary that provides mapping services).

[49] The US has constituted an equities review board which comprises representatives from different government agencies, and whose main function is to arrive at consensus about whether to disclose or restrict vulnerability information. A VEP secretariat is tasked with record-keeping and disclosure duties (Government of the United States, 2017).

instance, Apple initially planned to encrypt backed up data of users on the iCloud service. This would clearly improve user privacy and enhance the security of data stored in back-up, and would accord with the general move towards incorporating "privacy by design" into digital products and services.[50] However, it is claimed that pressure from the FBI led Apple to drop these plans (Menn, 2020). Similarly, WhatsApp, which had enabled encryption for user messages backed up on the cloud has reversed its decision to enable E2E on its backed up chats (Brewster, 2017; Lomas, 2017; Griffin, 2018; Brinkmann, 2018). Thus, while messages between users are encrypted during transit, they are not similarly secured once pushed to the cloud (Google Drive or iCloud), thereby enabling LEAs to access to such content relatively easily (WhatsApp, 2020a, 2020b). This can be problematic, particularly as back-ups are enabled by default. Normal users may therefore be unaware of how to disable such a feature, let alone that back-ups in the cloud are un-encrypted.[51]

It is undoubtedly the case that even with these tools and methods at hand, E2E slows down police investigation and reduces the efficiency of digital surveillance. However, the principles underlying a constitutional democracy recognise that individuals enjoy a "sphere of freedom from intrusion by the government" (Manes, 2019). As mentioned, robust encryption mechanisms serve the same purpose as robust fair trial and criminal due process guarantees – they re-balance the asymmetric power distribution between the State, which has a monopoly on coercive force, and the private individual. This is particularly important in a system where evidence obtained by law enforcement illegally is admissible in trial (*Pooran Mal v. Director of Inspection, 1974*).

Fourth, policy makers will have to analyse whether the benefits to law enforcement from mandating backdoors is worth the cost to society in terms of loss of privacy and security. Any such exercise should, in part, require an analysis of the number of cases where unrecoverable encryption has actually prevented, and not just delayed the decryption process. For instance, in the United States, the annual Title III wiretap reports for interception under the Communications Assistance for Law Enforcement Act reveal that a very small share encounter encryption, and a "majority" of those are eventually decrypted (Lewis et al., 2017). From 2012-2015, out of the 14,500 wiretaps ordered, 0.2% encountered unrecoverable encryption. Undoubtedly, this share has already increased in the last few years and will continue to increase in the future, but policy makers in India should conduct a similar empirical analysis to understand the impact of unrecoverable encryption. This also illustrates the need to create a proper evidence base in India, before making any significant policy changes.

A cost-benefit analysis would also involve examining whether the kind of software used by criminal actors would fall within the purview of the law. For instance, it has now emerged that many terrorist organisations and drug cartels rely on open source disk encryption software, produce their own encrypted communication apps, or use burner phones, which would not follow a traditional intermediary model (Callimachi, 2016). Alternatively, they may be using encryption software that is outside the jurisdiction of Indian LEAs. LEAs from different jurisdictions, industry stakeholders and academics have also noted that the focus on combating encryption has led many criminals to use certain 'new' methods to hide their information such as the use of steganography (Murphy, 2004;

[50] Notably, requirements to implement privacy by default/design, are included in the European GDPR, California's Consumer Privacy Protection Act and the draft Indian privacy law.

[51] It is relevant to note that much of WhatsApp's advertising focuses on the E2E encryption built into its services and the purported safety this provides a user. A normal user may well take this to imply that their data will be secured at all times.

Europol & Eurojust, 2020; Cabaj et al., 2018).[52] Steganography is the process of sending data, concealed within other apparently legal content.[53] By embedding illegal content within digital media files and by mimicking traffic behaviour of legitimate applications, illegal information can be hidden from those who are unaware of its existence (Cabaj et al., 2018; Murphy, 2004).[54] Such methods can be even more worrying to LEAs than the use of encryption, as the very existence of communications becomes difficult to detect.[55] Therefore actors who want to communicate secretly can do so with the help of different types of technology available. Legally restricting the quality of encryption available in popular platforms may risk the security and privacy of regular, law-abiding citizens, without assuring any substantive improvement in the government's ability to monitor and prevent actual criminal actors.

Fifth, another factor to consider is the cost of mandating recoverability, and effectively, a change in platform architecture for the intermediaries. This can take the form of the research and change in technology needed to introduce a backdoor, or lower sales due to increased privacy and security concerns of consumers. This should also include the cost of building and operating complex key recovery infrastructures and the cost of an increased likelihood of a data breach.

The Carnegie Institute (2019) has suggested, as a starting point, a middle ground to respond to the concerns of LEAs and civil society and privacy advocates. It recommends that data in motion should be treated differently from data at rest - while law enforcement would be prevented from carrying out surveillance of conversations happening in real time; they could apply for a judicial warrant to see the text, video, and audio files on a suspect's phone (data at rest). Apart from questions relating to viability Alford (2020), it is questionable whether such a solution will alleviate the security concerns about creating a backdoor. Under current Indian law, the police have the power to seize a mobile phone, with or without a judicial warrant,[56] but the legal basis to compel a suspect to provide their passcode to give access to their files is suspect, and has not been specifically adjudicated upon (Sekhri, 2020).

