DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

ENCRYPTION AND THE DIGITAL ECONOMY

Balancing Security, Privacy and National Security

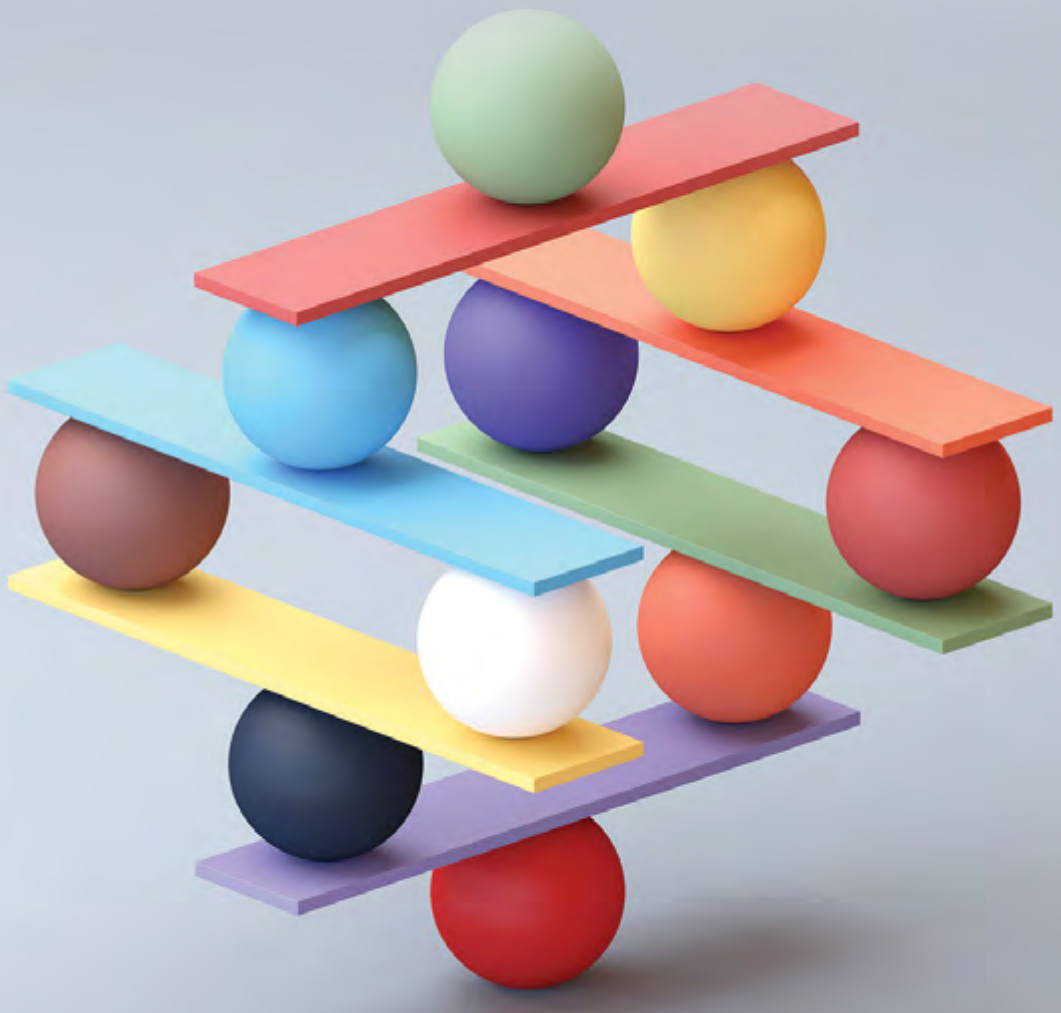


Table of CONTENTS

1

Introduction

Today's India is digital and interconnected. Innovation in Internet-based services and products have created new avenues for sustainable economic growth and development. But the digital economy can only maintain growth and generate opportunities for individuals and businesses alike if the underlying Internet infrastructure is strong, secure and trustworthy. Without a secure basis, India's digital economy is exposed to risk. The building block for a secure communications and information infrastructure is encryption. It is used for everything from preventing illicit access to stored data, to protecting messages in transit, and authenticating financial transactions.[1]

Encryption ensures protection of information and communications in different spheres – personal, commercial, and in the public sector. It secures data against unwanted access, helps ensure the confidentiality of data, and delivers trust in the digital economy. It is essential for all key actors: governments, individuals, and businesses.

Encryption ensures protection of information and communications in different spheres – personal, commercial, and in the public sector. It secures data against unwanted access, helps ensure the confidentiality of data, and delivers trust in the digital economy. It is essential for all key actors: governments, individuals, and businesses. For citizens, encryption provides privacy and anonymity, while businesses use encryption to secure trade secrets, communicate securely, and build trust. Governments use encryption to protect critical information, secrets, and systems.[2] Encryption has also become a ubiquitous part of the digital economy and is the necessary protection that underpins the digital marketplace. Across sectors, encryption has emerged as the tool that has allowed for the financial transformation of the modern Indian economy. It has enabled innovation, growth, research and development, and ultimately redefined digital trust.

At the same time, there is growing risk to public safety as organized crime, terrorists, and child pornographers are drawn to the use of encrypted platforms that are technically impossible to access by law enforcement or by the companies that provide the devices and applications.[3]

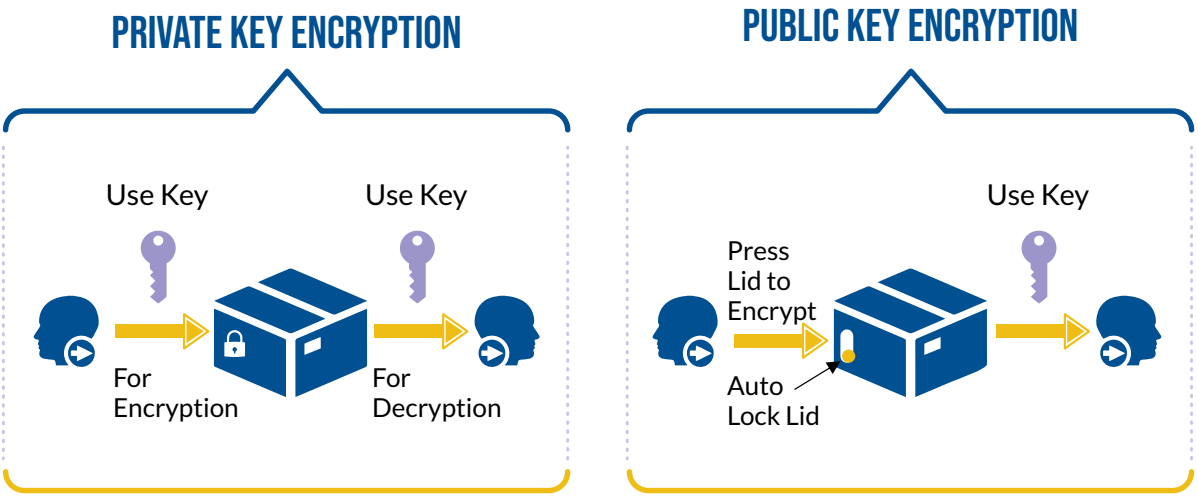
Understanding Encryption

Encryption involves the transformation of 'plaintext' or readable information into unintelligible data. This process of transforming data into encrypted information uses cryptography, a discipline that embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorised use.[4]

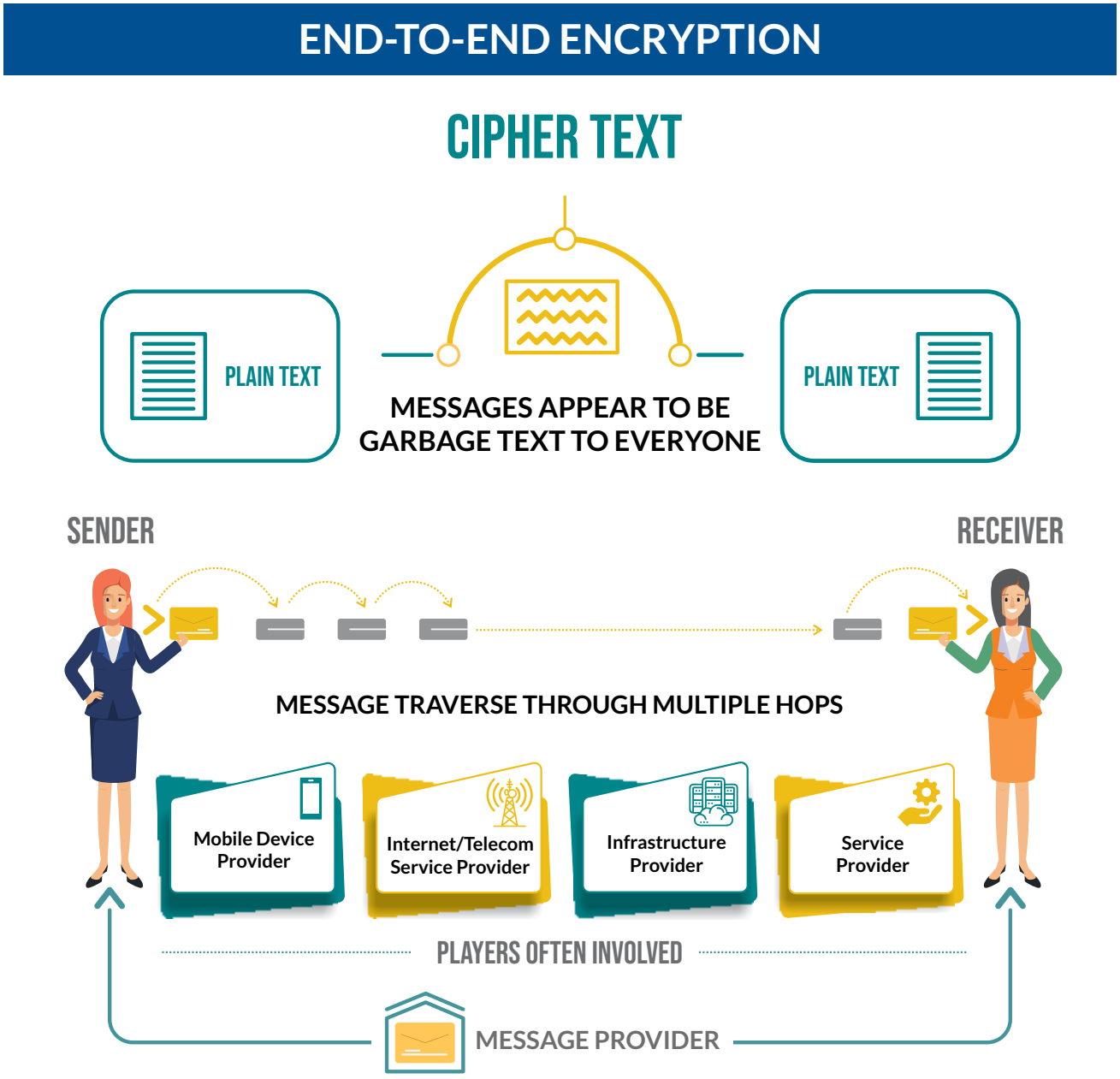
At the most fundamental level, algorithms are used to encrypt information and generate keys. The key is used to scramble the data into unreadable text. Depending on the type of encryption, the same key can be used to decrypt[5] the data, or a separate set of keys will be used.[6] For a given algorithm, the strength of the encryption increases with the length of the key, which is measured in bits.[7] An algorithm can be applied to encrypt data in transit, i.e., when it is sent from one place to another through a network; or at rest, i.e., where it is stored, such as on a server, end-device, or hard-drive.

Encryption can either be symmetric or asymmetric, or a combination of both. In symmetric encryption, the same key is used for encrypting and decrypting. In addition to its security benefits, it also does not take a lot of time to encrypt and decrypt data. On the other hand, in asymmetric encryption, the key used for encrypting is different from the key used for decrypting. This is also called 'public key cryptography', because one of the keys used for encryption is public. For example, a user can list one of their keys in a public directory, which would allow anyone to send them a message. However, the message can only be decrypted by the user through their private key, which remains secret.

FUNDAMENTAL TYPES OF ENCRYPTION



On another level, encryption can be either server-side or user-side.[8] In the former, the server of the service provider manages the encryption and the decryption of the data, by managing the keys. For example, e-mail encryption is typically server-side, as users expect to be able to access stored



e-mails, recover account passwords if they forget them, access their e-mail from any device, and send e-mails to their friends using different e-mail platforms.[9] Notably, because the service provider has access to the encryption keys, they can share them with law enforcement or other third parties pursuant to a legal request.

On the other hand, user-side encryption refers to cryptography applied by the user, or at the device of the user. This can include both user-deployed encryption such as VPNs, and technologies such as end-to-end encryption that are deployed by the service provider at the application level. The service provider does not hold access to the keys and will be unable to share them with law enforcement, regardless of a legal request

or court order. Also known as unrecoverable encryption, it is used to secure both data in transit and data at rest.

Law Enforcement Perspective on Encryption

Over time, encryption has become stronger, more widespread, and easier to use. Major technology companies are increasingly enabling user-side or unrecoverable encryption,[10] such as end-to-end encryption, encryption of smartphone operation systems, as well as default encryption of mobile devices.[11] This has complicated law enforcement investigations, leading to calls to access encrypted information. Intelligence communities have found it increasingly difficult to carry out investigations in an age where the internet is going dark. Law Enforcement Agencies find that encrypted system pose a unique legal challenge when it comes issuing warrants and granting access. Intelligence agencies have consistently asked for a backdoor to encrypted systems in order to solve and prevent a battery of crimes, including child pornography, curbing hate speech and the illegal sales of armaments, to name a few. A key pivot, globally, was the 2016 San Bernardino showdown between the Federal Bureau of Investigation and Apple over access to an encrypted iPhone.[12] The FBI argued that encryption presented a significant barrier to investigation. To overcome this, Apple would have to provide the FBI with the tools to circumvent the encryption. Apple disagreed, highlighting the harmful security implications of creating such a backdoor.

Closer to home, the Indian government persuaded Research-in-Motion (now Blackberry) to provide it access to its encrypted systems, while a slew of incidents caused by the dissemination of misinformation over the

Major technology companies are increasingly enabling user-side or unrecoverable encryption, such as end-to-end encryption, encryption of smartphone operation systems, as well as default encryption of mobile devices. This has complicated law enforcement investigations, leading to calls to access encrypted information.

Internet propelled the government to impose a traceability obligation onto messaging platforms. The traceability requirement is similar to regulatory developments in different countries that obligate companies to develop capabilities to provide law enforcement with on-demand access to information – even when deploying user-side encryption.[13] On the other hand, weakening encryption through such mandates may hurt the privacy of users, weaken security, damage the economic viability of technology companies, and also result in significant economic harm for the nations.[14]

In this context, the key consideration for policymakers in India and across the world is to balance these competing facets of encryption, i.e., privacy, cybersecurity, and national security. This whitepaper attempts to answer some of these questions, with a focus on understanding the impact of encryption and its regulation on law enforcement access to data, cybersecurity and systems architectures, businesses and the digital economy, and civil and fundamental rights.

2

Encryption in India: Regulatory Landscape

Governments across the world have been considering the regulation of encryption for law enforcement and national security purposes.[15] India is no different. Due to the difficulties faced by its security establishment to intercept secure communications using high-level encryption, India is also grappling with the question of balancing the privacy of individuals and making data available for prosecuting or preventing offences.

While India does not have an over-arching law or policy that governs the use and deployment of encryption, it is host to a fragmented regulatory framework that either defines encryption standards or enables access to encrypted information for national security and law enforcement purposes.[16] The Indian Telegraph Act, 1885 (**Telegraph Act**) and Information Technology Act, 2000 (**IT Act**) are the overarching laws that define the use of encryption, and also describe the powers of government agencies to intercept or decrypt communications. Sectoral regulations specify the strength of encryption to ease law enforcement access, secure data and transactions. Simultaneously, India awaits a personal data protection law and national cyber-security policy. Discussions around the legal liability of service providers and platforms have also emerged in the context of encryption[17], while concerns with India's cybersecurity capabilities have exacerbated since a spate of recent attacks on its digital infrastructure.[18] Overall, the legal framework for encryption in India is still a quagmire, which has created an uncertain business and regulatory environment for encryption technologies.

Historical Context

The use of encryption in India to ensure the security of digital communications only picked up over the last 15-20 years. The discourse around cryptography and encryption remained limited to the defence and diplomatic circles.[19] Practically no Indian market for encryption existed in the 1990s.[20] A lack of technical know-how, departmental limitations on the use of encryption, and export restrictions in developed markets such as the United States of America contributed to this underdevelopment.[21]

Yet, the promise of growth in the e-commerce and digital banking sectors fuelled concerns over the lack of an Indian encryption market. At this time, the Central Vigilance Commission reportedly considered making it mandatory for Indian banks and financial institutions to use only domestically developed cryptographic software – possibly in a bid to boost India's encryption market.[22] Similarly, with the use of the Internet increasing in the mid-90s, the Indian government recognized the need to regulate encryption. Triggered in part by the inability of Indian intelligence agencies to intercept encrypted Pakistani communications,

a Kargil Review Committee recommended that India develop its own encryption and decryption capacity for intelligence purposes.[23]

It was not until 1999 that the central government introduced encryption specific regulations for the first time. Instead of framing rules that would support the use of encryption, the Department of Telecommunications (**DoT**) imposed conditions on internet service providers **(ISP(s))** to ensure that no individual, group, or organization uses encryption exceeding a 40-bit key length without prior DoT approval.[24] With the passing of the IT Act in 2000, the use of Public Key Infrastructure (**PKI**) was also endorsed for authenticating digital signatures in online transactions.[25] This was followed by the Reserve Bank of India (**RBI**) and the Securities and Exchange Board of India (**SEBI**) recommending 128-bit Secure Socket Layer (**SSL**) encryption for ensuring secure transactions.[26]

In 2008, the IT Act was amended to empower the central government to prescribe modes and methods for encryption for promoting e-governance and e-commerce.[27] This represented the first nation-wide legal endorsement of encryption. At the same time, the IT Act was also amended to allow the government to prescribe procedures of interception and decryption of encrypted information.[28] Importantly, the government has only issued rules describing the procedure to be followed for interception and decryption.[29] A comprehensive policy regulating and promoting the use of encryption is still awaited, notwithstanding the currently withdrawn National Encryption Policy of 2015 (**NEP**).[30]

Creating legislation around encryption has consistently proven to be a challenge to policymakers. On the one hand, there is the need to consider the legitimate concerns of the law enforcement agencies (**LEA**), while on the other hand, there is a constitutional requirement to protect free speech and thought. With the call for the **NEP** and the new traceability[31] and data localization requirements[32], it seems that the government is pushing to change the legal framework around encryption. Apart from legal considerations, there have also been legislative push to construct backdoors as in the case of Research-in-Motion[33].