Finally, there is a risk that laws that mandate backdoors can become entangled in global politics, as has been the case with Huawei and ZTE. On June 30, 2020, the US FCC designated both these Chinese companies as threats to national security, thus preventing the use of money in the FCC Universal Service Fund from purchasing Huawei and ZTE equipment or services. Explaining its decision, the FCC Chairman Ajit Pai stated, *"both companies have close ties to the Chinese Communist Party and China's military apparatus, and both companies are broadly subject to Chinese law obligating them to cooperate with the country's intelligence services"* (Federal Communications Commission, 2020). Similarly, amidst, tension across the

[52] Europol, citing Professor Alan Woodward of the University of Sussex, notes that "there is increasing evidence that criminals are using data-hiding techniques to enhance existing attack vectors, develop novel attack vectors and exfiltrate data. The difficulty in analysing the threat is exacerbated by the difficult in detecting even the presence of such techniques. However, the anecdotal evidence has reached a level where we have to do more to understand the true nature of this threat" (Europol and European Cybercrime Centre, 2018).

[53] The concept has been used since ancient times. An early example is said to date back to the 5th Century BC when a greek prisoner shaved the head of a slave, tattooed a message onto his scalp and dispatched the message once the slave's hair had grown back, though it is now increasingly being used in the online space (Murphy, 2004; Shulmin & Kryolova, 2017)

[54] Examples of this method could include techniques to disguise information as regular online activity (such as Twitter traffic), to mask the presence of encrypted hard drives on a computer system, using fingerprint databases to transmit secret messages, etc.(Leyden, ^{2018}; Sheng Li & Xhang, ^{2019}; Shujun Li, ^{2016}).

[55] Steganography is not merely a method of hiding the contents of the communication, but the communication itself (Cabaj et al., 2018). Steganographic methods can in fact avoid deeppacket- inspection based systems or security checks by anti-malware and other tools (Shulmin & Kryolova, 2017).

[56] Sections 91, 93, 94, 100, 102, and 165 Code of Criminal Procedure, 1973.

Indo-Chinese border, the Indian government recently blocked access to 118 Chinese mobile apps in view of reports around use of Chinese apps for mining data of Indian users illegally (MeiTY, 2020). Under Chinese law, effective from January 2020, encryption is divided into three classes – core, common, and commercial. Foreign encryption systems can be sold in China, but will likely have to be duly approved and certified. The State Cryptography Administration (under the Communist Party) has been authorised to monitor and inspect the implementation and use of any cryptography system, although it cannot force companies to disclose their source code (Covington, 2019). As researchers have pointed out, this effectively means that unrecoverable encryption cannot be achieved, with all the data being accessible to the Chinese government (Dickinson, 2019; Lindsey, 2019).

If Indian law were to mandate backdoors, it could provide an opportunity to foreign governments to use this to designate Indian companies as threats to national security. Such a move would impact the efforts of the Indian government to develop an indigenous market in cyber security tools and products. Coupled with India's move to enact laws that restrict the cross-border transfer of certain types of data by companies, this can negatively impact India's trade and security relations.[57] This therefore, requires us to re-examine the oft-repeated assertion regarding the apparent conflict between national security and encryption, and highlights that deploying high standards of encryption may increase faith in Indian companies by foreign states (and the private sector) and consequently serve the interest of our national security, data security and economic development.

We therefore believe that, at this stage, the Indian government should refrain from enacting any law or amending the existing Intermediary Guidelines to expand the scope of the duty of technical assistance to require intermediaries to create backdoors and provide government access to unrecoverable encryption.

3.3 The way forward

Given the recommendation above that the law should not mandate the creation of backdoors or weaken encryption standards through government fiat, what is the way forward?

We believe that the Indian government would do well to take a more long-term perspective to the issue. Excessive focus on regulating a particular technology is generally unwise. The technology space can be difficult to regulate as technical development occurs at a rapid pace, implying that it is difficult for law and policy to keep up. The global nature of technology development means that the global diffusion of technologies is difficult to prevent. This is particularly the case when it comes to open source technologies, where there may not be a single actor responsible for the technology. The unintended consequences of excessive regulation can also be difficult to predict.[58] Therefore, it makes little sense for the State to either dictate network architecture or business models, particularly in the absence of any identified market failures.[59] This is not something the State is generally good at (Shah & Kelkar, 2019). Keep in mind too that the digital ecosystem and the internet more generally have largely developed, particularly from a technical perspective, on the basis of bottoms-up standard development processes. Given state capacity concerns in India, excessive intrusion into the standards/technical development of networks and platforms may be unwise (Shah & Kelkar, 2019).

[57] See Clause 33 of the Draft Personal Data Protection Bill, 2019.

[58] As an example, consider the increase in use of VPN technology after attempts at banning access to pornographic content in India.

[59] While the need to enforce criminal laws may be deemed a negative externality, as we have pointed out previously, a failure to create backdoors would not in itself render LEAs out of options.

It is also relevant to consider that while State concerns may be driven by the need to combat particularly egregious illegal content/conduct (such as distribution of child abuse material, terrorist content, etc.) it may be difficult to limit any exceptional access only to such use cases. Irrespective of the specific nature of the targeted content, intermediaries would still have to create backdoors or weaken encryption as a general practice. As described above, this can be problematic from the perspective of network security and civil liberties. This could also lead to a 'slippery slope' problem, where similar obligations are applied to more and more types of alleged offences.[60]

It goes without saying that as technology changes, new hurdles can indeed be created insofar as LEA access to user data is concerned. Rather than adopting ill-considered or knee jerk solutions to any perceived problems, the Indian government may therefore be wise to take steps such as enhancing its own investigative capacities, including by developing and utilising new digital forensics and other hacking tools (which would enable surveillance to be carried out in a more targeted manner). This however must be paralleled with improvements of oversight and review mechanisms.