Recent legal developments have also brought the conversation around backdoors and traceability to the fore. In 2017, the Indian Supreme Court affirmed the fundamental right to privacy for all Indian citizens and imposed safeguards to assess the validity of restrictions on individuals' informational privacy.[34] At the same time, in the on-going originator traceability case, the Supreme Court is addressing questions regarding the validity and practicality of the legal procedure for decryption, along with the now-in-effect traceability requirement.[35] The constitutionality of the traceability requirement has been separately challenged in the Delhi High Court by WhatsApp and Facebook.[36] Separately, the Personal Data Protection Bill- tabled in Parliament in December 2019- proposes stronger data protections, such as encryption, while simultaneously offering broad exemptions to government agencies.[37] All of which indicates that the state of encryption regulation in India is becoming increasingly obscure, not unlike its western counterparts.[38] One thing is clear, however: as the Indian government seeks to regulate encryption and expand means to access encrypted information, both future and existing regulations will have to heed to the need for encryption in information security and privacy.

Summary of recent cases

Case 1

1. K.S. Puttaswamy v. Union of India (Right to Privacy)

Supreme Court

Brief Description

The Supreme Court recognised the fundamental right to privacy and recognised that it contains, amongst other facets, the right to informational privacy. It further established the standard tests to measure justifiable intrusion into individual right to privacy.

Case 2

2. In Re: Prajwala

Supreme Court

Brief Description

The Supreme Court took cognizance of a letter it received from activists about the circulation of videos depicting sexual violence. It called upon all social media and tech platforms. WhatsApp stated in court that their E2EE technology makes removal technically infeasible.

Case 3

3. Antony Clement Rubin v. Union of India

Madras High Court

Brief Description

The petitioner sought to link social media accounts with Aadhaar IDs. This was rejected, however, the issue of breaking traceability and ensuring E2EE came up. Affidavits by subject matter experts such as Prof. Kamakoti and Prof. M. Prabhakaran were filed on the modalities of breaking encryption to encourage traceability.

Case 4

4. Facebook Inc. v. Antony Clement Rubin

Supreme Court

Brief Description

Facebook and WhatsApp separately sought to transfer the Madras High Court petition at (3) above.

Case 5

5. WhatsApp Inc v. Janani K.

Supreme Court

Brief Description

Facebook and WhatsApp separately sought to transfer the Madras High Court petition at (3) above.

Case 6

6. Omanakuttan v. Union of India

Kerala High Court

Brief Description

Petitioner sought action against WhatsApp for allegedly false claims that cannot trace messages because of E2EE. This case was dismissed.

Case 7, 8, 9, 10, 11

7. **Mahua Moitra v. Union of India**
8. **S.G. Vombatkere v. Union of India**
9. **Internet Freedom Foundation v. Union of India**
10. **Amit Sahni v. Union of India**
11. **Shreya Singhal v. Union of India**

Supreme Court

Brief Description

Several petitions were filed in public interest to challenge the application of Section 69 (1) of the IT Act and the Interception Rules.

Case 12

12. Praveen Arimbrathodiyil v Union of India

Kerala High court

Brief Description

Public interest petition filed to challenge the Intermediary Guidelines 2021 and the traceability requirement. The petitioner says this violates the right to privacy under Article 21.

Case 13

13. WhatsApp LLC v. Union of India

Delhi High Court

Brief Description

Facebook and WhatsApp filed separate writ petitions challenging the validity of the traceability provision under the Intermediary Guidelines 2021.

Encryption and Decryption Laws in India

The encryption and decryption of information is administered under two laws: the Telegraph Act and the IT Act. Beyond this, several sectoral regulations specify encryption conditions in the form of ceiling and floor limits. Broadly, the existing framework can be divided into: (a) laws enabling or supporting encryption; and (b) laws enabling government access to encrypted information.

Laws enabling Encryption

The IT Act emphasises the importance of encryption in ensuring the security of data and IT systems. It encourages the use of encryption technologies to secure e-governance and e-commerce transactions[39] and requires entities managing sensitive data to adopt reasonable security practices.[40] Apart from describing technical standards to encrypt digital signatures,[41] it does not prescribe encryption standards, nor does it explain the conditions for its use. However, encryption standards and limits have been stipulated by various sectoral regulators in India:

Law/Regulator	Supports Encryption	Allows Decryption	Prescribed Standard
IT Act	✓	✓	Not prescribed
UIDAI	✓	X	2048-bit (max)[42]
DoT - Unified License	X	✓	No bulk encryption
RBI	✓	X	128-bit (min)
SEBI	✓	✓	128-bit (max)
MoHFW	✓	X	256-bit (min)
Meghraj GI Cloud	✓	X	128-bit (min)
CII Guidelines	✓	X	Not prescribed
Smart Cities Framework	✓	X	Not prescribed

> **Department of Telecommunications (DoT):** In the past, the DoT required all individuals, groups, and organizations to obtain the government's permission before deploying encryption standards that are higher than 40 bits.[43] However, this requirement was dropped unexpectedly.[44] Now, the Unified License (**UL**), an umbrella license encompassing telecom and internet services, only prohibits the deployment of 'bulk encryption' without setting key-length limits.[45] The government also reserves the right to evaluate any encryption used by the licensee.[46] While the term 'bulk encryption' is undefined, it could be understood to mean stronger, high-level encryption, or encryption deployed on a larger scale. Service providers in the past have attempted to restrict users from using encryption, presumably in a bid to comply with this requirement.[47]

This is concerning for two reasons: first, the possibility of misuse of private information might arise within the service provider or government level; and second, it contradicts other sectoral regulations that mandate the use of stronger encryption.

> **Reserve Bank of India (RBI):** The RBI directs all banks to use a minimum 128-bit encryption standard for maintaining the security of financial transactions.[48] Non-Banking Financial Companies **(NBFC)** rendering mobile financial services are required to put in place end-to-end encryption technology. Where NBFCs use social media platforms, they are required to use encryption to secure transactions and prevent the risk of malware distribution.[49] Additionally, the RBI directs Payment Aggregators and Payment Gateways to deploy and institute data security standards and best practices such as encryption, without prescribing specific standards.[50] In February 2021, the RBI released guidelines on digital payments security controls, which without specifying the parameters of encryption, mandate the use of encryption, multifactor authentication, and other measures to secure payments applications and networks.[51]

> **Securities and Exchange Board of India (SEBI):** India's securities regulator directs regulated entities to use encryption for Internet-enabled securities trading. It prescribes that data in transit should be protected with 128-bit encryption.[52] The cybersecurity and resilience framework applicable to stockbrokers and depository participants mandates the use of industry standard strong encryption algorithms, "wherever encryption is implemented".[53] Similarly, share transfer agents must encrypt data-at-rest and data-in-transit using strong encryption methods.[54]

> **The Ministry of Family Health & Welfare (MoHFW):** The Electronic Health Record Standards **(EHR)** issued by the MoHFW provide that all personally identifiable health data has to be protected at all times from any unauthorised access, particularly during transit. To secure such data, EHR standards prescribe a minimum 256-bit key strength

of encryption.[55] Similarly, the MoHFW also notified the Health Data Management Policy (**HDMP**) under the National Digital Health Mission (**NDHM**). The HDMP sets out minimum standards for securing privacy of health data collected, shared, stored, etc. within the NDHM ecosystem. This includes the implementation of necessary security measures including encryption.[56]

- **The Unique Identification Authority of India (UIDAI):** The UIDAI stipulates a 2048-bit encryption standard for Aadhaar authentication APIs.[57/58] It also recognises that these standards may be revised over time. It provides that industry standards/best practices will be adhered to in absence any such specifications.[59]
- **MeghRaj 'GI Cloud':** To tap into the advantages of cloud computing for the government, the Ministry of Electronics and Information Technology (**MeitY**) launched the GI Cloud initiative MeghRaj. Under MeghRaj, various government departments can procure services offered by empanelled Cloud Service Providers (**CSP**).[60] The empanelment guidelines issued by the MeitY require all CSPs to protect/handle data at rest and in transit by deploying a minimum 128-bit encryption.[61]
- **Critical Information Infrastructure Guidelines:** The Guidelines for Protection of Critical Information Infrastructure (**CII**), 2015 issued by the National Critical Information Infrastructure Protection Centre (**NCIIPC**) require the deployment of strong encryption for the protection of CII data.[62]
- **Smart Cities Model Framework:** The Ministry of Housing and Urban Affairs issued a model framework for setting up smart cities, which prescribes guidelines to preserve the security across different layers in a smart city.[63] It requires the encryption of all of the information that flows through the networks of the smart city. It also requires that the end points of all the devices should be authenticated, and that all the traffic from sensors to servers would be encrypted and secured, among other measures.[64]

Laws enabling Government Access

Several laws, rules, and license conditions obligate service providers to enable government access to protected information. All of these laws bestow broad powers with the law enforcement LEAs to seek assistance from intermediaries, that include requirements to provide information on users, to enable surveillance over them or require intermediaries to decrypt data, where practical.[65] These are explained below:

Law/Policy	Interception	Emergency Requirement	Continuous Monitoring	Decryption (with keys)	Decryption (without keys)	Metadata
Telegraph Act	✓	✓	✓	X	X	✓
Telecom Licenses	✓	✓	✓	✓	◆	X
Sec 69, IT Act	✓	✓	✓	✓	X	X
Sec 69B, IT Act	X	✓	✓	X	X	✓
Intermediary Guidelines, IT Act	X	✓	X	X	X	✓
Criminal Procedure Code	X	X	◆	✓	◆	✓

Yes ✓ | No X | Unclear ◆

> **The Telegraph Act:** This law allows the government to lawfully intercept and monitor communications over post, telegraph/telephone and telecommunication networks.[66] For either the central or state governments to authorise the interception of any communication, two conditions need to be met: there should be a public emergency or an issue of public safety; and the interception is necessary for the sovereignty of India.[67] The Indian Telegraph Rules, 1951 (**Telegraph Rules**) set out the procedural framework for interception, including the process and authority for sanction, review, and length of the interception.[68]

Directions for interception may be issued by the Secretary, Ministry of Home Affairs, or the Secretary in charge of the Home Department of the relevant state government.[69] In emergent or unavoidable cases, the head of the particular intercepting agency may issue directions for interception.[70] A review committee comprising of the Cabinet Secretary, Secretary of Legal Affairs, and the Telecom Secretary is tasked with reviewing if the interception orders are compliant with the Telegraph Rules.[71] The constitutionality of the Telegraph Rules has previously been challenged in the Supreme Court,[72] which resulted in the Court laying down guidelines to reduce privacy violations during wiretaps.[73] However, the Court did not mandate prior judicial review – a prevalent critique of the Telegraph Rules – due to the absence of such a mandate within the text of the Telegraph Act.

> **Section 69, IT Act**: Under this law, central and state government agencies can intercept, monitor, decrypt any

information contained or transmitted through a computer resource.[74] The IT Act considerably widens the government's powers of surveillance and interception, as compared to telephone interceptions under the Telegraph Act.[75] It is not necessary that a condition of public emergency should exist to intercept communications under the IT Act; rather, interception can be authorised for additional grounds like the defence of India and the investigation of any offence. Further, service providers are obligated to provide technical assistance to the intercepting agency.[76]

The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (**Interception Rules**) set out the procedure for decryption of private communications.[77] A decryption order can relate to any information sent to or from a person or class of persons or relate to any subject matter.[78] A review committee – consisting of members only from the executive branch of government – reviews the interception directions.[79] The Interception Rules imitate the procedure described in the Telegraph Rules, to the extent possible.

The Interception Rules also set out the accompanying responsibilities of service providers during this process. Service providers are required to provide technical assistance to enable the government's monitoring, interception, or decryption directions. However, decryption access is defined as allowing LEA access to the maximum possible extent; only when the service provider has control over decryption keys.[80] This can mean that the service provider does not have any obligation to decrypt information unless it is the holder of the decryption key.[81] Although, service providers may be obligated to provide technical assistance (including hardware, software, firmware, storage access) for monitoring and interception purposes, despite not holding the decryption key.[82]

Since the process does not include any judicial oversight, both the Interception Rules and the Telegraph Rules have received strong criticism.[83] The Justice Srikrishna Committee had noted the necessity of judicial review in cases where individuals' privacy is being violated.[84] Further, the fact that these rules are prescribed through subordinate legislation, and are not codified in law, has also been criticized.[85] They may also contravene the tests laid down in Puttaswamy, which requires that a state invasion of privacy should satisfy the tests of legality, legitimate aim, suitability, necessity, and proportionality.[86]

Regardless, it is clear that under the Interception Rules, service providers must provide technical assistance in fulfilling LEA requests for interception to the extent they are capable of. It is unclear what is meant by technical assistance; whether its scope includes obligations to build backdoors or change the architecture of the platform. This is one of the issues that the Supreme Court is inspecting in one of the cases clubbed with the originator traceability case.[87] Regardless, a requirement to build backdoors could fail the necessity and proportionality tests laid down in the Puttaswamy judgment, given the privacy and security concerns, and because LEAs have other less intrusive alternatives to access data (such as legally accessing unencrypted stored data on devices and metadata access).[88]

> **Section 69B, IT Act**: The central government can also authorise any government agency to monitor and collect traffic data for broadly defined cybersecurity purposes.[89] The procedural framework to monitor traffic data like metadata is provided under the Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009. Obligations similar to those under the Interception Rules are placed on service

providers to provide technical assistance for the collection and monitoring of traffic data.[90]

- **Safe Harbour Rules**: The IT Act also places certain conditions and obligations upon service providers to maintain their safe harbour protection.[91] For instance, under the Information Technology (Intermediaries Guidelines) Rules, 2011 requires service providers to provide information or any other assistance to government agencies for a wide range of purposes.[92] The government updated these rules in February 2021 by notifying the Information Technology (Intermediaries Guidelines and Digital Media Ethics) Rules, 2021 (**2021 Intermediaries Guidelines**). These guidelines have expanded the scope of assistance to be provided by social media intermediaries, who are now required to share information for a broad range of purposes, proactively monitor child sexual abuse material (**CSAM**), and enable the tracing of originators of communications.[93] The scope of the traceability requirement is still unclear – for example, it could require platforms to overhaul their platform architecture.[94] According to experts, this requirement will be impossible to implement while maintaining end-to-end encryption (**E2EE**), and could undermine the security and privacy of Indian users.[95] Both civil society and industry stakeholders have also opposed the traceability requirement on grounds of lack of due process, adverse civil rights impacts, regulatory uncertainty, and technological infeasibility.[96] While these guidelines have now been notified, their validity (and that of the traceability requirement) has been challenged in the Delhi High Court.[97]
- **Telecom licenses**: The UL provides the government wide powers to mandate TSPs and ISPs to assist law enforcement in intercepting private communications.[98] While these license conditions do not expressly mandate service providers to provide the government with the means of decryption, the language is sufficiently broad to potentially cover such requests.[99] For instance, licensees are obligated to provide monitoring/interception facilities/ equipment to the government.[100] Licensees must also provide traceability functionality, and must offer their entire networks for continuous monitoring and inspection.[101] This also includes making necessary provisions to install suitable monitoring equipment, software, hardware to enable law enforcement access from a centralised location.[102] This allows for the government to mandate telecom and internet service providers to provide broad access into their systems and other access mechanisms for purposes deemed legitimate.[103] The UL, despite its broad scope, has not been the subject of any judicial or legislative scrutiny.
- **Criminal Procedure Code**: LEAs are also known to use the Criminal Procedure Code (**CrPC**) to gain access to encrypted information such as metadata, stored data, or data at rest.[104] The CrPC authorizes any LEA to request the submission of any document or thing in possession of any person necessary for a criminal investigation.[105] Law enforcement often uses this provision to retrieve the key from the user, or enable access to encrypted information or devices.[106] These provisions lack the process safeguards present under the Telegraph Rules and the Interception Rules.

Policy Proposals

In addition to the existing legal framework, the government is considering proposals to enable traceability, mandate local storage of data, registration of encryption using entities, breaking end-to-end encryption (**E2EE**),[107] and others, to address the technological and jurisdictional issues faced by Indian security agencies.

- **Draft National Encryption Policy, 2015**: In 2015, the Government released a draft NEP that sought to set encryption standards and lay down conditions for decryption

of information by LEAs.[108] The draft NEP required service providers to enter into agreements with the government prior to deploying any encryption technologies. It also proposed registration requirements for encryption products and that users of encryption retain the plaintext of their encrypted communications for 90 days. However, the NEP drew criticism over its focus on only enabling LEA access and reducing encryption standards, which led to its withdrawal.

- **Parliament Committee Report on Child Sexual Abuse Material**: Recently in 2019, an ad-hoc committee of the Rajya Sabha (set up to address issues of relating to CSAM) recommended that LEAs should be allowed to break E2EE in order to trace people responsible for spreading CSAM on online platforms. It also recommended that service providers should be mandated to institute minimum essential technologies to monitor and detect CSAM on their platforms.[109] No action has been taken on these recommendations, yet.
- **National Cyber Security Policy**: In 2013, the erstwhile Ministry of Communication and Information Technology released the National Cyber Security Policy (**NCSP**). While no specific standards for encryption were prescribed, the NCSP encouraged organizations to put in place information security policies and measures to secure the flow of information (in process, storage and transit). At the same time, the NCSP also proposed to create a framework to address security challenges arising out of encrypted services and other technological developments.[110] The government is expected to update the National Cyber Security Strategy in 2021.[111] However, it is premature to assume if it will address issues relating to encryption and LEA access.
- **Personal Data Protection Bill, 2019 (PDP Bill)**: Against the backdrop of several proposals that aim to enable government access to encrypted information, India is proposing to implement a strong data protection law. The PDP Bill recognizes encryption as a security measure to be adopted by organizations processing personal data.[112] Organizations must implement measures such as encryption in accordance with the degree of risk associated with the data processed. At the same time, the PDP Bill grants broad powers to the central government to exempt any government agency from the scope of the Bill.[113] This shows the conflicting proposals within the PDP Bill, which concurrently advocates for the use of encryption while allowing the exemption of government agencies from the scope of the Bill.[114] This concern is compounded by the traceability requirement under the 2021 Intermediary Guidelines, which contradicts the PDP Bill's support of encryption. Moreover, the Bill proposes local storage requirements for sensitive and critical personal data, imposes restrictions[115] on the cross-border transfer of data, and. A key motivation for localisation requirements has been the issues faced by LEAs in accessing information stored abroad. Existing procedures for information sharing under Mutual Legal Assistance Treaties (MLATs) have led to significant delays, and exacerbated LEA concerns about data access- which has partly triggered the push for localization under the Bill.[116]

3 The Traceability Mandate

In India, the encryption debate has recently been concentrated around the issue of traceability, or the ability to track down the originator of a particular communication. The 2021 Intermediaries Guidelines require social media companies- with more than 5 million registered users- to enable traceability of individuals sharing objectionable or illegal content on their platform.[117] Law enforcement agencies have called for traceability as they believe tracking down the originator might lead to apprehending heinous criminals who use the cover of E2EE as a safe harbour for perpetuating crimes. The 2021 guidelines state that if traceability is not enabled, social media companies could be held liable for the objectionable content as publishers.[118] By focusing on traceability rather than decryption, the government is aiming to resolve the tension between law enforcement access to data and data security and privacy[119]. But traceability, and the method of its implementation, may defeat the key promises of encryption. Cybersecurity experts believe that traceability is incompatible with end-to-end encryption, and that any threats to strong encryption will put citizens in danger by compromising their privacy at scale[120]. This raises several questions, including: what is the feasibility and achievability of traceability within E2EE platforms? Is the traceability provision legal? And what are its ramifications on user security and privacy? In this section, we attempt to answer these questions.