Improvements in procedural frameworks around data access are also important given that the primary impediment to LEAs accessing data may arise not out of the use of encryption, but due to problems such as the inability to secure timely access to data from intermediaries (Parsheera & Jha, 2020). This could be caused by factors such as: (a) the poor legal frameworks around data requests and the processes that need to be followed in this respect;[61] and (b) the volume of requests that may need to be made, and the possibility of having to piece together information from multiple intermediaries (Parsheera & Jha, 2020; Parsheera & Bailey, 2018a). Such problems may in fact be further exacerbated in the near future with the deployment of 5G technology in India. This could require LEAs to liaise with many more service providers than is currently the case (Europol & Eurojust, 2020; Rathee, 2020; Tech Desk, 2020).[62]

Consequently, the government must, as a priority, seek to implement detailed rights preserving processes to enable LEAs timely access to data sets, in strict accordance with constitutional norms. Improving and formalising liaison and cooperation mechanisms with intermediaries is a must. This must be done at both domestic and international levels. In addition to ensuring procedures are put in place to ensure oversight and streamlining of access requests, one could also seek to place greater obligations on intermediaries pertaining to transparency about the the number and scope of LEA requests. Further, attention must be paid not just to the legal framework, but more prosaic implementation related issues such as ensuring that officials (in LEAs and the government) are appropriately trained. A recent EU Council resolution makes similar recommendations (Council of the European Union, 2020). Addressing process related issues may also lead to less unintended consequences on the digital ecosystem as a whole, due to the limited intervention in technological development.

[60] Such a problem has in fact been noted in the context of obligations cast on intermediaries to monitor or filter illegal content (Bahl, Rahman & Bailey, 2020).

[61] This may particularly be the case when it comes to intermediaries that are based abroad or otherwise subject to foreign laws.

[62] A critical component of 5G technology is the use of 'network splicing which simply put, involves multiple virtual network operators (VNOs) using a single shared physical network to provide services to users. Each VNO will use a 'slice' of the network to provide relevant services to its customers. This could therefore increase the number of intermediaries involved in the provision of services to users. The deployment of 5G may also enable greater use of 'Multi-access Edge Computing', where data and processing is moved from centralised locations to edges of the network (Quoc-Viet Pham et al., 2020). This could impact data retrieval by LEAs who typically access data through centralised nodes (Europol & Eurojust, 2020).

Another avenue of intervention would be for the government to support greater research and development, and to enhance coordination with academia and industry groups pertaining to public policy goals in the areas of encryption and related technologies. The aforementioned resolution of the European Council for instance, recognises the need for governments, industry, research and academia to work together to find a better balance between the need to ensure strong encryption while providing relevant access to LEAs (Council of the European Union, 2020; Agrawal, 2020a). The resolution also reiterates the need to adopt "innovative approaches" in view of the development of new technologies (Council of the European Union, 2020).

Ensuring appropriate government support for R&D in the cyber security space and supporting the growth of an indigenous market in security products will therefore be important. One specific area of focus could relate to the development of quantum computing and related technologies. The introduction of quantum computers is expected to render existing methods of encryption obsolete due to the higher level of computing speeds that will be made possible, the relative ease of carrying out factorisation, etc.[63] While in the short term, this may prove beneficial to State actors (as they are more likely to have access to quantum technology than private actors due to factors such as the expense involved), in the longer term one can expect the development of "quantum safe" standards of encryption (Europol, 2019; Kwiatowski, 2019; Princeton University CITP, 2019; Europol & Eurojust, 2020; Bernstein & Lange, 2017). In fact, various "promising proposals" for quantum safe encryption have already been published, with numerous international and domestic bodies engaged in developing standards for such systems (Bernstein & Lange, 2017). The existing debate is therefore likely to continue, only in the context of newer technology.

The State must therefore recognise the importance of maintaining a cutting-edge in what is essentially an arms race. While it may still be 10-20 years before quantum technology becomes generally available, globally, researchers are already involved in developing encryption systems that are secure against both quantum and classical computers (Europol, 2019; Princeton University CITP, 2019). The Indian government must ensure that it is at the forefront of such developments, which will enhance its ability to respond to changes in technological systems. Investing in indegenous capacities of both the private and public sector would also enable India to play a more meaningful part in international discussions around issues of standard setting, which are currently dominated by more developed countries.[64]

We note that more developed jurisdictions, such as the UK, EU and US have indeed focussed on such methods rather than using the State's coercive powers to attempt to limit technology development (Privacy Enhancing Technologies Working Group, 2019; Europol & Eurojust, 2020; Murphy, 2004). Notably, one of the more developed countries in this space, Israel, follows a policy that does not focus on excessive regulation of technology or using the State's coercive powers to demand creation of vulnerabilities or depositing decryption keys. Instead, Israel seeks to develop the State's capacities to take advantage of security vulnerabilities in encryption products by hiring and funding research into encryption and cyber security and by developing synergies with the private sector (Donahue, 2018). Processes are designed so that the State is at the forefront of encryption and cyber security developments, and can effectively engage with the private sector with respect to identified security

[63] Encryption techniques, such as RSA, rely on multiplying two large prime numbers to create the encryption key. Factoring this product is a difficult task for classic computers. However, quantum computers can do so quickly using 'Shor's Algorithm'. Other methods of encryption can also be rendered ineffective using what is known as 'Grover's Algorithm' (Princeton University CITP, 2019; Bernstein & Lange, 2017).