In India, the encryption debate has recently been concentrated around the issue of traceability, or the ability to track down the originator of a particular communication. The 2021 Intermediaries Guidelines require social media companies, with more than 5 million registered users, to enable traceability of individuals sharing objectionable or illegal content on their platform.

Legal Challenges

The traceability provision has been challenged in court. In two separate petitions filed in the Delhi High Court, Facebook and WhatsApp have stated that traceability will force them to break E2EE, and, as a consequence, violate people's fundamental right to privacy[121]. According to the Puttaswamy judgement, any invasion of privacy must satisfy a three-part test of: legality, i.e., should be based on an existing law; necessity, so that it protects against arbitrary state action; and proportionality, which ensures a balance between

the outcomes and the harms caused by limiting the right[122]. Experts allege that traceability may fail *Puttaswamy's* three tests:

Legality: The IT Act is the parent law under which the 2021 Intermediaries Guidelines are issued. But, the IT Act does not enable the government to enact rules that require service providers to fundamentally change the architecture of their platform or break end-to-end encryption or implement a technical solution such as traceability[123]. Rather, the 2021 Intermediary Guidelines are issued under provisions that allow the government to block content, and avail safe harbour protections. Experts argue that neither of these allow the government to introduce requirements such as traceability or infringe upon the fundamental right to privacy.[124] As the parent act does not provide any power to infringe user privacy, the introduction of the traceability requirement through delegated legislation does not meet the legality test.[125]

Necessity: There is little evidence to suggest that the government's current surveillance powers and data sources are inadequate. The availability of metadata and the increase in digital forensic tools have arguably increased LEA capabilities to access data[126]. Even if traceability could be operationalised as envisioned by the government, its potential use cases are very limited[127]. On the other hand, traceability would require service providers to make architectural changes that will reduce privacy and security guarantees for Indian citizens, at scale. There are concerns about its effectiveness as well[128]. In light of this, it is unclear how the government will demonstrate how traceability is necessary for it to meet its objectives.[129]

Proportionality: The 2021 Intermediaries Rules require LEAs issuing a traceability order to consider if there are other less invasive methods of obtaining this information. In the government's view, this should meet the proportionality test[130]. But experts argue that the inclusion of this provision, by itself, may not satisfy the proportionality test. This is because traceability would require service providers to build a privacy-invasive mechanism, and then implement at scale for every single user and communication. This is irrespective of whether the user, or the piece of communication, is part of an investigation. Similarly, permanently linking a user's identity with a message jeopardizes anonymity and privacy, and causes a chilling effect on the right to freedom of expression[131]. Service providers would also have to store this information. In addition to violating key data protection principles of data minimisation and storage limitation, this will also open up new surfaces for cybersecurity attacks[132]. All of this infringes a key element of the proportionality criteria, i.e., the violation of a fundamental right must "be through the least restrictive alternatives".[133] Eroding user privacy and security, at scale, is not the least restrictive measure. Overall, critics argue that compliance with the traceability requirement would endanger the fundamental right to privacy for millions, without any because undermining encryption for one would mean doing so for all.[134]

Procedural Safeguards: Experts argue that the traceability mandate will fail the necessity test, as it does not protect users against arbitrary state action. A key component of this test is the safeguard of judicial review, which the traceability requirement does not provide.[135] There is an absence of any parliamentary oversight as well. The framework is alleged to be opaque, which means that affected parties are not able to find out if they are under surveillance or even to challenge the surveillance.[136] Due to lack of any material safeguards against arbitrary state interference, experts also believe that the traceability requirement will not meet this criterion.[137]

The 2021 Intermediaries Guidelines, including the traceability provision, have been separately challenged in the Kerala High Court by the Freedom Software Community of India.[138] The petition alleges that the 2021 Intermediaries Guidelines are unconstitutional, as it undermines E2EE, which is a fundamental subset of the right to privacy.[139] A mandate to remove or disable harmful content, and moderate content under private communications, or enable traceability, on platforms that are end-to-end encrypted will force service providers to dilute strong encryption, and snoop on their users' private communication.[140]

This challenge also raises other concerns about the traceability requirement, and its impact on service providers that do not primarily provide messaging services, which includes free and open source software **(FOSS)** providers, but even platforms like Dunzo or Zomato.[141] As the 2021 Intermediary Rules do not define the meaning of the term "messaging", the scope of these rules remains unclear.[142] Imposing this requirement on these entities, especially FOSS providers, would burden them with substantial financial costs, for which they may not have the finances necessary for compliance.[143]

Conversely, the interpretation of the term "primarily" has appeared inconsistent so far. Apple's iMessage has been reportedly exempted from complying with the traceability requirement, since it does not primarily provide messaging services- in the government's view.[144] According to sources in the government, iMessage is not a standalone messaging platform that can be downloaded on any device, and therefore cannot be considered as an entity separate from Apple, or an entity that "primarily or solely" enables communication.[145] However, this adds to the confusion surrounding the traceability provision, as it appears to exempt an end-to-end messaging platform with a high Indian user-base. Experts believe that this will result in discriminatory and subjective application of the law, leading to a regulatory imbalance and a non-level playing field.[146] This interpretation also appears violative of constitutional principles of equality before law, fair procedure, and natural justice.[147] Effectively, this would mean that iMessage will be the only end-to-end encrypted platform in India, as it does not have to enable traceability.

Technical Considerations

Two methods have been proposed to implement the traceability requirement, while preserving E2EE. First, attaching the originator's identity information as a digital signature to each message, and encrypting it with a key held by the service provider; and second, assigning an alphanumeric hash to each message, and comparing it with the hashes stored by the service provider. Professor Kamakoti, whose assistance was sought in the originator traceability case,[148] proposed the first method, while the representatives at MeitY, recently

appeared to endorse the second technique.[149] These techniques can supposedly achieve traceability without undermining encryption, or specifically, E2EE.[150] Yet, to comply with traceability requirement, these techniques may force service providers to break or dilute end-to-end encryption. It would also considerably weaken the security and privacy of their products.[151] This is explained in greater detail below:

Report on Originator Traceability – Proposal 1 &2: Under this method, when a message is created, the user who creates the message shall be designated as the originator of the message. The user's phone number will be tagged with the message, and this originator information, along with the normally encrypted message, will be bundled together and shared with every recipient of the forwarded message.[152] The originator information of a particular message will be encrypted with a separate private-public key. The service provider will retain access to the private key and share it with LEA when required.[153]

In response, experts have argued that it is impossible to track the originator without undermining E2EE and the privacy and security of end-users.[154] They observe that the proposal is ineffective at meeting its intended outcome of identifying the originator, since provenance breaks any time someone in a chain of forwards downloads and re-uploads a message, takes a screenshot or obtains content from another platform.[155] So it will be hard to establish, beyond reasonable doubt, who the originator is.[156] The proposal may prove to be vulnerable to falsification and abuse, and can lead to the victimization and prosecution of an innocent forwarder who is deemed as the originator because the chain begins with them.[157] Also, private keys, if held by third parties like the service provider, could be vulnerable to hacking by bad actors; and such a method may not be workable across platforms since different platforms and services use different protocols.[158] There are also technical, operational and practical concerns with enabling traceability of over 400-million Indian users, along with ensuring that it only affects Indian users.[159]

Alpha-numeric Hashing: Hashing is the practice of using an algorithm to link information of any size to a fixed value.[160] For example, the message "hello" may have a hash value of "abc123". Using this technique, the service provider attaches an alpha-numeric hash value to each message. It would also have to maintain a database housing the hash values of every single message sent on its platform. On request by a LEA, the service provider would have to compare the value of the transgressing message against its database of hashes, thus providing it (and the LEA) with the originator information. But experts argue that this is an even faultier method.[161] It is a one-way operation, meaning that recovering the original text from its hash is generally considered computationally infeasible.[162]

This is because the protocol underlying leading social media applications often ensures forward secrecy. This ensures that a set of new keys is generated for every message that is sent.[163] It ensures that the end-to-end encrypted platform takes into account the unique identity keys of that particular sender and receiver in addition to the encrypted message itself.[164] For example, A messages "hey" to B, and B forwards "hey" to C. Both messages, while consisting of the same content, will carry a different hash value. So, if LEA shares B's message with the service provider to find out the originator information, it will not reveal A's message to B. Similarly, the hash value of a message can change with the slightest alteration, inhibiting the ability to establish provenance. As an example, the hash value of "hello" and "Hello" would be different.

In addition, messaging applications on end-devices can be easily modified by a motivated individual to attach an incorrect hash.[165] Because the service provider only sees the encrypted version and not the contents of the message, it cannot verify the hash. So, experts argue that there is no feasible method of ensuring appropriate digital attribution that could establish criminal liability.[166] If anything, it heightens the concern that innocent users could be implicated in investigations.

Impact on User Privacy and Security

Beyond its technical implementation, digital rights advocates believe that traceability is also incompatible with privacy, and security, at a fundamental level. This is because it erodes the expectation of privacy and security attached to messages sent on an E2EE platform, by forcing service providers to track messages and store information that can be used to ascertain the content of a user's message.[167] Critically, in order to trace even one message, service providers would have to trace and track every message. It would also create substantial privacy and security risks associated with the infrastructure set up to enable traceability. Service providers will have to move away from privacy-focused engineering and data minimization principles normally characterize secure private messaging platforms.[168] This will also have a chilling effect on the right to freedom of expression and speech.

Traceability also impugns the "off-the-record" deniability **(OTR)** function of the E2EE platforms. Users may naturally expect their conversation to be OTR, so that even if one party publicizes their private conversation, the other party can deny its veracity.[169] Forcing service providers to keep track of who-said-what and who-shared-what data would effectively require the removal of this feature. This would mean a change in the overall design of the product, one which would move service providers away from privacy-focused engineering and data minimization principles that should characterize secure private messaging apps.[170]

The hashing method, in particular, will undermine the expected confidentiality of messages, as it is possible for a resourceful actor to guess the contents of a message from its hash.[171] Bad actors can calculate hashes of combinations of commonly used words and phrases to guess the contents of some messages from just their hashes. This can significantly compromise the service provider's infrastructure. In addition, anyone with the ability to add an item to the hash database can censor or identify any piece of content.[172] This database can be used to identify anyone who has shared a particular content, regardless of their status as an originator of the message.[173] This can turn hashing into a tool of mass surveillance, profiling, and censorship.

Beyond its technical implementation, digital rights advocates believe that traceability is also incompatible with privacy, and security, at a fundamental level. This is because it erodes the expectation of privacy and security attached to messages sent on an E2EE platform, by forcing service providers to track messages and store information that can be used to ascertain the content of a user's message.

On the other hand, originator traceability proposal to attach additional metadata to messages will allow third parties such as the message recipients or the service provider (depending on the variant chosen) to view originator information.[174] This will seriously weaken communication privacy , especially at a time when service providers are trying to minimise the amount of personal data they collect. This proposal to modify system design to collect more metadata than is required weakens privacy guarantees .[175]

There are also concerns that the traceability requirement will compel service providers to access the contents of messages themselves, due to the lack of any effective technical method to comply with the traceability requirement. While the 2021 Intermediaries Guidelines clarify that that no service provider is required to disclose the content of any message, it does not preclude service providers from accessing message content for the purpose of identifying the relevant chain of messages for which it must disclose the originator.[176]

The notion of a "first originator" is not without flaws. A key assumption driving the traceability requirement is that forwarding is the only way a message circulates on a messaging platform. This is not correct. Messages can be downloaded, re-uploaded, altered slightly, re-sent as screenshots, or forwarded on the messaging platform from another service (such as email).[177] At any point, someone might copy and paste the same piece of content and send it along to others in an entirely different circumstance.[178] Each one of these scenarios would start a new messaging chain. So, the originator of each of these chains would be different. From a practical standpoint, it would be onerous or impossible to identify the "first originator" of a message, without accessing the content of E2EE communications.[179] From a security and privacy standpoint, this would mean that the only effective manner to enable traceability would be to break E2EE altogether.[180]

International Experience with Traceability

While it is the first country to impose traceability, India is not the only country to call for it. There is a similar call emerging in Brazil. The Brazilian National Congress is actively considering legislation that would force companies to add a permanent identity stamp to the private messages people send.[181] The objective of this legislation is to address concerns emerging from the spread of fake news. However, similar to the experience in India, this proposal has met with significant opposition due to its potential to harm privacy and freedom and expression.[182]

4

Encryption Regulation in Other Countries

Worldwide, different countries are attempting to balance the trade-off between the privacy enhancing benefits of encryption against the data access obstructions it creates for law enforcement agencies' (LEA). While the basic contours of the debate are similar across the globe, there is little consensus on the approaches adopted by different nations. Countries like Germany have actively supported the use of strong encryption, while instituting procedures to allow state authorities to hack into encrypted systems. The United Kingdom and Australia allow state access to decrypted information for a broad range of purposes, including obligations for intermediaries to provide technical assistance. In China and Russia, intermediaries are subject to strict licensing requirements for deploying encryption, along with having to comply with wide-ranging obligations to provide the government with access to encrypted information.

In this chapter, we have classified these different approaches as: (i) light regulation, i.e., countries that encourage the commercial and widespread use of encryption; (ii) moderate regulation, i.e., nations that allow the commercial use of encryption but with obligations on service providers to provide law enforcement with access to information; and (iii) heavy regulation, i.e., jurisdictions that restrict the commercial use of encryption and impose obligations on service providers to re-architect their systems.

Country	Encryption design mandate	Licensing requirement	Technology-neutral access mandates	Weak encryption mandate	Backdoor mandate	User decryption mandate	Government hacking
Germany	X	X	X	X	X	X	✓
France	✓	X	✓	X	◆	✓	✓
Israel	◆	✓	X	X	◆	X	✓
UK	X	X	✓	◆	◆	✓	✓
USA	X	X	◆	X	X	X	✓
Australia	◆	✓	✓	X	✓	✓	X
Russia	✓	✓	✓	◆	✓	✓	✓
China	✓	✓	✓	◆	✓	✓	✓
India	X	✓	✓	✓	X	✓	◆

Yes ✓	No X	Unclear ◆

Light Regulation of Encryption

Some jurisdictions support the use of strong encryption commercially, and do not impose requirements on service providers to enable LEA access by either weakening encryption, building backdoors, or making changes to their technological architectures.

Germany

Germany has long championed the use of encryption as an important tool for data privacy and security. This position is premised in the country's strong privacy right, along with other fundamental rights, like the right to secrecy of communications, the right of personality, and the right to freedom of expression.[183] Accordingly, Germany does not prohibit the use of encryption, compel service providers to build backdoors, or require mandatory decryption of encrypted data.[184] Instead, the government has encouraged its investigatory agencies to conduct widespread hacking in order to gain access to encrypted information.[185]

The foundation of the German position is found in its first policy on encryption that sets out five 'crypto principles'.[186] Released in 1999, it articulates two key principles: first, that there will be no ban or limitation on encryption; and second, that LEA and security agencies will not be weakened by the use of encryption. 2014's Digital Agenda, a whitepaper on Germany's digital policy, also reiterates these principles and declares Germany's desire to become a global leader in the adoption of encryption.[187] This is also evident from the "security through encryption" and "security despite encryption" framing of the German Cybersecurity Strategy.[188] Many German laws and regulations require the use of encryption, and the government has funded and promoted a number of projects on the development and implementation of encryption such as the national identity card, the e-government mail, and the Smart Meter Gateway.[189]

At the same time, in 2006, Germany introduced amendments to its criminal law to enhance the technical capabilities of law enforcement[190] and security agencies to access encrypted information. These amendments enable the hacking of encrypted systems by law enforcement. Government agencies can engage in lawful hacking under certain conditions, i.e. for investigations that involve danger to life, limitations to freedom, and national security.[191] A court order is required to engage in lawful hacking, while any data that relates to the private life an individual must be deleted immediately.[192] LEAs are also required to notify anyone targeted by lawful hacking.[193]

These mechanisms have also faced criticism due to growing concerns of their unconstitutionality and the potential weakening of IT systems.[194] This has resulted in a constitutional challenge to the hacking provisions, which is currently pending.[195] German courts have previously considered the impact of government hacking on an individual's privacy. The Constitutional Court ruled, in a 2008 case, that hacking into a person's device is disproportionate and unconstitutional unless specific requirements (such as threat to life or the state itself) and safeguards (such as frequent review to prevent violations of privacy) are met.[196] In a 2016 case, the Constitutional Court reinforced these safeguards, while also enquiring about the legal basis for the hacking powers,[197] which led to the amendments mentioned above. Similarly, due to the absence of any framework for a 'vulnerabilities equities process'[198] , there is little information on how law enforcement manages known and unknown security vulnerabilities. Although the creation of a new agency, the Central Authority for Information Technology in the Security Sphere **(ZITiS)**, appears to have a mandate to address these concerns.[199]

United States of America

Since the 1990s, the issue of encryption has been subject to a broad, active and contentious policy debate in the United States. This resulted in the passing of the Communications Assistance for Law Enforcement Act (**CALEA**), which requires telecommunications providers and equipment manufacturers to ensure the possibility of effective wiretapping and interception of communications. However,

there is no legislative power which can be used to require telecommunication or online service providers to facilitate the decryption of encrypted communications.[200]

The United States also has passed regulations that promote and require the use of cryptographic methods.[201] These acts contain security requirements and thereby indirectly require or stimulate the use of encryption in certain circumstances.[202] There are also strong constitutional protections that prevent LEA access to encrypted data. The First Amendment of the US Constitution protects encryption code written by the equipment makers or service providers,[203] while the Fourth Amendment protects citizens from unreasonable search and seizure actions from the state. The Fifth Amendment protections safeguard an individual against self-incrimination.

The Federal Bureau of Investigation **(FBI)** has recently been using federal writ legislation to obtain court orders on service providers to circumvent device access. The famous 'San Bernardino' legal dispute between Apple and the FBI is the best-known example of this new line of cases. At the same time, the US Supreme Court has held that a person cannot be compelled to provide a password or any such information that could lead to self-incrimination.[204] Similarly, despite various LEAs seeking access to encrypted material through backdoors or otherwise, courts in the US have prevented any such access being granted.[205]

However, the United States government has continued its efforts to solve the 'going dark' problem for LEAs. Proposed legislations such as the EARN IT Bill aim to make service providers liable for not implementing 'best practices' such as client-side scanning for the purpose of detecting CSAM.[206] Experts argue that this is veiled attack on E2EE, citing the incompatibility of content scanning systems with E2EE.[207] Similarly, the proposed Lawful Access to Encrypted Data Act would grant government agencies and courts broad powers to order service providers to offer technical assistance to decrypt information.[208]

Israel

Any engagement in encryption, i.e. the development, production, modification, integration, use, purchase of encryption items requires the procurement of a relevant license.[209] The licensing framework is smooth and lenient, and encourages government and private sector collaboration. For instance, under the 'free means' category license, certain types

of encryption are exempt from the licensing requirements.[210] To date, nearly 11,000 products have been designated under this license.[211] Additionally, the government has established an internal use rule that allows an individual person or organization to encrypt data for personal or intra-company purposes without obtaining encryption licenses.[212] There are other broad exceptions that include the work of patent attorneys, exceptions relating to electronic signatures, and exemptions for downloads of online open-source encryption for personal uses, and others.[213]

There is no legal requirement on intermediaries to enable exceptional access or provide technical assistance.[214] In fact, the confidentiality of "conversation, or the writings or records" of an individual cannot be violated under existing law,[215] unless it is a state of emergency. LEAs also require a court warrant to search the device of an individual,[216] a view supported by the Israel Supreme Court in 2017.[217]

Moderate Regulation of Encryption

In October 2020, the 'Five Eyes Alliance'[218] along with India and Japan published a joint statement calling on companies to assist authorities to lawfully access data and embed public safety in their technological architectures.[219] Two of the five eyes, i.e., the United Kingdom and Australia have introduced laws that enable LEA access to decrypted information, by either mandating the sharing of decryption keys, or by mandating the development of capabilities to enable decryption. However, the use of encryption is not restricted, nor is there a mandate to use weak encryption. The situation is analogous in France, where the issue of backdoors has been the subject of ardent legislative debate.

United Kingdom

Since 2000, law enforcement in the United Kingdom can seek access to encrypted material.[220] However, the recent increase in default and end-to-end encrypted systems prompted the UK to pass new regulations that increase the ability of law enforcement to access encrypted information.[221] These changes empower the government to impose technical requirements on broadly defined communication service providers to provide information access. These requirements can be imposed in the form of secretly issued "technical capability notice" or a "national security notice".[222] While the scope of obligations under these notices is unclear, they may require service providers to create and maintain the capability to assist with lawful surveillance, including having the capability to decrypt their users' encrypted communications.[223]

The law is written so broadly that it potentially encompasses the removal or undermining of encryption, building backdoors, or any manner of technical assistance.[224] These concerns have been raised by both private sector and civil society alike, who argue that the new law can be used to undermine or ban encryption, along with requirements to build backdoors.[225] Recent amendments to the law[226] have not provided any clarity.[227] In addition to the power to impose obligations on intermediaries, the government also has bulk interception and bulk encryption removal powers.[228] The government can also engage in legally sanctioned large and small scale investigative hacking of devices.[229]

Australia

Similar to developments in the United Kingdom, Australia has given its law enforcement and intelligence agencies wide-ranging powers to compel service providers[230] to enable access to their encrypted systems.[231] Triggered by the 'going dark' problem posed by E2EE systems, these laws have prompted a seismic shift in Australia's encryption landscape.[232]

Now, authorities can compel technical assistance from service providers by way of:[233]

(i) "Technical assistance requests", which are voluntary request for service providers to use interception or data access capability they already have;[234] or

(ii) "Compulsory assistance notice", where service providers must compulsorily provide assistance based on current capabilities;[235] or

(iii) "Technical capability notice", which would require service providers to build technological capabilities to assist LEA in the future.[236]

Notably, the scope of this assistance can include the removal of electronic protections such as authentication or encryption; providing technical information; installing software or equipment; assisting access to devices; and notifying authorities of any change of technology.[237] However, the law does not mandate service providers to introduce any "systemic vulnerability" or "systemic weakness" within their systems.[238] Although the uncertainty around how these terms are defined, and their implementation in practice, has been a major concern for industry and civil society alike.[239] This promoted a parliamentary committee to seek a report from an independent security watchdog, which identified three key issues with the law: the absence of independent authorisation for assistance notices; unclear definitions; and lack of independent technical scrutiny for assistance notices.[240] It also recommended changes to the law, which have not been acted by the government.[241] The end result is a legislation that is so broad that it can compel service providers to perform any act to enable government access to encrypted information. However, the Australian government is yet to act upon this law.

France

France has expressly recognised a right to encryption.[242] While there is no law that clearly allows the government to force intermediaries to facilitate government access or demand backdoors, there are multiple legal provisions spread across the French criminal and security laws that may be used to compel the disclosure of encryption keys or the decryption of data. However, these provisions may only apply in cases where the service provider has access to the keys.

Under French law, judges have the power to order the disclosure of information that is relevant to an inquiry and necessary for the discovery of the truth.[243] The government also has powers to require any individual or private entity to carry out technical operations in order to obtain plaintext version of the information needed.[244] Importantly, this obligation does not necessarily mandate service providers to build backdoors, and is largely understood to apply onto intermediaries who have access to decryption keys.[245] Similarly, the French Penal Code requires key holders to decrypt information, but only in cases where the relevant entity has access to the keys.[246] Finally, the Internal Security Code[247] gives the Prime Minister the power to order companies to provide data necessary to decipher data (such as decryption keys) and also mandate companies to decrypt the data themselves. However, service providers who receive such requests are allowed to demonstrate their inability to comply, which could presumably be used in cases when the technical design of a product does not enable decryption.

France has also brought regulations that enable hacking by the government for criminal or intelligence investigations.[248] The law also prescribes limits on this power. For instance, LEA must obtain a judicial order prior to undertaking hacking. For hacking by intelligence agencies, prior approval from the Prime Minister is required. However, unlike Germany, hacking is not yet considered a viable alternative method for obtaining encrypted information.[249]

In recent years, there has been a widespread anti-crypto sentiment in both the legislature and the executive branch, fuelled in part by a nationalist disdain for US tech companies and an increasing number of terror attacks.[250] Accordingly, the French Parliament has brought changes to expand the governments surveillance and hacking capabilities, expanded penalties for failure to comply with key disclosure requirements, and created a new mandatory key disclosure and decryption authority for use in intelligence investigations.[251] Despite extensive legislative debate on the issue,[252] France has not yet passed any law that clearly obligates service providers to build backdoors or redesign their system architecture to enable state access.

Strict Regulation of Encryption

Several countries impose strict licensing requirements on service providers who wish to deploy encryption. At the same time, countries like Russia and China also have broad powers to compel service providers to provide LEA with access to encrypted data.

China

The Chinese anti-terrorism law[253] requires service providers to offer technical support and assistance to law enforcement, including decryption, to prevent terrorist activities. In 2019, China passed a specific law applicable to commercial encryption under which all such encryption technologies must adhere to government-stipulated technological requirements, and comply with strict registration, testing and certification norms. In essence, this empowers the government to authorise only those encryption technologies that they are able to access.[254] It also authorizes the Chinese government to impose design mandates on companies seeking to avail certifications.[255] For instance, service providers such as Apple have built specific hardware modules for storing encryption keys in China.[256] These are different to the modules it uses in other countries.

Russia

Service providers in Russia are subject to strict licensing or approval-based requirements for deploying encryption, and at the same time must provide LEA with access to encrypted information. For instance, service providers must obtain a mandatory license before using any encryption facility, maintaining encryption facilities, providing encryption services, and developing and manufacturing encryption facilities protected by means of encryption.[257]

Further, service providers must include additional software and hardware, and create other conditions required by LEA to implement operational and technical measures to enable decryption.[258] This gives Russian agencies sweeping powers to require companies to install backdoors, provide access to keys, and carry out any other technological intervention it deems fit.

5 Key Encryption Debates

The growing popularity of the internet has led to an explosion in online activity and communication, with personal and sensitive personal information increasingly being stored and transmitted online. To protect this information and promote trust in their services, technology companies have increased the deployment of stronger cryptographic techniques. This has fuelled concerns in intelligence and law enforcement communities that their investigative and interception capabilities are 'going dark'.[259] Supposedly, certain encryption architectures inhibit the government's ability to access information.

While this problem could cover a broad range of encryption technologies, the adoption of unrecoverable encryption architecture in the form of default end-to-end encryption services or full disk encryption has become the focal point of this debate. Similarly, many cloud service providers also offer client-side encryption, which allows users to maintain control of the encryption keys.[260] By deploying unrecoverable encryption, even the service provider does not have access to the encryption keys. As a result, the information cannot be intercepted, or accessed, by any third party, let alone law enforcement agencies **(LEA(s))**. This distinction is crucial because a large number of people communicate through Internet platforms like email clients and social media platforms, which do not deploy unrecoverable encryption, but use recoverable encryption. In this scenario, law enforcement can intercept and seek access to protected information held by service providers by triggering the appropriate legal procedure. On the other hand, without access to the keys, companies deploying end-to-end encryption **(E2EE)** or full-disk encryption are incapable of providing law enforcement with the means to access the information.[261]

For this reason, LEAs have been pushing companies to maintain means to enable exceptional access to encrypted information.[262] The private sector, along with civil rights activists, have opposed these calls. Their apprehension stems from the security and privacy risks posed by guaranteeing such access, along with the potential harm to the economic and technological viability of the products and services offered by technology companies.

Against this backdrop, this chapter will identify and connect ongoing domestic and global debates in the encryption universe, with a view to understand the role of service providers in enabling government access to encrypted information. Specifically, this chapter will try to answer:

(a) What is the national security rationale for weakening encryption?

(b) How does the deployment of encryption relate to the protection of human rights?

(c) What are the different methods of gaining access to encrypted information?

(d) Which alternative data access mechanism can preserve privacy and security?

National Security and Law Enforcement Access

During the 'crypto wars' of the 1990s, the governments of the United States and other industrialized countries are said to have attempted to weaken encryption, or compel service providers to provide access to encryption keys.[263] This push was abandoned in 2000 because of pressure from the private sector and political resistance from the European Union.[264] Today, the problem faced by law enforcement is different.

While in the past most commercially available encryption allowed the service provider to decrypt users' data or communications, i.e., recoverable encryption, today many service providers are implementing unrecoverable encryption. Law enforcement argue that this form of encryption is virtually unbreakable, and interferes with their existing powers of investigation and intelligence gathering.[265] The scale and scope of systems dependent on encryption today is also far greater today, along with society's dependence on digital networks. As the importance of digital evidence grows as more of daily life moves online, LEAs are finding it difficult to to access encrypted information.[266] As a result, law enforcement across the world has been calling on technology companies to weaken encryption or provide backdoor access under certain circumstances.[267] In this section, we examine and contextualize the law enforcement and national security rationale to weaken encryption, or to compel service providers to enable access to encrypted data.

Key Arguments of Law Enforcement and Intelligence Agencies

Warrant-proof encryption

This is the scenario in which law enforcement satisfies the established legal processes to obtain information or permission to intercept information, only to find the information they seek is inaccessible due to encryption.[268] As more service providers move towards stronger architectures that utilize longer key-lengths, E2EE, and perfect forward secrecy[269], government agencies fear that existing legal processes for accessing information will become redundant. Even brute force attacks are computationally impossible because of unrecoverable encryption.[270] Perfect forward secrecy also ensures that the keys are automatically changed, which means that even if LEA can access the latest keys, it will only deliver a small portion of the information. In such cases, the data can only be decrypted if the user provides the necessary keys.

Impact on investigation

Unrecoverable encryption is increasingly being offered with products by default, meaning that users do not have to manually turn on encryption. This has led to millions adopting stronger encryption without their active knowledge. LEAs argue that the amount of data encrypted today dwarfs what was encrypted in the past.[271] This has led to an increased use of encryption by bad actors, criminals, and terrorists. According to law enforcement, this enables common crimes, organized crimes, and terrorist activities, and obstructs their ability to conduct investigations and prevent crime.

Authentication and ephemerality

Authentication is a fundamental tenet of encryption. This provides assurance that persons at both ends of the communication are who they say they are. The usage of more robust authentication methods, such as forced-time delays and auto-erasures, also make it harder for LEA to access data.[272] Further, the use of transient messaging that automatically deletes messages from devices and servers after they are viewed, render data inaccessible to LEA, regardless of encryption.

Unrecoverable encryption is good for business

LEAs argue that companies are engineering systems that deny them access to data for

business reasons, rather than to improve security. They believe companies are making these changes so that they will be more competitive abroad when selling to customers who do not want the government to access their data.[273]

National Security Perspective

Law Enforcement and Intelligence communities often find themselves coming up against roadblocks when carrying out investigations in the digital age, especially the problem of going dark. Encryption is often used as a haven by criminals who want to take advantage of the security it awards. LEA are often tasked with the responsibility of unearthing cybercriminals who take shelter behind encrypted systems, which leads to law enforcement requests for backdoors and traceability. Now, while the concerns put forward by law enforcement and security agencies across the world are legitimate, encryption is not a zero-sum game. Which implies that increased privacy (through the form of encryption) necessarily reduces security (from a law enforcement perspective). Rather, privacy and security are mutually reinforcing. For the following reasons, government calls to weaken encryption may be disproportionate to the ends they seek to achieve.

Law Enforcement and Intelligence communities often find themselves coming up against roadblocks when carrying out investigations in the digital age, especially the problem of going dark. Encryption is often used as a haven by criminals who want to take advantage of the security it awards. LEA are often tasked with the responsibility of unearthing cybercriminals who take shelter behind encrypted systems, which leads to law enforcement requests for backdoors and traceability.

First, there is no conclusive empirical analysis that suggests that unrecoverable encryption is significantly preventing law enforcement agencies from solving cases.[274] The data available on the effect on encryption is limited. For example, data from the United States suggests that encryption has not had a notable impact on hampering wiretaps or unlocking phones.[275] A study conducted by Europol also supports this point, and indicates that LEAs do not primarily seek access to the content of encrypted information for investigations.[276] In fact, LEAs cited short retention periods, the lengths of MLAT processes, and difficulty in understanding the processes of sending requests as bigger barriers to investigations, rather than encryption.[277] Second, criminal actors always have the option of using open source encryption tools, creating their own strong encryption software, or using foreign encryption products.[278] For instance, ISIS was using TrueCrypt, a widely available encryption software, to improve its operational security and evade the scrutiny of law enforcement agencies.[279] Third, accessing encrypted data is not the only way for LEA to fight crime and protect national security. Law enforcement have access to a wide variety of information sources to conduct investigations. This includes metadata sources, which comprises of information crucial for the purposes of investigation, such as location data from cell phones and other devices, telephone calling records, header information in e-mail, and so on. This information provides an enormous amount of surveillance data that was unavailable before.[280] With the growth and impending ubiquity of networked sensors and the Internet of Things **(IoT)**, the sources for LEAs are only bound to increase.

Moreover, the argument that encryption curtails the long-standing ability of LEA to access data, even encrypted data, might be worth a relook. There has always been certain kinds of information that LEA has been unable to access. For instance, from the 1970s to 1990s, LEAs had no practical way to access data encrypted with the Data Encryption Standard **(DES)**, since

no third party controlled the keys.[281] While the proliferation of unrecoverable encryption may have given government agencies reason to compel service providers to share encrypted data, the problem of 'going dark' is not new.

The ubiquity of unrecoverable encryption is also questionable. End-to-end encryption and similar technologies are unlikely to be adopted pervasively by companies. This is because the majority of businesses that provide communications services rely on access to user data for revenue streams and product functionality, including for providing targeted advertisements or for user data recovery.[282]

Encryption and Human Rights

Encryption is inextricably linked to the protection of human rights.[283] The security and reliability provided by encryption facilitates the right to privacy and anonymity, the right to free speech and expression, and the right to free association and assembly. Encryption protects the security interests of all individuals, and in extension, facilitates the exercise of key civil rights as well as protecting privacy. From this perspective, encryption is vital for a free and open internet.[284] Attempts at weakening encryption or mandating backdoors could arguably undermine these protections, if they are not subject to appropriate safeguards.[285] In this section, we examine the implications of weakening or bypassing encryption on fundamental human rights and civil liberties.

Encryption and the right to privacy

The right to privacy as recognised by the Indian Supreme Court includes within its scope, the right to individuals to control their private and confidential communication.[286] It is also often understood as a gateway right for the enjoyment of other rights and freedoms, such as the freedom of speech and expression.[287] In order for individuals to exercise their right to privacy, they should be in a position to make certain that their communications remain private and secure.[288] By guaranteeing the security and confidentiality of communication, encryption can facilitate the ability of individuals to exchange ideas and information freely and privately.[289] This can, in turn, safeguard the integrity of intellectual activity and the development of innovative ideas.[290]

The privacy and security of encrypted communication also reduces the chilling effect that may impede the free flow of ideas and speech.[291] In order to exercise freedom of speech, users must be able to maintain privacy so that they are protected from retaliation for expressing lawful but unpopular opinions.[292] Diluting strong encryption undermines the privacy of users of encrypted platforms, which can have a chilling effect on lawful speech.

The privacy and security of encrypted communication also reduces the chilling effect that may impede the free flow of ideas and speech.

Specific individuals, such as journalists, activists, whistle-blowers, would be more vulnerable to adverse actions for sending messages that are critical of the government, or other powerful organizations and individuals.

This is especially true in the context of the government demands to bypass or weaken encryption, such as the traceability requirement. The United Nations Special Rapporteurs on freedom of expression, privacy, and freedom of assembly highlighted the human rights concerns associated with the 2021 Intermediaries Guidelines. In a letter to the Indian government, they argued that the traceability requirement curtailed the right to freedom of expression, and the right to privacy which is ensured through encryption.[293]

Encryption and civil liberties

Encryption can also ensure protection against adverse government action. Substantive and due process requirements that introduce friction within the criminal investigation and prosecution framework help protect civil liberties,[294] such

as the constitutionally guaranteed right against self-incrimination.[295] This is important today, especially when the surveillance capabilities of LEAs are expanding.[296] Encryption similarly increases the transaction costs for law enforcement agencies to access personal communication and information, which forces them to allocate their resources efficiently and prevents over-zealous mass surveillance.[297]

Encryption and digital security

Encryption is not simply a tool used by criminals. It helps keep data secure and communications private and protects users from fraud.[298] It has significant value for journalists, human rights defenders, businesses, financial and banking services, and ordinary citizens by helping them safeguard their digital communication and reducing the risk of data breaches.[299]

Encryption is not simply a tool used by criminals. It helps keep data secure and communications private and protects users from fraud.

As a security tool, encryption helps maintain message confidentiality, ensuring that the encrypted message can only be read by the intended recipient, who has the key. It also helps authenticate the identity of the sender, to confirm that the sender is who she says she is and allow the recipient to trust the source of the message. Finally, encryption helps maintain the integrity of the message, such that it is not modified or manipulated in transit.[300] Authenticated encryption as a practice, enhances the security of all actors.[301]

Even governments benefit from the use of stronger encryption. This assists in the protection and confidentiality of national secrets and sensitive information.[302] Individuals use encryption to communicate with each other without fear of surveillance, and to keep key aspects of their digital lives stored on their device private.[303] At the same time, encryption helps businesses by reducing the risk of cybercrime, which costs the global economy an estimated $400 billion a year,[304] and by keeping their commercial proprietary information secure. Trust in the security of information (whether personal or commercial data) is necessary for business innovation and economic growth.[305]

Encryption plays an important role in securing the information society, which forms the basis of the digital economy today.[306] This is evident in the data governance legislations of different jurisdictions. For instance, the European Union's General Data Protection Regulation **(GDPR)** explicitly recognises encryption as an appropriate technical and organisational measure to process personal data securely,[307] while the Indian Personal Data Protection Bill, 2019, **(PDP Bill)** also recognises encryption as an adequate security safeguard measure[308].