[64] The lack of meaningful engagement with international processes can allow foreign governments to further their interests at the cost of India's security and strategic interests, for instance, by adopting encryption standards that contain backdoors (Rathi, Grover & Abraham, 2018).

threats (Donahue, 2018). Similar methods are favoured in Germany, which generally adopts a pro-encryption stand in its policies, while at the same time focussing State resources on developing techniques for investigative hacking (Acharya, Bankstone, Schulman & Wilson, 2017; Glance, 2011; Hudig, 2012; Anonymous, 2017; Grull, 2020). While undoubtedly even such systems would require appropriate oversight and other legal/procedural mechanisms to be implemented, "hacking" based policies may provide a more rights-preserving alternative than weakening entire networks.

4 Conclusion

The rising use of encryption the world over has proven to be tricky for LEAs in that it directly impacts their ability to collect data required to prevent, investigate, and prosecute offences. This has led to various policy and technical proposals to address this perceived impasse, though no globally accepted best practice or standard has been evolved in this regard yet. 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. 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 of decrypting the encrypted information. Courts have also weighed in on this debate, with the Madras High Court and the Supreme Court hearing petitions that seek to create mechanisms whereby LEAs could have access to end-to-end encrypted content used by popular platforms such as WhatsApp - potentially through the creation of backdoors. A recent Rajya Sabha Ad-hoc Committee Report has recommended that LEAs be permitted to break or weaken E2E to trace distributors of illegal content.

Against this background, this paper has sought to examine 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, for instance, through the creation of backdoors. We have also examined proposals for alternatives, such as the use of escrow mechanisms and ghost protocols, in brief.

We argue that while LEAs have relevant concerns about the increasing use of certain types of encryption (in particular unrecoverable encryption) that obstructs investigative and law enforcement efforts, implementing a general mandate for creating backdoors under the guise of "technical assistance" can have significant effects on privacy of individuals and overall network security. We argue that such a mandate has significant privacy and security concerns, may not pass a cost-benefit analysis, and more importantly, may be against constitutional guarantees, being disproportionate and unnecessary. In particular, we point to the fact that use of encryption may not be the primary hurdle to investigate online offences in India, particularly since LEAs can utilise relevant processes to legally gain access to content that is encrypted using recoverable encryption. However, even with respect to unrecoverable encryption, the following factors should be considered as part of a balancing exercise to argue against the creation of backdoors: (i) LEAs can use alternative methods to assist their investigations, including through the use of metadata or unencrypted back-up data; (ii) LEAs can enhance their covert capacities and use regulated hacking procedures to decrypt unrecoverable encryption; (iii) the availability of various data minimisation and non-encryption based techniques to mask/conceal data, thereby implying that the focus on encryption may be unwarranted and counterproductive; and, (iv) the civil liberty, privacy, security, and economic costs of mandating changes in platform and network architecture.

We argue that rather than attempting to limit the use of certain technologies, or mandating significant changes in platform and network architecture, the Indian government would be better off taking a more rights-preserving and long-term view of the issue. Not only would this enable a more holistic consideration of the interests involved - for instance, in terms of considering the geopolitical implications of such a step - this would also avoid unintended consequences and limit the costs that come with excessive government interference in the technology space. The tussle between LEAs and criminal actors has always been an arms-race. Rather than taking knee-jerk steps that may have significant effects on the digital ecosystem, the government should focus on enhancing state capacity along numerous fronts, including through (i) appropriately funding LEAs, including by hiring security and technical researchers; (ii) standardising and improving current methods of information access; (iii) supporting academic and industry research into cryptography and allied areas; and (iv) enhancing coordination between industry, academia and the State.

Refrences

Abelson et al. (1997). The risks of key recovery, key escrow, and trusted third-party encryption. Retrieved from https://www.schneier.com/academic/paperfiles/paper-key-escrow.pdf

Abraham, S. & Hickok, E. (2012). Government access to private sector data in India. *International Data Privacy Law*, (4), 302–315. Retrieved from https://bit.ly/2z1KkaV

Access Now et al. (2019). Coalition letter to gchq on ghost proposal. Retrieved from https://tinyurl.com/yywqcb5y

Acharya and Bankston and Schulman and Wilson. (2017). *Deciphering the European encryption debate: Germany.* Open Technology Institute. Retrieved from https://d1y8sb8igg2f8e.cloudfront.net/documents/Transatlantic_Encryption_Germany.pdf

Acharya, B., Bankstone, K., Schulman, R. & Wilson, A. (2017). Deciphering the European encryption debate: Germany. Retrieved from https://d1y8sb8igg2f8e.cloudfront.net/documents/Transatlantic_Encryption_Germany.pdf

ACLU and EFF. (2015). *Brief of amicus curiae, American civil liberties union foundation of Massachusetts, the american civil liberties union foundation, and the electronic frontier foundation in support of the defendant-appellee.* ACLU and EFF. Retrieved from https://tinyurl.com/y36b8syv

Agencies. (2010). Rim gives in, blackberry server to be located in India. Retrieved from https://bit.ly/3h4R6wC

Agrawal, A. (2020a). No, the council of the European union is not considering a ban on end-to-end encryption. Retrieved from https ://www.medianama.com/2020/11/223-council-of-european-union-no-ban-on-encryption/

Agrawal, A. (2020b). We want backdoors to e2e encrypted platforms for law enforcement': India, japan, five eyes to companies. Retrieved from https : //www.medianama.com/2020/10/223- India- japan-five-eyes- backdoorsencryption/

Alford, D. (2020). Options to end the end to end encryption debate. Retrieved from https://www.infosecurity-magazine.com/opinions/end-encryption-debate/

Anonymous. (2017). Germany expands surveillance of encrypted message services. Retrieved from https : / /phys . org / news / 2017 - 06 - Germany - surveillance - encrypted-message.html

Anthony Clement Rubin v. Union of India. (2019). 2019 SCC Online Mad 11785.