Service providers and human rights

The absence of safeguards in frameworks that limit encryption and its security properties, either by enabling access through backdoors or demanding technical assistance from intermediaries, can trigger human rights related harms. When LEAs mandate service providers to share data in human rights sensitive cases, there is the risk of a diffusion or obfuscation of responsibility.[309] This can also result in unaccounted gag orders on service providers. For instance, decryption orders under the Indian Information Technology Act, 2000, **(IT Act)** often prevent service providers from informing the individual about this interception.

The absence of safeguards in frameworks that limit encryption and its security properties, either by enabling access through backdoors or demanding technical assistance from intermediaries, can trigger human rights related harms.

Similarly, the role of service providers and the legal framework they are subject to must be understood from the perspective of human rights. Especially in the context of cloud-based applications, users depend on the service provider for the protection of their fundamental rights.[310] Specifically, service providers not only have the role of intermediaries in relation to content and connecting users, but also one of security intermediaries, as their practices and defaults as regards encryption are highly relevant to the user's access to and effective usage of those technologies.[311] As security intermediaries, these companies are an important interface between governments and users. The encryption practices of these companies are highly relevant to the user's access to and usage of these technologies that facilitate the enjoyment of fundamental free speech, expression, confidentiality, and privacy rights.

Methods of gaining access to Encrypted Information

The intensification of the 'growing dark' debate has increased calls for security agencies to access encrypted information, either by compelling service providers to weaken encryption, or build backdoors, or through other data access mechanisms. There are multiple methods that governments can use to gain access to encrypted information. Some of these result in breaking encryption, some bypass it, and some methods involve gaining access to the keys. Each method carries with it a varying level of security risk. Overall, these methods increase the complexity of system architectures, which in turn can create unforeseen vulnerabilities. Making it easier for law enforcement to access encrypted communication might make it easier for others to do the same. In this section, we examine the security risks posed by different data access methods.

Method 1

Traceability[312]

Government benefit

Allows the government to identify the originator of a particular communication.

Security risk

Breaks end-to-end encryption, and its implementation will be imperfect, and will create significant security vulnerabilities.

Method 2

Backdoors

Government benefit

Compelling service providers to install backdoors can allow LEA and state agencies to circumvent encryption, often without notifying the user.

Security risk

If backdoors are discovered by malicious actors, they can exploit these vulnerabilities.

Method 3

Key escrow

Government benefit

Allows the state agencies to unlock encrypted information by forcing companies, or a neutral third party, or the government itself to store an extra key to all encrypted data.

Method 3

Security risk

Exposes businesses and consumers to additional risks from security breaches by creating "honeypots", and prevents usage of security features such as perfect forward secrecy.

Method 4

Weak encryption

Government benefit

Allows the LEA to develop in-house capabilities use secretly access encrypted information.

Security risk

Weakening encryption standards weakens encryption products that use those standards, allowing bad actors to also exploit vulnerabilities for access.

Method 5

Government hacking

Government benefit

Allows the government to hack into products or services without help from service providers.

Security risk

Creates new vulnerabilities which other attackers could exploit.

Method 6

Ghost protocol

Government benefit

Allows the government to secretly "sit-in" on end-to-end encrypted conversations.

Security risk

Precludes authenticated encryption; a key component of end-to-end encrypted systems.

Method 7

Client-side scanning

Government benefit

Compels the service provider to scan illegal content on the user's end-device.

Security risk

Defeats the privacy and security guarantees of E2EE and can become a tool for mass surveillance and censorship.

Backdoors

Law enforcement may compel intermediaries to build backdoors into their systems for direct access or by surreptitiously installing them on end-devices. For example, the Snowden revelations revealed that the NSA intercepted routers, servers, and networking equipment made by Cisco while the equipment was in transit so it could secretly insert backdoor surveillance tools without the company's knowledge.[313] These backdoors provide LEA extraordinary access to a secure product—whether it is through hardware (e.g., a physical access port) or software (e.g., code in a computer program). However, just as Google's database of targets under surveillance by US agencies was hacked by Chinese agents,[314] any backdoors created by intermediaries for law enforcement will also be susceptible to similar attacks.

If a backdoor is discovered by bad actors, they can exploit these vulnerabilities, which can create immense security risks. Backdoors have generally been found to create an additional attack surface because the code that will be written to create the backdoor must have unfettered access to the data.

If a backdoor is discovered by bad actors, they can exploit these vulnerabilities, which can create immense security risks. Backdoors have generally been found to create an additional attack surface because the code that will be written to create the backdoor must have unfettered access to the data.[315] Adding code also increases the risk of more bugs in the code that could make the system vulnerable to attack.[316] Researchers believe that when backdoors are required for intercepting communication, such as intercepting end-to-end encrypted conversations, the service provider needs momentary access to unencrypted communications.[317] This momentary access provides an opportunity to attackers to access data that they would be unlikely to reach in the absence of such backdoor codes. Moreover, a backdoor created only for law enforcement agencies can also be exploited by foreign governments and bad actors.

The Federal Bureau of Investigation **(FBI)** famously sought a backdoor from Apple in the San Bernardino shooting case. The FBI procured a court order requiring Apple to create and implement code that would disable security

features which would prevent successive password attempts and delete encrypted user data after ten failed attempts.[318] As stated in the amicus brief submitted by an independent company in the same case,[319] such a backdoor would compromise the overall security architecture of end-devices. Since backdoors are a code that provides access to decrypted data, it is only a matter of discovering that code through brute force attacks or any other vulnerability.

Further, providing backdoors for LEAs to access encrypted communication, and requiring intermediaries to maintain confidentiality about such access, will undermine the trust that consumers repose in technology products.[320] This may make them wary of security updates that are regularly pushed by tech companies to fix bugs on the platform.

Key escrow

Governments can also require key-recovery mechanisms, known as key escrow. In this system, the service provider is required to produce a second key, in addition to the original key, which is stored in an escrow. Law enforcement can use this key when it wants to intercept encrypted data or gain access to a device. The United States government in 2015 considered a system whereby a software is designed to create an extra key for a third party (the company or the government).[321] This key could be available in an escrow that would be made accessible upon a court order.

But key escrow is a flawed technology, and its adoption by one nation can inspire others to use it as well. This can create several negative results. This is because it creates a complex process framework with many stages, including obtaining a court order, authenticating it, finding the correct data, locating the correct key, and retrieving the data. Each one of these steps could be subject to attacks from bad actors. Creating a separate key for law enforcement agencies also creates a concentrated target described as a honey pot, which will more likely attract attention from bad actors.[322] Further, sharing an encryption key with a third party only creates an extra point of attack that can be exploited.

A key escrow mechanism also harms forward secrecy, which is a system that uses different keys to encrypt and decrypt shared information.[323] With the establishment of key escrows, it will be impossible to have this form of forward secrecy that protects information at every stage.

Moreover, key escrows may be technically infeasible in the context of unrecoverable encryption. For instance, using key escrow in E2EE implies that a master public key has to be generated by the third party escrow to decrypt data, which is encrypted using a symmetric key.[324] However, this involves altering every protocol in the encryption system, which may be infeasible, and would also create significant security vulnerabilities.[325] Similarly, ensuring a secure authentication process for decrypting end-devices, expensive and infeasible changes to the security hardware or software would be required.[326] There is also a high risk that a user's private key could get compromised, thereby permanently compromising all secured data.[327]

Overall, experts believe that security vulnerabilities would necessarily arise in the development of any key escrow system, as is evident from the experience of the Clipper Chip from the 1990s.[328] The United States government had introduced the Clipper Chip, a plan for building a key escrow system into communications technologies. However, this plan was halted, due to the discovery of a major security flaw that could allow a malicious third party to tamper with the device. [329]

Weakening encryption

Governments can weaken national standards for encryption, with the goal of limiting the strength of the encryption products and services. This is a straightforward mechanism through which governments seek access to encrypted data by prohibiting excessively strong encryption systems and mandating that all encryption providers offer only government-approved technologies.

For instance, China requires all encryption that affects national security to abide by strict testing and certification frameworks.[330] Similarly, Russian law requires products and services to be submitted for evaluation, where they may be

mandated to install hardware or software for government surveillance.[331] Even in the United States, intelligence agencies have weakened the encryption strength of standards such National Bureau of Standards' Data Encryption Standard.[332] In India, the withdrawn National Encryption Policy, 2015, proposed weakening encryption standards, along with a registration and approval regime for entities deploying encryption.[333]

This results in an overall reduction in the encryption standards of all the software and hardware in use within a particular country. There are countless instances of encrypted software being exposed to vulnerabilities without any such legal requirement to begin with.[334] In addition, no code is perfectly written, and it is those parts of the code that are targeted by attackers. When developers have the liberty to improve upon their previous program and a product passes through its development lifecycles, it will be less prone to attacks. If government-mandated requirements deliberately suppress this process and require the software to remain at a particular level of encryption, it makes the system more vulnerable to attack.[335]

Client-side scanning

Client-side scanning tools have been proposed as a measure to arrest the proliferation of child sexual abuse material **(CSAM)** on messaging and social media platforms. In essence, client-side scanning is a technology that scans images on the user's device before it is sent.[336] Software on the device will compare the hash of the image to a database of such hashes of known objectionable content. If a match is detected, the software on the user's device may prevent sharing of such content and could also report it to the authorities. This will typically involve the software communicating with the database, most likely on a remote server.[337] In India, the 2021 Intermediaries Guidelines require significant social media companies to "endeavor" to integrate scanning systems in their products, while the EARN IT Bill in the United States aims to make service providers liable for CSAM, unless they incorporate scanning.[338] The '5 eyes' also asked Facebook to not implement end-to-end encryption (E2EE) because it would hinder CSAM filtering.[339]

The primary risk is that client-side scanning increases the attack surface available for attackers.[340] Information being shared between the device and the server in this process is vulnerable when in transit. Additionally, the hash database itself may be a target. There is also a possibility of attackers adding hashes to this database and finding a way of monitoring certain types of user content being shared,[341] or by creating willful blind spots in the database. Similarly, these systems cannot be technically limited to only catch CSAM, as anyone with the ability to add an item to the hash database can require the client to block any image of their choice.[342] This is also problematic from a censorship standpoint, as any government or service provider can add the hash of an unwanted content to the database and surveil individuals sending that content or blocking its transmission.[343]

Experts also argue that client-scanning systems, although well-intentioned, can become tools of mass surveillance.[344] Which makes them incompatible with E2EE.[345] Client-side scanning necessarily introduces another entity that has access to the contents of messages (in whatever form) being shared. Exposing the hashes to the service provider can allow it to infer the contents of the message. This effectively would grant the service provider with direct access to effectively decrypt a significant portion of messages[346].

Ghost protocol

Proposed by the United Kingdoms' Government Communications Headquarters (GCHQ), the 'ghost protocol' requires the introduction of a law enforcement account on the device of the person being surveilled, or in the communication channel, who will have access to the information being shared. According to the GCHQ, the fundamental nature of the encryption would remain untouched under this mechanism, while also allowing them access to information in specific scenarios.[347]

At the outset, this either involves a lack of transparency about how the system works, i.e., individuals are not aware of the secret presence of another person, or a circumvention of the disclosed communication protocol by hiding the new addition. This mechanism requires service providers to give access to an outsider to participate in the conversation. While the aim would be to restrict such participation to LEAs alone, the protocol requires a change in software on part of the service provider. Thus, the threat of such attackers being able to participate due to this change in software cannot be ruled out.[348]

Notably, it will require service providers to alter their authentication mechanisms, i.e., the checking of codes to ensure that the conversation is between the expected users. This alteration will increase the scope for error because how encryption keys operate will have to be amended to allow LEA access.[349] Security and privacy experts have rebuked the assertion of the proposal that it does not weaken the encryption.[350] According to them this not only affects the fundamental trust between a service provider and its users, it is also akin to introducing a wiretap in every single user's application or device.[351] They further argued that introducing a ghost key is similar to introducing a backdoor that significantly weakens the security of the application.

Alternative Approaches for Enabling State Access to Encrypted Information

Weakening, breaking, or by-passing encryption is not the only means for law enforcement to access data. There are several alternative approaches that can offer better security and privacy benefits.

Ethical hacking

Ethical hacking is the hacking of systems or networks for the purpose of discovering vulnerabilities and assessing the strength of security of the systems or networks.[352] It is generally used by business organizations and companies to identify loopholes in the security of their systems and networks. For this, organizations generally hire third party ethical hackers or information security professionals to access the organization's system or network.[353] Ethical hacking usually helps in identifying: vulnerabilities which may expose sensitive information such as health or financial information or passwords; broken authentication process on a web application; security misconfigurations in

an organizations system; and injection attacks through which an attacker can inject unwanted input into a system.[354]

Ethical hacking has also gained popularity as an alternative to breaking encryption or mandating backdoor access for law enforcement agencies.[355] Germany, a country that has long favoured and supported encryption, was the first to allow lawful hacking as an alternative to breaking encryption.[356] France[357] and the United Kingdom[358] also have an institutionalized framework for ethical hacking, while LEAs in the US appear to have normalized the practice.[359]

However, several risks are associated with ethical hacking. For instance, hacking by law enforcement could weaken the security and leave the entire system or networks vulnerable to malicious attacks.[360] Ineffective hacking can also lead to security gaps in the systems or networks and potential data breach or leak. Further, not all governments consider balancing vulnerabilities and equities. On several occasions, governments have refrained from disclosing vulnerabilities to vendors resulting in severe losses.[361] The lack of appropriate legal frameworks that would regulate hacking by government and law enforcement agencies also add to concerns, while ethical hacking can also can result in lawsuits for disclosure of confidential information or data breaches.[362] Hacking tools have also been used for a wide variety of purposes, that extend beyond the serious crimes of terrorism and child abuse typically highlighted by LEAs.[363] In fact, a report highlighted the widespread use of hacking tools by American LEAs for relatively routine crimes like "graffiti, shoplifting, vandalism, petty theft, parole violations" and others.[364]

There are also concerns that ethical hacking may be used by governments to target journalists and activists.[365] The Pegasus scandal typifies these concerns.[366] Although the Indian government has denied its alleged involvement or usage of Pegasus spyware,[367] this has brought into focus the core issue of lack of an appropriate framework governing the use of hacking tools in India. And more broadly, it underscores the need for meaningful surveillance reform.[368] Currently, surveillance is ordered and overseen by different layers of the executive alone, for broadly defined purposes, with the complete absence of judicial oversight.[369] There are no mechanisms for appeal, or for surveillance targets to know that they are under surveillance. Similarly, there are no provisions that ensure the accountability of the government department, or any measures that bring transparency to the surveillance process.[370]

Private sector collaboration

Governments and intelligence agencies often state that they do not have access to necessary data due to the digital infrastructure being controlled by private entities. However, there are several instances of private sector collaboration and public-private partnerships. For instance, in the years following the '9/11' terror attacks, several internet service providers collaborated with the US security agencies to provide access to significant amounts of internet traffic.[371]

There are also several initiatives to enable data sharing and coordination between law enforcement and global technology companies and civil society. For instance, at the EU Internet Forum, several social media and technology companies took part in a discussion to understand how to make use of their products, services, tools, and mechanisms to better terror-threat responses.[372] International policing organizations such as the Europol and the Interpol are also collaborating with technology companies and service providers to exchange information. For instance, in 2019, more than 400 experts from law enforcement, private sector and academia came together at Europol's headquarters to exchange expertise, resources and insights on cybercrime.[373] There is a lot of engagement and collaboration between private sector, academic and law enforcement, which can be a viable alternative to weakening encryption.

Alternative data sources

Instead of it being an age of law enforcement 'going dark', experts have argued that this is a golden age of surveillance.[374] Law enforcement agencies already have access to unprecedented amount of information. The number of

components that collect valuable individual data have significantly grown, and includes valuable troves of metadata, and data derived from IoT sensors. It is easy to access location information, telephone records, information about contacts and confederates and new digital databases on individuals' lives.[375] Moreover, a large part of this data is not encrypted, such as web-based services, webmail, instant message and social networking websites.[376] Law enforcement agencies also have far greater surveillance capabilities than before,[377] giving them additional means of accessing unencrypted information. This is exemplified by the FBI's success in running an secure encrypted communications platform, but marketed to criminals.[378] The FBI attached a master key to every message sent on this platform, which allowed it to decrypt and store these messages.This yielded over 800 arrests in 90 countries. Again, this raises serious questions over the characterization of encryption as a serious impediment to the activities of LEAs.[379] Instead, this appears to undercut the longstanding belief that encryption derails investigations. While the concerns of LEAs and governments remain valid, recent trends indicate that the specific losses may be offset by other, sizable, gains.

6

Encryption and the Digital Economy

As India moves towards its objective of creating a 5 trillion-dollar economy, the role of the digital and IT sector will be critical. This contribution will not only be confined to the IT sector; sectors like retail, manufacturing, service, will also benefit from Internet-based processing and software services.[380] If the digital economy is to be a key driver for nation-wide economic growth, then the security mechanisms that underpin its functioning will invariably play an important part. In this context, supporting the use of security and privacy enhancing technologies like encryption is imperative. In the absence of a digital infrastructure secured by encryption, the financial, health, and personal data of Indians would be exposed to risk.

While the non-economic benefits of encryption are well researched,[381] the economic benefits of encryption are lesser known.[382] Several key sectors in the digital economy, such as online banking and financial transactions, e-commerce, ICT security, social media, cloud services, and others, have seen strong growth over the past quarter century. While it is not possible to attribute specific figures to the use of secure encryption, it is unlikely that these sectors would have boomed as they did without the security assurance that encryption provides.[383] At the same time, the Indian economy would also weaken without the use of secure encryption, to the detriment of users, businesses, and also government.[384] In this chapter, we will examine the contribution of encryption in the growth of the digital economy in India. Specifically, we will evaluate the role of encryption in:

i. Enhancing trust in digital products and services;

ii. Enabling innovation;

iii. Delivering critical services and products; and

iv. Ensuring protection of public sector infrastructure.

Creating Trust in the Digital Economy

The Internet has been a significant driver of the Indian economy. Advances in cloud technology have made it easier for businesses to get access to applications and technology on-demand, dramatically reducing the cost of entry into markets, especially for small and medium enterprises **(SMEs)**.[385] Similarly, because of the proliferation of digital payments, most transactions are now conducted online – from grocery purchases to bigger payments.

Covid-19 has only accelerated the process of shifting businesses and day-to-day activities online. The entire digital economy is now dependent on the Internet, with businesses, individuals, and communities increasingly connected with each other. However, even as the

usage of Internet-based services is increasing, the confidence and trust in Internet security continues to drop.[386]

Without trust, the future of India's digital economy and its limitless potential is threatened. The absence of an appropriate and resilient security apparatus can have serious, cascading effects. For example, the average cost of a data breach in 2020 was USD 2.6 million, per breach.[387] The NotPetya cyberattack of 2017 by itself cost the subject of the attack (Maersk) more than USD 300 million, and the damages to all other companies affected totalled more than USD 10 billion.[388] Particularly for Indian businesses, the average cost of a data breach was USD 2 million, an increase of 9.4% from 2019.[389] Apart from the monetary costs, it took businesses an average of 211 days to identify and contain the breach.[390] With the constant threat of data breach and violations, and the lack of adequate safeguards against them, the trust of the consumers and businesses in digital economy is slowly eroding.[391] The need to check this trend, and not compound it, has never been greater- especially as India continues its economic recovery from the Covid-19 pandemic.

Costs of undermining Encryption

Under this context, the imposition of state-sanctioned requirements to weaken encryption, either through building backdoors, or implementing measures such as traceability, can result in significant economic harm.[392] A study conducted on the impact of the recent amendments to Australia's encryption laws, suggests that this harm may be measurable in multiple billions of dollars.[393] There are numerous reasons because of which mandates to weaken encryption would result in this harm.

A study conducted on the impact of the recent amendments to Australia's encryption laws, suggests that this harm may be measurable in multiple billions of dollars.

First, these mandates increase business uncertainty, in the context of digital security. Service providers, in most cases, will be forced to re-architect their platforms on the basis of the specific design mandate. On the contrary, regulations that reduce uncertainty about digital security result in benefits worth billions of dollars.[394] Second, by compromising the digital security of their products and services, these mandates can harm the brand image and reputations of service providers. Both enterprise and retail customers would be concerned about the security of their data and may consequently take their business elsewhere. This can stifle local technology industries and tarnish their reputation internationally, both of which are detrimental to the economy.[395]

Third, a traceability mandate, or any other backdoor mandate, would erode trust in digital services, and the broader digital economy. Reduced trust in the digital economy will depress demand across the economy and induce service providers to induce higher costs to offset the consequent harms.[396] An absence of trust will harm competition the digital economy, as users will be less inclined to sign up for competing services.[397] This weakens the economic power of encryption and also a nation's ability to create jobs. It can also force global companies to leave such country, due to unfavourable legal and business environments.

Encryption as an enabler of Digital Trust

There is, therefore, an immediate need to strengthen and secure India's digital economy. This can be achieved by putting in place measures to protect data and digital transactions through the use of encryption.[398] Encryption ensures security and integrity of data stored on computer systems as well as data transmitted through a network.[399] For instance, in 2018, Telefonica, one of the largest telecommunications companies in

the world, suffered a data breach that exposed the identity, payment and contact information of millions of customers.[400] Had this data been encrypted, any leaked information would have been in an unintelligible format, rendering it futile for hackers or adversarial parties.[401]

Encryption, therefore, plays a positive and critical role in ensuring that the digital infrastructure underpinning the entire communications and information technology ecosystem is secure.[402] This further enhances the trust of businesses and consumers in the digital economy, as they are assured of the security and integrity of their data.[403]

Encryption Enables Innovation

At a time when security breaches and cyber-attacks are rampant, encryption does not only protect against losses and harms, but also enables innovation across different sectors. In an environment of accelerated digital transformation, and adoption of new products and supply chains, there is an increase in the level of cyber risk. This is due to the use of newer, less tested, processes and technologies.[404] However, encryption is designed to enable innovation by protecting the data and systems of companies developing such new products. Encryption is a pillar of business growth. Companies using stronger encryption will be better equipped for long-term success and obtaining customer trust. In this section, we discuss the role of encryption as a key enabler of innovation.

Allows scaling

Strong security programmes based on high-level encryption enable businesses to adapt to rapidly changing markets, focus on innovation, provide trusted system architectures and support agile practices. Perhaps more importantly, encryption provides strong security that can support the entire digital infrastructure of businesses and to help them grow, and add innovative functionalities to their products.[405] This can especially give emerging start-ups the necessary push to grow their business without worrying about data breaches and the ensuing costs.[406]

Strong security programmes based on high-level encryption enable businesses to adapt to rapidly changing markets, focus on innovation, provide trusted system architectures and support agile practices.

Encryption also plays a key role in protecting businesses from reputation loss.[407] In fact, strong security programs can be used to build a brand value based on the principles of greater security, privacy, and trust. For example, because it is an end-to-end encrypted platform, certain social media applications have successfully marketed themselves as entities that provide enhanced security.

Adopting encryption also increases the competitiveness of companies, since they will be able to offer secure technologies to their customers, in addition to securing their own data. Moreover, in a competitive digital market, businesses with futuristic technologies which can provide information security have an edge over those who do not.[408]

Enables digital transformation

A smart security and privacy approach can be an accelerator of digital transformation of enterprises. SMEs and start-ups especially stand to gain a lot from moving their businesses online in terms of productivity, better customer engagement, and retention of competitive edge. A lot of these businesses leverage expanded infrastructures based on cloud computing and IoT creating a network within which data is created, shared, and stored. However, the inter-connected nature of technology-driven operations and the pace of digital transformation mean that cyberattacks can have far more extensive effects than ever before, and businesses and their supply networks may not be prepared for the risks.[409] To keep networks and data safe, companies are increasingly adopting encryption across their cloud infrastructure. Especially in key sectors such as e-commerce, retail, and manufacturing, ensuring the security of their systems will ensure

their proprietary data cannot be accessed, maintain trust, protect reputation and brand, reduce operating costs and increase agility, and maintain an overall competitive advantage.

Supports emerging technologies

The use of encryption also serves as the basis for innovations in emerging technologies such as blockchain and IoT. Blockchains use encryption to provide anonymity, verify transactions, and prevent tampering. This provides their users with confidence over the security of their transactions and data.[410] Similarly, with countless IoT devices connected to the Internet, and each other, encryption is necessary to secure all of the information these devices collect, store, and transmit.[411] However, IoT presents some unique challenges because many devices have lower power and computing capabilities, which limits their ability to use best-in-class encryption.

> **Impact on SMEs**

A mandate to weaken encryption, either through backdoors, traceability, or any other means, will disproportionately impact start-ups and SMEs. Smaller companies will be unable to effectively operationalise a backdoor, handle the key, its retention and distribution operations, or implement traceability. By substantially increasing operational, technical, and compliance costs, a requirement to build backdoors or similar capabilities will disincentivize innovation. There are three systemic problems SMEs would face.[412]

First, building a backdoor, or enabling traceability, will require the development of new technology. Given that a lot of the Internet is run on legacy technology, companies with older infrastructure will have to incur great costs to update their systems. In addition to covering the cost of these new methods, they would also have to cover the costs of implementing security upgrades to account for these changes. Second, start-ups and SMEs will have to hire more personally to manage these complex systems. Third, because backdoors and traceability inherently weaken security, businesses will become more liable as their systems become less secure. These issues are especially challenging to smaller businesses, which may eventually risk their ability to continue operating on the Internet.

> **The importance of an enabling policy framework for encryption**

The Indian government has set out its vision for self-reliant India for a post-COVID economic upturn. Encryption could play a crucial role in this recovery. However, the provision of an enabling, predictable, and stable policy environment for encryption will be key to ensure this growth. This will provide technology companies, especially start-ups and SMEs, with the necessary support to realize the benefits of encryption. Regulations that do not restrict the use of best-in-class technology, and do not require businesses to undermine encryption, incentivize innovation among businesses, particularly in the ICT sector.[413] Without any restrictions, businesses are free to innovate and try out enhanced functionalities in their products and tools for digital security.[414]

Encryption and Critical Industries

The use of encryption is critical for businesses in critical industries such as healthcare, banking and transactions, retail and commerce, smart cities, communication, infrastructure, and others. It protects vital communication networks, internet infrastructures, and data centres from security risks and cyberattacks, and is central to instilling trust in the digital economy.

Banking and financial transactions

The use of high-level encryption is important for securing financial information. Just as businesses and banks use security, such as armoured truck services for transferring money in the real world, online financial services use encryption to provide security to their clients.[415] The

knowledge of security is essential for increasing user adoption of online financial services such as online banking, and digital payments. India already had the highest volumes of digital transactions worldwide when the pandemic struck, this number is expected to increase five-fold by 2025.[416] This growth would not have been possible without security protocols encrypting transactional data. But, to ensure a continuity of this growth, user confidence must not be compromised.[417] Weakening encryption will not ameliorate those concerns.

E-commerce and retail

E-commerce transactions, though still a small portion of total retail sales, have increased substantially over the past few years in India. Without the use of Secure Stocks Layer (SSL) and Transport Layer Security (TLS) protocols, which keeps customer data secure when in-transit, e-commerce would be far less trusted and used.[418] The use of strong encryption standards and overall data security offered by e-commerce players also has had a knock-on effect on other industries. Indian SMEs are increasingly being brought into the digital fold, as a result of which they are able to increase sales, expand scale, and reach new markets and customers. Again, this growth, and digital adoption, would be greatly diminished without the use of strong encryption.

Healthcare

The Covid-19 induced lockdown posed several challenges, including hindering people from accessing healthcare and medical services. To address this issue, the Indian government released guidelines to enable remote consultations, which eased the burden on in-person consultation but also required parties to exchange sensitive information digitally.[419] Additionally, the Indian government also launched the National Digital Health Mission **(NDHM)** to digitise the entire healthcare ecosystem.[420] These efforts together would increase healthcare access and coverage. But to ensure their effective operation, they must be accompanied with secure communication protocols, storage databases, authentication measures, and encryption tools to preserve the security and privacy of healthcare systems/ records. Hospitals already rely on sophisticated IT systems to ensure the secure delivery of critical healthcare services. But as healthcare increasingly moves to the Internet, encryption will be critical for service providers to maintain and establish secure e-health records, protect sensitive patient data and medical resources, and ensure effective delivery of critical services especially during the ongoing healthcare crisis.[421]

Communications and messaging services

The use of strong encryption in messaging platforms allows users to communicate instantly and securely around the globe, for both personal and professional use. While these platforms can also be used to spread of misinformation, they play perform a critical function as broadcasting channels that allow the widespread dissemination of information, especially in the context of emergency alerts for crime and natural disasters.[422] Encryption is also used to securely store and share photos, videos, documents, and other digital material. Finally, the group chat feature offered by many encrypted instant messenger apps provides all types of groups and communities — from friends and families to organizations and interest groups — the ability to securely communicate and connect continuously with fellow members, both within and across global borders.[423] Even at a professional and enterprise level, an increasing number of service providers (such as Google and Microsoft) have recognized the benefits of stronger encryption, and are making a shift towards enabling E2EE and client-side encryption within their products.[424]

Smart cities and public infrastructure

India must leverage the power of tech and IT systems to fulfil its objective to set up digitally connected and sustainable smart cities. These cities are backed by sensors and IoT technologies, along with other systems and devices. However, smart cities typically rely on traditional and advanced tools to function, which increases the risk of cyberattacks. Smart cities across the world have been exposed to such attacks which has resulted in disruption of services.[425] In May 2016, the Ministry of Housing and Urban Affairs issued

a model framework for executing solutions while setting up smart cities. The framework prescribed guidelines to preserve the security across different layers in a smart city including the sensor, communication, data and application layers. It noted that all the information that flows on the networks would be encrypted to preserve the privacy and confidentiality of data, end points of all the devices would be authenticated, all the traffic from sensors to servers would be encrypted and secured, among other cyber security measures.[426]

Benefits of Encryption in the State Machinery

Encryption is a key design feature of India's digital infrastructure. The government is increasingly leveraging communication networks to deliver services under flagship projects like Aadhar, national health ID, and several others. Secure systems, especially during the pandemic, enable governments to switch all communications and services to digital platforms and effectively meet citizens' needs. This also intensifies the need to put in place a robust cybersecurity framework that supports the use of strong encryption.

This is because the computers and networks operating that help conduct the business of the government are susceptible to harmful attacks. In 2021 alone, a database of Covid-19 test results of Indian patients was hacked, while a database with information of up to 500,000 police candidates was also breached.[427] Further, due to an increase in data breaches, especially during the pandemic, there has been a significant increase in identity fraud, with the most prevalent threats being financial fraud, phishing and electronic transfer fraud.[428] This is why several of such initiatives mandate the use of strong encryption. Even the proposed PDP Bill obligates organisations, including public sector bodies, to deploy encryption tools.[429] The Indian government also aims to leverage emerging technologies such as blockchain, IoT, AI, and 5G to deliver services and conduct governance, in the coming future. This will only increase the need to guard these systems through encryption.[430]

National security and intelligence

The Indian security establishment relies on strong encryption to protect state secrets and critical infrastructures. Various organisations within the government focus on enhancing India's cryptography profile through purchase of encryption systems for strategic purposes and development of indigenous technologies. The Defence Research and Development Organisation **(DRDO)** has a dedicated crypto evaluation lab – the Scientific Analysis Group.[431] The Scientific Analysis Group has recently developed quantum key distribution communication systems to demonstrate their ability to share keys securely between two devices.[432]

The Joint Cipher Bureau of the Ministry of Defence is responsible for the development of cryptology and signals intelligence **(SIGINT)**, coordinating with various military and intelligence agencies on these developments, and responsible for the deployment of key management systems and customized encryption products for defence purposes.[433] The Guidelines for Protection of Critical Information Infrastructure **(CII)**, 2015 issued by the National Critical Information Infrastructure Protection Centre **(NCIIPC)** require the deployment of strong encryption for the protection of CII data.[434]

E-governance and service delivery

With the increasing adoption of e-governance initiatives by various departments of the central and state governments, encryption has become a key factor in securing these initiatives. The IT Act states that the Central Government may prescribe the use encryption to promote 'e-governance and e-commerce'.[435]

The National Digital Communications Policy, 2018 states that the government must develop a policy on encryption by harmonizing the legal and regulatory framework in order to 'assure security of digital communications.'[436] The NITI Aayog also encouraged the use of blockchain to create a cryptography-based land record system, as well as in the public distribution and healthcare space.

[437] The Telangana Government's Draft Blockchain Policy identifies the use of blockchain in land records and microfinance areas, suggesting a greater reliance on encryption-based technologies for their governance programs.[438]

The Cloud Security Design Principles of the GI Cloud MeghRaj Initiative also recommend the use of encryption for securing data at rest and in motion.[439] Similarly, India's unique identification program for service delivery – Aadhaar – is made secure through strong, end-to-end, 2048-bit encryption.[440] Sensitive personal data including biometric data is also encrypted immediately upon collection.[441] Similarly, the National Digital Health Blueprint Report, when laying down its 'key building blocks for data and access management', states that an anonymizer must be deployed, which shall have encryption capabilities as needed.[442]

Electricity and energy sector

Electricity grid and energy networks are highly vulnerable to cyberattacks.[443] Recognising the seriousness of cyberattacks on electricity grid and the resultant information breach, a government expert group recently proposed measures to safeguard the national grid from spyware, malware, cyber-attacks, and network hacking.[444] It also directed the central electricity authority, load dispatch centres, state and centre transmission utilities to put in place information security policies for incident management, and instal firewalls for all systems to deal with an attack on their IT systems.[445] The report also required entities to develop a cyber crisis management plan of any major cyber-attack including 'continuity plans, recovery plans, communication plans, cyber incident response plans', among other things.[446] The use of encryption, and applied cryptography tools, is also critical towards preserving the security of electrical grids.[447]

Recommendations

As the previous chapters have demonstrated, the encryption debate has multiple facets, each of which presents unique challenges from a policy-making perspective. Any solution will have significant consequences for all actors involved. Because of this, there is no single policy or technological solve that can clarify the situation. But at the same time, strong encryption is undeniably an essential building block for the future of the Indian economy. By allowing consumers and businesses to secure and share sensitive information, encryption has enabled the digital economy to flourish. It enables secure banking, local and global business, running of power grids, communications networks, and almost every digital application/service.[448] On the other hand, the costs of weakening encryption can be substantial.[449] Rather than place barriers on encryption or pursue mandates to weaken encryption, the Indian government should encourage the use of stronger encryption and support innovation in encryption.

Focus on data at rest rather than data in transit

Accessing data in transit poses several challenges that do not emerge when accessing data at rest. For instance, modern encryption protocols for data in transit use perfect forward secrecy, meaning that a new set of keys is used for every separate communication. Even if the user's keys are compromised on the end-device, hackers cannot go back in time to decrypt previously transmitted messages.[450] Mechanisms to intercept, or access, data in transit will break forward secrecy.[451] Similarly, adopting mechanisms to undermine end-to-end encryption will fundamentally alter system mechanics, leaving it less secure.[452] On the other hand, the Carnegie Working Group on Encryption argues that shifting the debate to accessing end-device data may be more productive.[453] While there are no existing proposals that are unquestionably viable and balanced, the potential for fruitful debate with a clearer characterization of risks and benefits is more plausible here, as opposed

to data in transit.[454] This approach may prove beneficial in the context of Indian law, where law enforcement has unrestricted powers under the Criminal Procedure Code to gain access to mobile phones and hard-drives.[455] Along with the need to develop a technical solution that is feasible and does not compromise cybersecurity, a focus on this front can advance conversations around developing the legal duties, limits, and oversight mechanisms for law enforcement accessing data at rest.

Requirement to trace originator of information should be optional

There is no consensus on the feasibility of the traceability requirement. For many service providers, like end-to-end encrypted messaging intermediaries, it may not be possible to operationalize this requirement.[456] For others, it will effectively mandate service providers to change their platform architecture. Due to its significant implications on security, privacy, and overall platform design, the traceability obligation needs to be tested at both policy and technical levels. It is unclear if this requirement institutes appropriate safeguards that will preclude incomplete or unreasonable LEA requests, or if there is enough evidence to assess the technical feasibility or the privacy and security risks of this requirement. More importantly, the solutions proposed may not meet the high standards required to establish criminal liability of the originator.[457] In this environment of uncertainty, platforms who cannot technically comply with this obligation may be forced to take certain actions to avoid liability. This may include weakening encryption, or building backdoors, or dropping the use of end-to-end encryption altogether. All of these introduce significant security vulnerabilities and increase the likelihood of privacy violations. Given that the traceability solution is untested, unvetted, and non-peer reviewed, it will disproportionately impact both service providers and users. Accordingly, the requirement to enable tracing the originator of messages should only apply to intermediaries if it is technically feasible.

Build capacity of law enforcement

It is clear that in some cases, LEA capacity to investigate crime may be diminished due to the use of unrecoverable or user-side encryption. Generally as well, state and local law enforcement has been ill-equipped to investigate and prosecute Internet-dependent criminal activities.[458] Beyond accessing encrypted data, other policies and practices also affect LEA's ability to obtain necessary information. These include accessing data in the cloud and on internet-of-things devices, use of communications metadata, obtaining timely and full compliance with court orders and other legal process in situations not involving encryption, as well as such legal and policy tools as mutual legal assistance treaties, inter-departmental information sharing, greater cyber forensics capacity, etc.[459] Accordingly, the government should provide law enforcement agencies with new legal and educational tools to overcome this challenge. It should also offer additional resources to state and local law enforcement agencies for cyber forensics and to incentivize resource sharing between different departments, at both state and central levels.

Establish clear rules for government hacking

Existing law is unclear on the legality of government hacking. It remains a grey area as it is not dealt with under any existing laws.[460] The government should establish clear and consistent rules for how and when law enforcement can hack into systems, including any assistance the private sector should provide, and transparency requirements.[461] This will ensure that law enforcement has the appropriate authority to pursue investigations while also ensuring that fundamental rights are protected and the impact on companies is minimized. The government should also develop a framework to disclose 'zero-day' vulnerabilities to service providers.[462] Similarly, there is a need to acknowledge and enable the role of third-party security researchers in discovering vulnerabilities in existing products and services.[463] This can also help offset the security risks posed by government hacking.