Apple. (2016). *Answers to your questions about apple and security.* Retrieved from https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf

Apple. (2018). *Legal process guidelines:government and law enforcement within the united states.* Retrieved from https://www.apple.com/customer-letter/answers/

Armknecht, F., Boyd, C., Carr, C., Gjosteen, K., Jaschke, A., Reuter, C. A. & Strand, M. (2015). A guide to fully homomorphic encryption. Retrieved from https://eprint.iacr.org/2015/1192.pdf

Arun, C. (2019). The 'purdah' amendment: Proposed changes to the it act could draw a veil over the indian internet. Retrieved from https://tinyurl.com/y22da3xq

Bahl, V., Rahman, F. & Bailey, R. (2020). Internet intermediaries and online harms: Regulatory responses. Retrieved from http://datagovernance.org/report/internet-intermediaries-and-online-harms-regulatory-responses-inindia

Bailey, R., Bhandari, V., Parsheera, S. & Rahman, F. (2018). Use of personal data by intelligence and law enforcement agencies. Retrieved from https : //bit.ly/2CEzCoN

Bailey, R., Bhandari, V., Parsheera, S. & Rahman, F. (2020). Comments on the draft personal data protection bill, 2019: Part ii. Retrieved from https://blog.theleapjournal.org/2020/04/comments-on-draft-personal-data_10.html

Bailey, R., Parsheera, S. & Rahman, F. (2019). Comments on the (draft) information technology (intermediary guidelines (amendment) rules), 2018. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3328401

Baxi, A. (2018). Law enforcement agencies in India are using artificial intelligence to nab criminals – here's how. Retrieved from https://tinyurl.com/y3np54df

Bernstein, D. & Lange, T. (2017). Post-quantum cryptography. *Nature,* 188–194. Retrieved from https://www.nature.com/articles/nature23461

Bhandari, V., Kak, A., Parsheera, S. & Rahman, F. (2017). An analysis of puttaswamy: The supreme court's privacy verdict. Retrieved from https://blog.theleapjournal.org/2017/09/an-analysis-of-puttaswamy-supreme.html

Bhandari, V. & Lahiri, K. (2020). The surveillance state: Privacy and criminal investigation in India: Possible futures in a post-puttaswamy world. *University of Oxford Human Rights Hub Journal,* (2), 15.

Bharati, N. (2008). At last govt cracks blackberry code. Retrieved from https :/ / economictimes . indiatimes .com/At_last_govt_cracks_BlackBerry_code/articleshow/3510719.cms

Bhatia, G. (2018). Privacy and the criminal process: Selvi v. state of karnataka. Retrieved from https://tinyurl.com/y9gvmnyz

Branham, R. A. (2019). Hash it out: Fourth amendment protection of electronically stored child exploitation. *Akron Law Review,* 217–244. Retrieved from https: //tinyurl.com/y4464d4l

Brewster, T. (2017). Whatsapp quietly boosted its icloud encryption - fbi contractors think they can already break it. Retrieved from https://tinyurl.com/yy9qxpxr

Brewster, T. (2020). Fbi hacks iphones in pensacola terrorist shooting case, but the war with apple goes on. Retrieved from https://tinyurl.com/y4hpu4pf

Brinkmann, M. (2018). Whatsapp backups are not encrypted. Retrieved from https://www.ghacks.net/2018/09/04/whatsapp-backups-android/

Bruce Schneier. (2015). Why we encrypt? Retrieved from https://www.schneier.com/blog/archives/2015/06/why_we_encrypt.html

Buterin, V. (2020). Exploring fully homomorphic encryption. Retrieved from https://vitalik.ca/general/2020/07/20/homomorphic.html

Cabaj, K., Caviglione, L., Mazurczyk, W., Wendzel, S., Woodward, A. & Zander, S. (2018). The new threats of information hiding: The road ahead. Retrieved from https://arxiv.org/pdf/1801.00694.pdf

Callimachi, R. (2016). How isis built the machinery of terror under europe's gaze. Retrieved from https://www.nytimes.com/2016/03/29/world/europe/isisattacks-paris-brussels.html?_r=0

Cardozo, N. (2019). Give up the ghost- a backdoor by another name. Retrieved from https://www.eff.org/deeplinks/2019/01/give-ghost-backdoor-anothername

Carnegie Institute. (2019). *Moving the encryption policy conversation forward.* Carnegie Endowment for International Peace. Retrieved from https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573

Chandra, A. (2020). Proportionality in india: A bridge to nowhere? *University of Oxford Human Rights Hub Journal,* (2), 55–86.

Coldewey, D. (2017). Wtf is a backdoor? Retrieved from https://techcrunch.com/2017/01/29/wtf-is-a-backdoor/

Comey, J. (2014). *Going dark: Are technology, privacy, and public safety on a collision course?* Federal Bureau of Investigation. Retrieved from https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-publicsafety-on-a-collision-course

Council of the European Union. (2020). Draft council resolution on encryption - security through encryption and security despite encryption. Retrieved from https://tinyurl.com/y3helyvy

Covington. (2019). China enacts encryption law. Retrieved from https://www.cov.com/-/media/files/corporate/publications/2019/10/china_enacts_encryption_law.pdf

Department of Homeland Security. (2015). *Going dark - covert messaging applications and law enforcement implications.* U.S. Department of Homeland Security. Retrieved from https://tinyurl.com/y3scbe2z

Dickinson, S. (2019). China's new cryptography law: Still no place to hide. Retrieved from https://www.chinalawblog.com/2019/11/chinas-new-cryptographylaw-still-no-place-to-hide.html

Doffman, Z. (2020). Why you should stop using facebook messenger. Retrieved from https://tinyurl.com/y285ob7v

Donahue, J. L. (2018). A comparative analysis of international encryption policies en route to a domestic solution. Retrieved from https://calhoun.nps.edu/handle/10945/58291

EFF. (2011). *Brief of amicus curiae, eff, in support of defendant fricosu's opposition to the government's application under the all writs act requiring defendant to assist in the execution of previously issued search warrants.* Electronic Frontier Foundation. Retrieved from https://www.eff.org/node/58527

EFF. (2018). A deep dive on end to end encryption: How do public key encryption systems work? Retrieved from https://tinyurl.com/y4ylekcw

Europol. (2019). Do criminals dream of electric sheep: How technology shapes the future of crime and law enforcement. Retrieved from https://tinyurl.com/y4tkk87w

Europol and European Cybercrime Centre. (2018). Internet organised crime threat assessment (iocta). Retrieved from https://www.europol.europa.eu/internetorganised-crime-threat-assessment-2018

Europol & Eurojust. (2020). Second report of the observatory function on encryption. Retrieved from https://bit.ly/3lPT2g1

Federal Communications Commission. (2020). Fcc designates huawei and zte as national security threats. Retrieved from https : / / docs . fcc . gov / public / attachments/DOC-365255A1.pdf

Finklea, K. (2016). Encryption and the "going dark" debate. Retrieved from https://fas.org/sgp/crs/misc/R44481.pdf

Fisher, J. (2017). Group chat with end-to-end encryption. Retrieved from https://bit.ly/3nRPhaj

Freeh, L. (1997). *Statement of louis j. freeh, director, federal bureau of investigation.* Federal Bureau of Investigation. Retrieved from https://www.epic.org/crypto/legislation/freeh_797.html

Gill, L. (2018). Law, metaphor, and the encrypted machine. Osgoode Hall L.J.440–477.

Glance, D. (2011). Ein spy: Is the german government using a trojan to watch its citizens? Retrieved from https://theconversation.com/ein- spy- is- thegerman-government-using-a-trojan-to-watch-its-citizens-3765

Goffman, E. (1959). *The presentation of self in everyday life.* Doubleday. Government of the United States. (2017). Vulnerabilities equities policy and process for the united states government. Retrieved from https://tinyurl.com/ycj6dzw3

Green, M. (2018). On ghost users and messaging backdoors. Retrieved from https://blog . cryptographyengineering .com/2018/12/17/on- ghost - users - andmessaging-backdoors/

Greenberg, A. (2018). Hacker lexicon: What is perfect forward secrecy? Retrieved from https://www.wired.com/2016/11/what-is-perfect-forward-secrecy/

Griffin, A. (2018). Whatsapp update brings backups that are not encrypted. Retrieved from https://tinyurl.com/ybz5qse5

Gripman, D. (1999). Electronic document certification: A primer on the technology behind digital signatures. *John Marshall J. Computer and Info* L. 17. Retrieved from https://repository.jmls.edu/jitpl/vol17/iss3/3/

Grull, P. (2020). Eu states ponder means to access encrypted data. Retrieved from https://tinyurl.com/yymkz3db

Hardy, K. (2020). Australia’s encryption laws: Practical need or political strategy? *Internet Policy Review,* (3).

Harold Abelson et al. (2015). *Keys under doormats: Mandating insecurity by requiring government access to all data and communications.* MIT Computer Science and Artificial Intelligence Laboratory Technical Report. Retrieved from http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAILTR-2015-026.pdf

Hartzog, W. & Selinger, E. (2015). Surveillance as loss of obscurity. *Washington and Lee Law Review,* (3), 1343–1387.

Haunts, S. (2019). *Applied cryptography in .net and azure key vault: A practical guide to encryption in .net and .net core.* Apress.

Hudig, K. (2012). Analysis - state trojans: Germany exports ‘spyware with a badge’. Retrieved from https://www.statewatch.org/media/documents/analyses/no-189-state-trojans.pdf iamtrask. (2017). Safe crime detection. Retrieved from http://iamtrask.github.io/2017/06/05/homomorphic-surveillance/

INSLM. (2019). Inslm review of the telecommunications and other legislation amendment (assistance and access) act 2018 (tola act). Retrieved from https://www.inslm.gov.au/current-review-work

Jaikaran, C. (2016). Encryption : Frequently asked questions. Retrieved from https://fas.org/sgp/crs/misc/R44642.pdf

Jjemba, E. & Ben-Avie, J. (2020). Australian watchdog recommends major changes to exceptional access law tola. Retrieved from https://tinyurl.com/y3m7fscy

Justice KS Puttaswamy (Retd.) v. Union of India. (2017). 2017 (10) SCC 1.

Justice KS Puttaswamy (Retd.) v. Union of India. (2019). (2019) 1 SCC 1.