Institute appropriate process safeguards under the interception framework

Requiring decryption of information involves a higher degree of intrusion than standard search and seizure of electronic documents.[464] Generally, information protected by encryption safeguards can be presumed to be sensitive. In this respect, India's interception framework is dependent upon executive approval for interception, decryption, and monitoring. The lack of judicial review or legislative oversight has been heavily criticised, even by the Justice Srikrishna Committee that was set up to recommend a draft data protection law for India.[465] Accordingly, the government should mandate that every request for decryption should be accompanied with a judicial warrant, while the orders themselves should be subject to appeal.

Clarify the scope of technical assistance under the Decryption Rules

Existing processes for intercepting digital communications[466] are unclear about the scope of technical assistance required from service providers.[467] For instance, service providers are only obligated to answer decryption requests if they are in possession of the encryption keys.[468] At the same time, they are obligated to provide "all facilities, cooperation, and assistance" for electronic surveillance,[469] along with obligations to provide access to their software, hardware, firmware, equipment, and so on.[470] The manner of technical assistance that service providers can be asked to provide, therefore, remains open-ended. It could result in an obligation to build a backdoor or alter their system architecture. Questions around the scope of technical assistance are also being considered by the Supreme Court.[471] Regardless, the government should ensure that the scope of technical assistance does not include requirements to build backdoors, weaken encryption, or introduce any manner of systemic vulnerability.

Remove the restriction on usage of bulk encryption

Worldwide, one of the core issues in the encryption debate has been about whether the government should regulate the strength of communications encryption.[472] In India, the prohibition on using bulk encryption under the ULA presumably disallows the use of strong encryption by telecom and internet service providers, and potentially other service providers using their networks.[473] The earlier restriction of 40-bit encryption was also very weak. Encryption that is not strong or relies on lower key lengths reduces the overall security of the nation-wide information and communications infrastructure. It is therefore critical that the government should not place restrictions on the usage of stronger encryption by ULA licensees.

References

1. Lindsey Sheppard et al., The Spectrum of Encryption: Safety and Security Considerations, Centre for Strategic & International Studies, August 2020, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200831_Encryption_Full_WEB.pdf.

2. Rishab Bailey et al., Backdoors to Encryption: Analysing an intermediary's duty to provide 'technical assistance', DGN Working Paper 15, February 2020, https://datagovernance.org/files/research/1615814633.pdf.

3. James Lewis et al., The Effect of Encryption on Lawful Access to Communications and Data, Centre for Strategic & International Studies Technology Policy Program, February 2017, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/encryption/csis_study_en.pdf.

4. OECD, OECD Recommendations Concerning Guidelines for Cryptography Policy, 27 March 1997, http://www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm#:~:text=The%20OECD%20Recommendation%20Concerning%20Guidelines,for%20which%20they%20were%20developed.

5. Decryption refers to the process of using the key to transform the scrambled text into its original form.

6. Rishab Bailey et al., Backdoors to Encryption: Analysing an intermediary's duty to provide 'technical assistance', DGN Working Paper 15, February 2020, https://datagovernance.org/files/research/1615814633.pdf.

7. Stewart A. Baker, Decoding OECD Guidelines for Cryptography Policy, The International Lawyer 31 (3), Fall 1997, https://core.ac.uk/download/pdf/216909193.pdf.

8. Also, recoverable or unrecoverable encryption.

9. James Lewis et al., The Effect of Encryption on Lawful Access to Communications and Data, Centre for Strategic & International Studies Technology Policy Program, February 2017, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/encryption/csis_study_en.pdf.

10. User-side encryption, or unrecoverable encryption, refers to an application of encryption where the service provider does not have access to the decryption key. Only the user holds access to the encryption and decryption keys. This is discussed in more detail on page (30) of this Whitepaper.

11. Matt Olsen et al., Don't Panic. Making Progress in the "Going Dark" Debate, The Berkman Centre for Internet & Society at Harvard University, 1 February 2016, https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

12. Jack Nicas et al., FBI Asks Apple to Help Unlock Two iPhones, The New York Times, 7 January 2020, https://www.nytimes.com/2020/01/07/technology/apple-fbi-iphone-encryption.html.

13. Isobel Hamilton, WhatsApp faces international pressure to hand over access to encrypted chats, Business Insider India, 31 July 2019, https://www.businessinsider.in/tech/whatsapp-faces-international-pressure-to-hand-over-access-to-encrypted-chats/articleshow/70467569.cms.

14. George Barket et al., The Economic Impact of Laws that Weaken Encryption, Internet Society, 05 April 2021, https://www.internetsociety.org/wp-content/uploads/2021/05/The_Economic_Impact_of_Laws_that_Weaken_Encryption-EN.pdf.

15. Matt Olsen et al., Don't Panic. Making Progress in the "Going Dark" Debate, The Berkman Centre for Internet & Society at Harvard University, 1 February 2016, https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

16. Pranesh Prakash et al., How India Regulates Encryption, Centre for Internet Society, 30 October 2015, https://cis-india.org/internet-governance/blog/how-india-regulates-encryption.

17. 2021 Intermediary Guidelines.

18. Trisha Ray, The Encryption Debate in India: 2021 Update, International Encryption Brief, Carnegie Endowment for International Peace, 31 March 2021, https://carnegieendowment.org/2021/03/31/encryption-debate-in-india-2021-update-pub-8Tri4215.

19. Dr. Nehaluddin Ahmad, Privacy and the Indian Constitution: A Case Study of Encryption, Communications of the IBIMA Volume 7, 2009, https://ibimapublishing.com/articles/CIBIMA/2009/455684/455684.pdf.

20. Global Internet Liberty Campaign, Cryptography and Liberty 1999: An International Survey of Encryption Policy, February 1998, http://gilc.org/crypto/crypto-survey-99.html.

21. Bedavyasa Mohanty, The Encryption Debate in India, International Encryption Brief, International Encryption Brief, Carnegie Endowment for International Peace, 30 May 2019, https://carnegieendowment.org/2019/05/30/encryption-debate-in-india-pub-79213.

22. Mayur Shetty, Red Alert Issued Against US Network Software, 12 January 1999.

23. Kargil Committee Report, Executive Summary, 25 February 2000, www.nuclearweaponarchive.org/India/KargilRCA.html.

24. Department of Telecommunications, Notification No.820-1/98-LR (Pt. II), 6 August 1999, https://dot.gov.in/sites/default/files/amendment_isp_6-8-1999_0.pdf?download=1.

25. Section 3, IT Act.

26. Reserve Bank of India, Internet Banking in India – Guidelines, 2000, https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=414&Mode=0; Press Release, Committee on Internet Based Securities Trading and Services – First Report, SEBI, Government of India, https://www.sebi.gov.in/sebi_data/commondocs/99290report_p.pdf.

27. Section 84, IT Act.

28. Section 69, IT Act.

29. Decryption Rules, IT Act.

30. Draft National Encryption Policy, Department of Electronics and Information Technology, https://info.publicintelligence.net/IN-DraftEncryptionPolicy.pdf.

31. Rule 4(2), Information Technology (Intermediaries Guidelines and Digital Media Ethics) Rules, 2021, http://egazette.nic.in/WriteReadData/2021/225464.pdf

32. Clause 33, Personal Data Protection Bill, 2019.

33. Amy Wills, India threatens to ban BlackBerry Services, The Telegraph, 12 August 2010, https://www.telegraph.co.uk/technology/blackberry/7940964/India-threatens-to-ban-BlackBerry-services.html.

34. Justice K.S. Puttaswamy (Retd.) v Union of India, (2017) 10 SCC 1.

35. Facebook Inc. v. Antony Clement Rubin, Diary No.32478/2019, Supreme Court of India.

36. WhatsApp LLC v. Union of India. See copy of petition here: https://www.medianama.com/wp-content/uploads/2021/05/WhatsApp-v.-Union-of-India-Filing-Version.pdf.

37. Clause 24, Personal Data Protection Bill,2019.

38. Trisha Ray, The Encryption Debate in India: 2021 Update, International Encryption Brief, Carnegie Endowment for International Peace, 31 March 2021, https://carnegieendowment.org/2021/03/31/encryption-debate-in-india-2021-update-pub-8Tri4215.

39. Section 84, IT Act.

40. Section 43A, IT Act.

41. The Information Technology (Certifying Authorities) Rules, 2000.

42. 2048-bit RSA key is comparable/equivalent to the strength of a 112-bit symmetric key

43. Clause 2.2 (vii), ISP License Agreement for Provision of Internet Services, Department of Telecommunications, 2010, www.dot.gov.in/sites/default/files/L%20A%20after%2025.01.10%281%29_0.doc.

44. Bedavyasa Mohanty, The Encryption Debate in India, International Encryption Brief, International Encryption Brief, Carnegie Endowment for International Peace, 30 May 2019, https://carnegieendowment.org/2019/05/30/encryption-debate-in-india-pub-79213.

45. Clause 37(1), License Agreement for Unified License, Department of Telecommunications, Ministry of Communications, Government of India, 8 January 2014, https://dot.gov.in/sites/default/files/Amended%20UL%20Agreement_0.pdf?download=1.

46. Clause 37.1, 37.5, License Agreement for Unified License, Department of Telecommunications, Ministry of Communications, Government of India, 8 January 2014, https://dot.gov.in/sites/default/files/Amended%20UL%20Agreement_0.pdf?download=1.

47. Bedavyasa Mohanty, The Encryption Debate in India, International Encryption Brief, International Encryption Brief, Carnegie Endowment for International Peace, 30 May 2019, https://carnegieendowment.org/2019/05/30/encryption-debate-in-india-pub-79213.

48. Reserve Bank of India, Internet Banking in India – Guidelines, 2000, https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=414&Mode=0.

49. Reserve Bank of India, Master Direction – Information Technology Framework for the NBFC Sector, 8 June 2017, https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10999.

50. Reserve Bank of India, Guidelines on Regulation of Payment Aggregators and Payment Gateways, 17 March 2020, https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11822&Mode=0.

51. Reserve Bank of India, Master Direction on Digital Payments Security Controls, 18 February 2021, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MD7493544C24B5FC47D0AB12798C61CDB56F.PDF.

52. Securities and Exchange Board of India, Chapter 2 - Trading Software and Technology, 31 January 2000, https://www.sebi.gov.in/sebi_data/commondocs/chapter2trading_p.pdf.; Press Release, Committee on Internet Based Securities Trading and Services – First Report, https://www.sebi.gov.in/sebi_data/commondocs/99290report_p.pdf.

53. Securities and Exchange Board of India, Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants, , 03 December 2018, https://www.sebi.gov.in/legal/circulars/dec-2018/cyber-security-and-cyber-resilience-framework-for-stock-brokers-depository-participants_41215.html.

54. Securities and Exchange Board of India, Cyber Security and Cyber Resilience framework for Registrars to an Issue/ Share Transfer Agents, https://www.sebi.gov.in/sebi_data/attachdocs/oct-2017/1509260192319.pdf.

55. Electronic Health Record (EHR) Standards for India, Department of Health & Family Welfare, Ministry of Health & Welfare, 30 December 2016, https://www.nhp.gov.in/NHPfiles/EHR-Standards-2016-MoHFW.pdf.

56. National Digital Health Mission: Health Data Management Policy, Ministry of Health and Family Welfare, https://ndhm.gov.in/assets/uploads/NDHM%20Health%20Data%20anagement%20Policy.pdf.

57. 2048-bit RSA key is comparable/equivalent to the strength of a 112-bit symmetric key

58. Government of India, FAQs – Aadhaar Data Vault / Reference Keys, 25 July 2017, https://uidai.gov.in/images/resource/FAQs_Aadhaar_Data_Vault_v1_0_13122017.pdf.

59. *Id.*

60. GI Cloud (MeghRaj), A Cloud Computing Initiative, Ministry of Electronics and Information Technology, https://www.meity.gov.in/content/gi-cloud-meghraj.

61. Application for Empanelment of Cloud Service Offerings of Cloud Service Providers, Ministry of Electronics and Information Technology, May 2020, https://www.meity.gov.in/writereaddata/files/tender_upload/Application_CSP.pdf

62. Guidelines for Protection of Critical Information Infrastructure, 2015, https://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf.

63. Cyber Security Requirement for Smart City – Model Framework, National Security Council Secretariat, 19 May 2016, http://mohua.gov.in/pdf/58fd92b5545b85821b621a862dCyber_Securitypdf.pdf.

64. Cyber Security Requirement for Smart City – Model Framework, National Security Council Secretariat, 19 May 2016, http://mohua.gov.in/pdf/58fd92b5545b85821b621a862dCyber_Securitypdf.pdf.

65. Rishabh Bailey et al., Backdoors to Encryption: Analysing an intermediary's Duty to Provide Technical Assistance, DGN Working Paper 15, February 2020, https://datagovernance.org/files/research/1615814633.pdf.

66. Section 3(1AA), Telegraph Act.

67. Section 5(1), Telegraph Act.

68. Rule 419A, Telegraph Rules.

69. Rule 419A, Telegraph Rules.

70. Rule 419A, Telegraph Rules.

71. Rule 419A, Telegraph Rules.

72. PUCL v. Union of India, (1997) 1 SCC 301.

73. These include designating the Home Secretary as the authorised officer; requiring the specification of the communication to be intercepted and the address from where itis to be intercepted; requiring a consideration of whether the target information could be reasonably acquired by other means, limiting the duration of interception and the use of intercepted material, record keeping, and establishing a review committee.

74. Section 69, IT Act.

75. Rishab Bailey et al., Use of Personal Data by Intelligence and Law Enforcement Agencies, National Institute for Public Finance and Policy, 1 August 2018, https://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data.pdf.

76. Section 69(3), IT Act.

77. Section 69(2), IT Act.

78. Rule 7, Interception Rules.

79. Rule 22, Interception Rules.

80. Rule 13 and 17, Interception Rules.

81. Bedavyasa Mohanty, The Encryption Debate in India, International Encryption Brief, International Encryption Brief, Carnegie Endowment for International Peace, 30 May 2019, https://carnegieendowment.org/2019/05/30/encryption-debate-in-india-pub-79213.

82. Rule 19, Interception Rules.

83. Section 69(3), IT Act.

84. Committee of Experts under Justice B.N. Srikrishna, A Free and Fair Digital Economy Protecting Privacy, Empowering Indians, July 2018, https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

85. Software Freedom Law Centre, Blog, 1 September 2015 https://sflc.in/indias-surveillance-state-procedural-legal-framework.

86. Justice K.S. Puttaswamy (Retd.) v Union of India, (2017) 10 SCC 1.

87. Internet Freedom Foundation v Union of India, W.P. (C) No. 44/2019, Supreme Court of India.

88. Section 3(1AA), Telegraph Act.

89. Section 69B, IT Act.

90. Section 69B, IT Act.

91. Section 79, IT Act.

92. Rule 3(7), Information Technology (Intermediaries Guidelines) Rules, 2011.

93. Rule 4, 2021 Intermediaries Guidelines, 25 February 2021, http://egazette.nic.in/WriteReadData/2021/225464.pdf.

94. For a detailed discussion on the traceability, please see Chapter 3 of this Whitepaper.

95. Experts' Workshop Series on Encryption in India, Traceability and Cybersecurity, Internet Society, November 2020, https://www.internetsociety.org/wp-content/uploads/2020/11/2020-Encryption-in-India-EN.pdf.

96. Deepak Arora, NASSCOM – DSCI Feedback on the Draft Information Technology (Intermediary Guidelines (Amendment)) Rules, 2018, COMMUNITY by NASSCOM Insights, 26 November 2018, https://community.nasscom.in/communities/policy-advocacy/nasscom-dsci-feedback-on-the-draft-information-technology-intermediary-guidelines-amendment-rules-2018.html; Software Freedom Law Centre, The Future of Intermediary Liability in India, January 2020, https://sflc.in/sites/default/files/2020-01/SFLC.in%20-%20Intermediary_Liability_Report_%282020%29_1.pdf.

97. WhatsApp LLC v. Union of India. See copy of petition here: https://www.medianama.com/wp-content/uploads/2021/05/WhatsApp-v.-Union-of-India-Filing-Version.pdf; Praveen Arimbrathodiyil vs Union of India, WP(C) 9647/2021.

98. License Agreement For Unified License, Department of Telecommunications, Ministry of Communications, Government of India, 8 January 2014, https://dot.gov.in/sites/default/files/Amended%20UL%20Agreement_0.pdf?download=1.

99. Pranesh Prakash et al., How India Regulates Encryption, 30 October 2015, https://cis-india.org/internet-governance/blog/how-india-regulates-encryption.

100. Clause 23.2, License Agreement For Unified License, Department of Telecommunications, Ministry of Communications, Government of India, 8 January 2014, https://dot.gov.in/sites/default/files/Amended%20UL%20Agreement_0.pdf?download=1.

101. Clause 39.2, License Agreement For Unified License, Department of Telecommunications, Ministry of Communications, Government of India, 8 January 2014, https://dot.gov.in/sites/default/files/Amended%20UL%20Agreement_0.pdf?download=1.

102. Claude 39, License Agreement For Unified License, Department of Telecommunications, Ministry of Communications, Government of India, 8 January 2014, https://dot.gov.in/sites/default/files/Amended%20UL%20Agreement_0.pdf?download=1.

103. Rishabh Bailey et al., Backdoors to Encryption: Analysing an intermediary's Duty to Provide Technical Assistance, DGN Working Paper 15, February 2020, https://datagovernance.org/files/research/1615814633.pdf.

104. Software Freedom Law Centre, India's surveillance state: Other provisions of law that enable collection of user information, 2015; Further, 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" in the WhatsApp traceability case.

105. Section 91, 92, Code of Criminal Procedure, 1973.

106. Abhinav Sekhri, Mobile Phones and Criminal Investigations in India, 25 June 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3590996.

107. Matt Olsen et al., Don't Panic. Making Progress in the "Going Dark" Debate, The Berkman Centre for Internet & Society at Harvard University, 1 February 2016, https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

108. Draft National Encryption Policy, Department of Electronics and Information Technology, https://info.publicintelligence.net/IN-DraftEncryptionPolicy.pdf.

109. Rajya Sabha, Report of the AdHoc Committee of the Rajya Sabha to Study the Alarming Issue of Pornography on Social Media and its Effect on Children and Society as a Whole, January 2020, https://rajyasabha.nic.in/rsnew/Committee_site/Committee_File/ReportFile/71/140/0_2020_2_16.pdf.

110. The Cyber Security Policy 2013, The Ministry of Communication and Information Technology, July 2013, https://www.nciipc.gov.in/documents/National_Cyber_Security_Policy-2013.pdf.

111. Rajya Sabha, Finalization of the National Cyber Security Strategy for 2020-2025, Ministry of Electronics and Information Technology, https://pqars.nic.in/annex/253/A391.pdf.

112. Clause 24, Personal Data Protection Bill, 2019.

113. Clause 35, Personal Data Protection Bill,2019.

114. Trisha Ray, The Encryption Debate in India: 2021 Update, International Encryption Brief, Carnegie Endowment for International Peace, 31 March 2021, https://carnegieendowment.org/2021/03/31/encryption-debate-in-india-2021-update-pub-8Tri4215.

115. Clause 33, 34, PDP Bill.

116. Madhulika Srikumar et al., India-US Data Sharing for Law Enforcement: Blueprint for Reforms, 2019, https://www.orfonline.org/wp-content/uploads/2019/01/MLAT-Book-_v8_web-1.pdf.