Justice Srikrishna Committee. (2018). A free and fair digital economy: Protecting privacy, empowering indians. Report of the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna. Retrieved from http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

Kahney, L. (2019). The fbi wanted a backdoor to the iphone. tim cook said no. Retrieved from https://www.wired.com/story/the-time-tim-cook- stoodhis-ground-against-fbi/

Kamakoti, V. (2019). Report of prof. kamakoti in wp nos. 20214 and 20774 of 2018. Retrieved from https://tinyurl.com/y2blq4vp

Kayel, D. (2015). *Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression.* United Nations, Human Rights Council. Retrieved from https://tinyurl.com/y4nto224

Krishnakumar, T. (2019). Law enforcement access to data in India: Considering the past, present, and future of section 91 of the code of criminal procedure, 1973. *Indian J of Law and Tech.* 67–101.

Krzyzanowski, P. (2004). Cryptographic communication and authentication. Retrieved from https://www.cs.rutgers.edu/~pxk/rutgers/notes/content/13-crypto.pdf

Kwiatowski, K. (2019). Towards post quantum cryptography in tls. Retrieved from https://blog.cloudflare.com/towards-post-quantum-cryptography-in-tls/

Levy, I. & Robinson, C. (2018a). Principles for a more informed exceptional access debate. Retrieved from https : / /www. lawfareblog .com/ principles - more - informed-exceptional-access-debate

Levy, I. & Robinson, C. (2018b). Principles for a more informed exceptional access debate. Retrieved from https : / /www. lawfareblog .com/ principles - more - informed-exceptional-access-debate

Lewis, J., Zheng, D. & Carter, W. (2017). *The effect of encryption on lawful access to communications and data.* Centre for Strategic and International Studies (CSIS). Retrieved from https://tinyurl.com/yyjs4lqd

Leyden, J. (2018). Russian doll steganography allows users to mask covert drives. Retrieved from https://portswigger.net/daily-swig/russian-doll-steganographyallows-users-to-mask-covert-drives

Li, S. [Sheng] & Xhang, X. (2019). Towards construction-based data hiding: From secrets to fingerprint images. Retrieved from https://ieeexplore.ieee.org/document/8510853

Li, S. [Shujun]. (2016). New information hiding technology to be commercialised by crossword cybersecurity. Retrieved from https://tinyurl.com/yy5gwrng

Lindsey, N. (2019). China’s new encryption law highlights cryptography as a strategic priority. Retrieved from https://tinyurl.com/y2rpzwuz

Lomas, N. (2017). Whatsapp quietly added encryption to icloud backups. Retrieved from https://tinyurl.com/yxjtnhu2

Luciano, D. & Prichett, G. (1987). Cryptology: From caesar ciphers to public-key cryptosystems. *College Mathematics* J. 2–17.

Manes, J. (2019). Secrecy and evasion in police surveillance technology. *Berkeley Technology* L.J. 503–566.

MeiTY. (2018). Comments invited on draft of intermediary guidelines 2018. Retrieved from https://www.meity.gov.in/comments-invited-draft-intermediaryrules

MeiTY. (2020). Government blocks 118 mobile apps which are prejudicial to sovereignty and integrity of india, defence of india, security of state and public order. Retrieved from https : //www. pib . gov. in /PressReleasePage . aspx? PRID=1650669

Menn, J. (2020). Exclusive: Apple dropped plan for encrypting backups after fbi complained - sources. Retrieved from https://www.reuters.com/article/usapple-fbi-icloud-exclusive-idUSKBN1ZK1CT

Mohan, V. (2020). New e-tools being developed to trace sources of fake news. Retrieved from https://tinyurl.com/y36akdv5

Mohanty, B. (2019). *The encryption debate in india.* Carnegie Endowment for International Peace. Retrieved from https://carnegieendowment.org/2019/05/30/encryption-debate-in-india-pub-79213

Murphy, S. (2004). Steganography - the new intelligence threat. Retrieved from https://bit.ly/3lQrgQF

National Academies of Sciences, Engineering, and Medicine. (2018). *Decrypting the encryption debate: A framework for decision makers.* National Academies Press.

Parsheera, S. & Bailey, R. (2018a). Data localisation in india: Questioning the means and ends. Retrieved from https://macrofinance.nipfp.org.in/releases/BP2018_Data-localisation-in-India.html

Parsheera, S. & Bailey, R. (2018b). The aadhaar judgement uses the right-toprivacy test in two completely different ways. Retrieved from https://tinyurl.com/y328ahhv

Parsheera, S. & Jha, P. (2020). Cross-border data access for law enforcement: What are indias strategic options? Carnegie India Working Paper. Retrieved from https://carnegieendowment.org/files/ParsheeraJha_DataAccess.pdf

Pell, S. (2013). Jonesing for a privacy mandate, getting a technology fix – doctrine to follow. *North Carolina J. of Law and Tech.* 489–555.

Peterson, A. (2015). The ‘crypto wars’ of the 1990s are brewing again in washington. Retrieved from https://tinyurl.com/y2ykd8ln

PIB. (2020). Rajya sabha committee calls for mandatory apps on all devices and filters to regulate children’s access to pornography content. Retrieved from https://pib.gov.in/PressReleseDetail.aspx?PRID=1600505

Pirker, B. (2013). *Proportionality analysis and models of judicial review.* European Administrative Law Series. Retrieved from https://core.ac.uk/download/pdf/79426664.pdf

Pooran Mal v. Director of Inspection. (1974). (1974) 1 SCC 345.

Princeton University CITP. (2019). Implications of quantum computing for encryption policy. Retrieved from https://tinyurl.com/y4wv8bao

Privacy Enhancing Technologies Working Group. (2019). Protecting privacy in practice: The current use, development and limits of privacy enhancing technologies in data analysis. Retrieved from https://tinyurl.com/y4tlnnrp

Quoc-Viet Pham et al. (2020). A survey of multi-access edge computing in 5g and beyond: Fundamentals, technology integration, and state-of-the-art. Retrieved from https://tinyurl.com/y3np54df

Rajalakshmi, T. (2019). The pegasus fiasco: Privacy in peril. Retrieved from https://bit.ly/35kdcJv

Rathee, K. (2020). 5g trials: Telecom operators with non-chinese vendors to get dot approval. Retrieved from https://tinyurl.com/yy5pt677

Rathi, A., Grover, G. & Abraham, S. (2018). Regulating the internet: The government of india and standards development at the ietf. Retrieved from https://cis-india.org/internet-governance/files/regulating-the-internet Reuters. (2019). Government of india and whatsapp are debating encryption laws: All you need to know. Retrieved from https://tinyurl.com/y29r9nuk

Richards, N. (2013). Don't let u.s. government read your e-mail. Retrieved from https://edition.cnn.com/2013/08/18/opinion/richards-lavabit-surveillance/index.html

Richards, N. (2015). *Intellectual privacy: Rethinking civil liberties in the digital age.* Oxford University Press.

Rivers, J. (2006). Proportionality and variable intensity of review. *Cambridge Law Journal,* 174–190.

Sekhri, A. (2020). Mobile phones and criminal investigations in India. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3590996

Selinger, E. (2015). What is intellectual privacy, and how yours is being violated. Retrieved from https://tinyurl.com/yxmnecyg

Selvi v. State of Karnataka. (2010). (2010) 7 SCC 263.

Shafi, H. (2018). Are whatsapp group chats vulnerable to spying despite end-to-end encryption? Retrieved from https://tinyurl.com/y48k68rf

Shah, A. & Kelkar, V. (2019). In *service of the republic:* The art and science of economic policy. Penguin Books.

Shantha, S. (2019). Indian activists, lawyers were 'targeted' using israeli spyware pegasus. Retrieved from https://thewire.in/tech/pegasus-spyware-bhimakoregaon-activists-warning-whatsapp

Sharma, B. (2015). Modi government withdraws draft encryption policy: It minister. Huffington Post. Retrieved from https://bit.ly/336yirS

Shulmin, A. & Kryolova, E. (2017). Steganography in contemporary cyberattacks. Retrieved from https ://securelist .com/steganography- in- contemporary -cyberattacks/79276/

Solove, D. (2007). "i've got nothing to hide" and other misunderstandings of privacy. San Diego Law Review, 745–772.

Srikanth RP. (2019). How policing in india is getting a tech makeover. Retrieved from https://www.expresscomputer.in/editorials/how-policing-in-india-isgetting-a-tech-makeover/41446/

Tech Desk. (2020). Reliance jio made in india 5g solution announced at ril agm 2020. Retrieved from https://tinyurl.com/y9q7wwhl

Tillett, A. (2019). Encryption laws leave local tech industry in a ‘chokehold’. Retrieved from https://tinyurl.com/y5ypjosz

Townsend, P. (2019). Rsa vs aes encryption: A prime. Retrieved from https://info.townsendsecurity.com/rsa-vs-aes-encryption-a-primer

TRAI. (2018). *Recommendations on privacy, security and ownership of data in the telecom sector.* Telecom Regulatory Authority of India. Retrieved from https://trai.gov.in/sites/default/files/RecommendationDataPrivacy16072018_0.pdf

TRAI. (2020). *Recommendations on regulatory framework for over-the-top (ott) communication services.* Telecom Regulatory Authority of India. Retrieved from https : / /www. trai . gov . in / sites / default / files / Recommendation_14092020_0.pdf

Union, E. (2016). Article 32-security of processing. Retrieved from https://gdprinfo.eu/art-32-gdpr/

van den Berg, B. (2010). *The situated self: Identity in a world of ambient intelligence.* Wolf Legal Publishers.

Venkatanarayanan, A. (2019). Dr kamakoti’s solution for whatsapp traceability without breaking encryption is erroneous and not feasible. Retrieved from https://tinyurl.com/y23rk42u

Welch, C. (2020). The fbi successfully broke into a gunman’s iphone, but it’s still very angry at apple. Retrieved from https://tinyurl.com/yc48t8fk

WhatsApp. (2019). *Whatsapp legal info*. Retrieved from https://www.whatsapp.com/legal/#key-updates

WhatsApp. (2020a). Faq: About google drive backups. Retrieved from https://faq.whatsapp.com/android/chats/about-google-drive-backups/?lang=fb

WhatsApp. (2020b). Faq: How to backup to icloud. Retrieved from https://faq.whatsapp.com/iphone/chats/how-to-back-up-to-icloud/?lang=en

Wong, J. C. (2020). The fbi and apple are facing off over an iphone again. what’s going on? Retrieved from https://www.theguardian.com/us-news/2020/jan/14/fbi-apple-faceoff-iphone-florida-shooting

Zhang, D. (2019). Vulnerabilities equities process revisited. Retrieved from https://georgetownsecuritystudiesreview.org/2019/05/28/vulnerabilities-equitiesprocess-revisited/

Acknowledgements

We thank participants at the Data Governance Network meetings of August 6 and October 28, 2020, Smriti Parsheera, Gaurav Jain, Udbhav Tiwari, Divij Joshi and Devendra Damle for comments and discussions. All errors are our own.

About the Authors

Rishab Bailey and Faiza Rahman are technology policy researchers at the National Institute of Public Finance and Policy, New Delhi. Vrinda Bhandari is a practicing advocate. Authors are listed in alphabetical order

datagovernance.org   dgn@idfcinstitute.org

@datagovnetwork   /datagovnetwork   /datagovnetwork