117. Rule 4(2), Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules), http://egazette.nic.in/WriteReadData/2021/225464.pdf; The IT Rules will replace the 2011 set of intermediary guidelines.

118. See page (30) of this Whitepaper.

119. Anandita Singh Mankotia et al., After Pegasus Spying Row, India Asks WhatsApp to Explain Privacy Breach, Economic Times, 02 November 2019, https://economictimes.indiatimes.com/tech/internet/after-pegasus-spying-row-india-asks-whatsapp-to-explain-privacy-breach/articleshow/71851802.cms.

120. Traceability and Cybersecurity: Experts' Workshop Series on Encryption in India, The Internet Society, November 2020, https://www.internetsociety.org/resources/doc/2020/traceability-and-cybersecurity-experts-workshop-series-on-encryption-in-india/.

121. Justice K.S. Puttaswamy (Retd.) v Union of India, (2017) 10 SCC 1.

122. Aditi Agarwal, Facebook, WhatsApp sue Indian Government over traceability requirement, Forbes India, 26 May 2021, https://www.forbesindia.com/article/take-one-big-story-of-the-day/facebook-whatsapp-sue-indian-government-over-traceability-requirement/68175/1.

123. Torshka Sarkar et al., On the Legality and Constitutionality of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, 21 June 2021, https://cis-india.org/internet-governance/legality-constitutionality-il-rules-digital-media-2021; Gurshabad Grover et al., The Ministry and the Trace: Subverting End-to-End Encryption, 14 NUJS L. Rev. 1 (2021), http://nujslawreview.org/2021/07/09/the-ministry-and-the-trace-subverting-end-to-end-encryption/.

124. Aditi Agarwal, Can traceability and end-to-end encryption co-exist? Here's the legal view, Forbes India, 17 May 2021, https://www.forbesindia.com/article/take-one-big-story-of-the-day/can-traceability-and-endtoend-encryption-coexist-heres-the-legal-view/67001/1

125. Gurshabad Grover et al., The Ministry and the Trace: Subverting End-to-End Encryption, 14 NUJS L. Rev. 1 (2021), http://nujslawreview.org/2021/07/09/the-ministry-and-the-trace-subverting-end-to-end-encryption/.

126. Peter Swire & Kenesa Ahmad, 'Going Dark' Versus a 'Golden Age for Surveillance', 28 November 2011, https://fpf.org/wp-content/uploads/Going-Dark-Versus-a-Golden-Age-for-Surveillance-Peter-Swire-and-Kenesa-A.pdf.

127. For instance, groups circulating child sexual abuse or extremist material are likely to be re-

stricted to a narrow set of individuals.□ See Gurshabad Grover et al., The Ministry and the Trace: Subverting End-to-End Encryption, 14 NUJS L. Rev. 1 (2021), http://nujslawreview.org/2021/07/09/the-ministry-and-the-trace-subverting-end-to-end-encryption/.

128. Matthew Green, Thinking about "traceability", 1 August 2021, https://blog.cryptographyengineering.com/2021/08/01/thinking-about-traceability/.

129. Torshka Sarkar et al., On the Legality and Constitutionality of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, 21 June 2021, https://cis-india.org/internet-governance/legality-constitutionality-il-rules-digital-media-2021.

130. Press Release by the Ministry of Electronics and Information Technology on Rule 4(2) of the IT Rules, 26 May 2021, https://pib.gov.in/PressReleasePage.aspx?PRID=1721915.

131. Latest Draft Intermediary Rules: Fixing big tech by breaking our digital rights? Internet Freedom Foundation, 25 February 2021, https://internetfreedom.in/latest-draft-intermediary-rules-fixing-big-tech-by-breaking-our-digital-rights/.

132. Traceability and Cybersecurity: Experts' Workshop Series on Encryption in India, The Internet Society, November 2020, https://www.internetsociety.org/resources/doc/2020/traceability-and-cybersecurity-experts-workshop-series-on-encryption-in-india/; Vijayant Singh, Aman Taneja, If WhatsApp Gives in to Indian Govt's Demands, Should We Worry?, The Quint, 28 May 2021, https://www.thequint.com/voices/opinion/whatsapp-sues-govt-of-india-data-privacy-concerns-end-to-end-encryption-traceability-of-messages-freedom-of-speech-surveillance#read-more.

133. Kerala State Beverages (M&M) Corp. Ltd. v. P.P. Suresh, (2019) 9 SCC 710, at para 30

134. Will Cathcart, Encryption Has Never Been More Essential – or Threatened, Wired, 05 April 2021, https://www.wired.com/story/opinion-encryption-has-never-been-more-essential-or-threatened/.

135. This is because the legal procedure of issuing a traceability order is couched under the framework of Section 69 of the IT Act. Section 69, and the Decryption Rules, make no provision for any judicial oversight or review. See Page (30) for more details.

136. Internet Freedom Foundation v. Union of India, Plaint filed by petitioner, (2017) 10 SCC 1.

137. Sharanya G. Ranga et al, Striking a balance between privacy, security, The Hindu Business Line, 13 June 2021, https://www.thehindubusinessline.com/business-laws/striking-a-balance-between-privacy-security/article34806162.ece; Kazim Rizvi et al, Does The Traceability Requirement Meet the Puttaswamy Test?, Live Law, 15 March 2021, https://www.livelaw.in/columns/the-puttaswamy-test-right-to-privacy-article-21-171181.

138. Trisha Jalan, India's FOSS Community Files Plea in Kerala High Court Against IT Rules, Challenges Traceability Mandate, Medianama, 10 April 2021, https://www.medianama.com/2021/04/223-india-foss-challenge-it-rules-2021/.

139. Pravin Arimbrathodiyil vs Union of India: SFLC.in assists in challenged Part II of the Intermediary Rules, 2021in Kerala High Court, 10 April 2021, https://sflc.in/praveen-arimbrathodiyil-vs-union-india-sflcin-assists-challenging-part-ii-intermediary-rules-2021.

140. *Id.*

141. Aditi Agarwal, Can traceability and end-to-end encryption co-exist? Here's the legal view, Forbes India, 17 May 2021, https://www.forbesindia.com/article/take-one-big-story-of-the-day/can-traceability-and-endtoend-encryption-coexist-heres-the-legal-view/67001/1.

142. *Id.*

143. Pravin Arimbrathodiyil vs Union of India: SFLC.in assists in challenged Part II of the Intermediary Rules, 2021in Kerala High Court, 10 April 2021, https://sflc.in/praveen-arimbrathodiyil-vs-union-india-sflcin-assists-challenging-part-ii-intermediary-rules-2021.

144. Jagmeet Singh, Government Withdraws Letter to Apple Seeking Compliance on IT Rules 2021: Report, NDTV, 15 July 2021, https://gadgets.ndtv.com/internet/news/apple-india-imessage-it-rules-2021-government-meity-letter-withdrawn-2487198.

145. Aashish Aaryan, Centre's letter to Apple asking for IT Rules compliance withdrawn, The Indian Express, 15 July 2021, https://indianexpress.com/article/india/govt-letter-to-apple-asking-for-it-rules-compliance-withdrawn-7405137/.

146. Mehab Qureshi, Govt's U-Turn Over iMessage and IT Rules 'Discriminatory': Experts, The Quint, 16 July 2021, https://www.thequint.com/cyber/policy/govts-u-turn-over-imessage-and-it-rules-discriminatory-experts#read-more.

147. *Id.*

148. V. Kamakoti, Report on Originator traceability in WhatsApp Messages, submissions to the Madras High Court, 31 July 2019, https://www.medianama.com/wp-content/uploads/Dr-Kamakoti-submission-for-WhatsApp-traceability-case-1.pdf.

149. Deeksha Bharadwaj, Hash constant: Govt's solution to tracing originator of viral messages, Hindustan Times, 02 March 2021, https://www.hindustantimes.com/india-news/hash-constant-govt-s-solution-to-tracing-originator-of-viral-messages-101614667706841.html; New IT Rules: Empowering Control or Controlling Empowerment? Deciphering the Intermedia, CCAOI India, 04 March 2021, https://www.youtube.com/watch?v=E8wkfidXaWs.

150. *Id.*; Sarvesh Mathi, All Your Questions on WhatsApp's End-To-End Encryption Answered, Medianama, 02 June 2021, https://www.medianama.com/2021/06/223-whatsapp-encryption-faq/.;

151. Internet Freedom Foundation, IFF files independent expert's submission before Madras HC on PIL relating to encryption and traceability, 23 August 2019, https://internetfreedom.in/iff-files-independent-expert-submission-before-madras-hc/.

152. Aditi Agarwal, IIT Madras's Kamakoti tells MediaNama how WhatsApp traceability is possible without undermining end-to-end encryption, 08 August, 2019, https://www.medianama.com/2019/08/223-kamakoti-medianama-whatsapp-traceability-interview/.

153. Software Freedom Law Centre, The Future of Intermediary Liability in India, 17 January 2020, https://sflc.in/future-intermediary-liability-india.

154. What is traceability and why does WhatsApp oppose it?, WhatsApp, 2021, https://faq.whatsapp.com/general/security-and-privacy/what-is-traceability-and-why-does-whatsapp-oppose-it/?lang=en.; Varsha Bansal, WhatsApp's Fight With India Has Global Implications, Wired, 27 May 2021, https://www.wired.com/story/whatsapp-india-traceability-encryption/.

155. What is traceability and why does WhatsApp oppose it?, WhatsApp, 2021, https://faq.whatsapp.com/general/security-and-privacy/what-is-traceability-and-why-does-whatsapp-oppose-it/?lang=en

156. Megha Mandavia, Digital rights body IFF files IIT-B Prof submission saying traceability on WhatsApp vulnerable to falsification, Economic Times, 25 August 2019, https://economictimes.indiatimes.com/tech/internet/digital-rights-body-iff-fil/es-iit-b-prof-submission-saying-traceability-on-whatsapp-vulnerable-to-falsification/articleshow/70826842.cms?from=mdr.

157. IFF files independent expert's submission before Madras HC on PIL relating to encryption and traceability, Internet Freedom Foundation, 23 August 2019, https://internetfreedom.in/iff-files-independent-expert-submission-before-madras-hc/; Shruti Dhapola, 'Fingerprint techniques to locate originator of message not absolute, vulnerable to impersonation', Indian Express, 08 April 2021, https://indianexpress.com/article/technology/tech-news-technology/fingerprint-techniques-to-locate-originator-of-message-not-absolute-vulnerable-to-impersonation-7264422/.

158. Internet Society, Traceability and Cybersecurity, Experts' Workshop Series on Encryption in India, November 2020, https://www.internetsociety.org/resources/doc/2020/traceability-and-cybersecurity-experts-workshop-series-on-encryption-in-india/.

159. Namrata Maheshwari et al, Part 2: New Intermediary Rules in India Imperil Free Expression, Privacy, and Security, Centre for Democracy and Technology, 04 June 2021, https://cdt.org/insights/part-2-new-intermediary-rules-in-india-imperil-free-expression-privacy-and-security/; Jonathan Meyer, Content Moderation for End-to-End Encrypted Messaging, Princeton University, 6 October 2019, https://www.cs.princeton.edu/~jrmayer/papers/Content_Moderation_for_End-to-End_Encrypted_Messaging.pdf.

160. Patrick Nohe, The difference between Encryption, Hashing and Salting, Hashed Out, 19 December 2018, https://www.thesslstore.com/blog/difference-encryption-hashing-salting/.

161. Namrata Maheshwari et al, Part 2: New Intermediary Rules in India Imperil Free Expression, Privacy, and Security, Centre for Democracy and Technology, 04 June 2021, https://cdt.org/insights/part-2-new-intermediary-rules-in-india-imperil-free-expression-privacy-and-security/; Sushmita Panda, 'Alphanumeric Hashing will affect encryption', The Sunday Guardian Live, 10 April 2021, https://www.sundayguardianlive.com/business/alphanumeric-hashing-will-affect-encryption.

162. Torshka Sarkar et al., On the Legality and Constitutionality of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, 21 June 2021, https://cis-india.org/internet-governance/legality-constitutionality-il-rules-digital-media-2021.

163. Please see page (30) of this Whitepaper for more details.

164. Aditi Agarwal, Traceability and end-to-end encryption cannot co-exist on digital messaging platforms: Experts, Forbes India, 15 March 2021, https://www.forbesindia.com/article/take-one-big-story-of-the-day/traceability-and-endto-end-encryption-cannot-coexist-on-digital-messaging-platforms-experts/66969/1.

165. Gurshabad Grover et al., The Ministry and the Trace: Subverting End-to-End Encryption, 14 NUJS L. Rev. 1 (2021), http://nujslawreview.org/2021/07/09/the-ministry-and-the-trace-subverting-end-to-end-encryption/ ; Ivan Mehta, Africa is using WhatsApp 'mods' with extra features we all want, The Next Web, 10 March 2020, https://thenextweb.com/news/africa-is-using-whatsapp-mods-with-extra-features-we-all-want.

166. Traceability and Cybersecurity: Experts' Workshop Series on Encryption in India, The Internet Society, November 2020, https://www.internetsociety.org/resources/doc/2020/traceability-and-cybersecurity-experts-workshop-series-on-encryption-in-india/.

167. What is traceability and why does WhatsApp oppose it?, WhatsApp, 2021, https://faq.whatsapp.com/general/security-and-privacy/what-is-traceability-and-why-does-whatsapp-oppose-it/?lang=en

168. Katitza Rodriguez, Why Indian Courts Should Reject Traceability Obligations, Electronic Frontier Foundation, 2 June 2021, https://www.eff.org/deeplinks/2021/06/why-indian-courts-should-reject-traceability-obligations.

169. Manoj Prabhakaran, On a Proposal for Originator Tracing in WhatsApp, 31 July 2019, https://drive.google.com/file/d/1vivciN8tNSbOrA9eZ8Ej0m-CAUBzRWu5N/view.

170. Katitza Rodriguez, Why Indian Courts Should Reject Traceability Obligations, Electronic Frontier Foundation, 02 June 2021, https://www.eff.org/deeplinks/2021/06/why-indian-courts-should-reject-traceability-obligations.

171. Gurshabad Grover et al., The Ministry and the Trace: Subverting End-to-End Encryption, 14 NUJS L. Rev. 1 (2021), http://nujslawreview.org/2021/07/09/the-ministry-and-the-trace-subverting-end-to-end-encryption/.

172. Erica Portnoy, Why Adding Client-Side Scanning Breaks End-To-End Encryption, Electronic Frontier Foundation, November 2019, https://www.eff.org/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption.

173. *Id.*

174. Torshka Sarkar et al., On the Legality and Constitutionality of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, 21 June 2021, https://cis-india.org/internet-governance/legality-constitutionality-il-rules-digital-media-2021.

175. Gurshabad Grover et al., The Ministry and the Trace: Subverting End-to-End Encryption, 14 NUJS L. Rev. 1 (2021), http://nujslawreview.org/2021/07/09/the-ministry-and-the-trace-subverting-end-to-end-encryption/.

176. Namrata Maheshwari et al, Part 2: New Intermediary Rules in India Imperil Free Expression, Privacy, and Security, Centre for Democracy and Technology, 04 June 2021, https://cdt.org/insights/part-2-new-intermediary-rules-in-india-imperil-free-expression-privacy-and-security/.

177. What is traceability and why does WhatsApp oppose it?, WhatsApp, 2021, https://faq.whatsapp.com/general/security-and-privacy/what-is-traceability-and-why-does-whatsapp-oppose-it/?lang=en.

178. *Id.*

179. Namrata Maheshwari et al, Part 2: New Intermediary Rules in India Imperil Free Expression, Privacy, and Security, Centre for Democracy and Technology, 04 June 2021, https://cdt.org/insights/part-2-new-intermediary-rules-in-india-imperil-free-expression-privacy-and-security/.

180. Aditi Agarwal, Traceability and end-to-end encryption cannot co-exist on digital messaging platforms: Experts, Forbes India, 15 March 2021, https://www.forbesindia.com/article/take-one-big-story-of-the-day/traceability-and-endto-end-encryption-cannot-coexist-on-digital-messaging-platforms-experts/66969/1.

181. Whatsapp, The threat of traceability in Brazil and how it erodes privacy, https://faq.whatsapp.com/general/security-and-privacy/the-threat-of-traceability-in-brazil-and-how-it-erodes-privacy/?lang=en.

182. Katitza Rodriguez, Seth Schoen, FAQ: Why Brazil's Plan to Mandate Traceability in Private Messaging Apps Will Break User's Expectation of Privacy and Security, Electronic Frontier Foundation, 7 August 2020, https://www.eff.org/deeplinks/2020/08/faq-why-brazils-plan-mandate-traceability-private-messaging-apps-will-break-users.

183. Monika Ermert, German High Court Defines New "IT Basic Law" Curbing Online Searches, Intellec-

tual Property Watch, 1 March 2008, https://www.ip-watch.org/2008/03/01/german-high-court-defines-new-it-basic-law-curbing-online-searches/.

184. Bhairav Acharya et al., Deciphering the European Encryption Debate: Germany, Open Technology Institute, July 2017, https://d1y8sb8igg2f8e.cloudfront.net/documents/Transatlantic_Encryption_Germany.pdf.

185. Thomas de Maizière et al., Letter to the European Commission, 20 February 2017, https://regmedia.co.uk/2017/02/28/french_german_eu_letter.pdf.

186. Press Release from the Federal Ministry of the Interior and Federal Ministry of Economics and Technology: Key points of the German Crypto Policy, 1999.

187. The Federal Government, Digital Agenda 2014-17, https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2014/digital-agenda.pdf?__blob=publicationFile.

188. The Federal Government, German Cybersecurity Strategy, 2016, https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf.

189. Sven Herpig et al., Germany's Crypto Past and Hacking Future, 13 April 2017, https://www.lawfareblog.com/germanys-crypto-past-and-hacking-future.

190. Jenny Gesley, Germany: Expanded Telecommunications Surveillance and Online Search Powers, Library of Congress, 7 September 2017, https://www.loc.gov/law/foreign-news/article/germany-expanded-telecommunications-surveillance-and-online-search-powers/.

191. Steven Herpig et al., The Encryption Debate in Germany, 30 May 2019, https://carnegieendowment.org/2019/05/30/encryption-debate-in-germany-pub-79215.

192. *Id.*

193. *Id.*

194. Kilian Vieth, New hacking powers for German intelligence agencies, About Intel, 27 October 2020, https://aboutintel.eu/germany-hacking-reform/.

195. David Martin, Germany's government hackers face Constitutional Court, 7 August 2018, https://www.dw.com/en/germanys-government-hackers-face-constitutional-court/a-44988326.

196. BVerfGe, Online Search Case, 2008, 120 BVerfGe 274.

197. BVerfG, Judgment of the First Senate, 20 April 2016, 1BvR 966/09.

198. A 'vulnerabilities equities' process guides state agencies to disclose the knowledge of zero-day security vulnerabilities to technology companies for the purposes of developing patches, or enabling law enforcement to retain the ability to leverage such vulnerabilities for future instances of legal hacking. See Sven Herpig, Ari Schwartz, The Future of Vulnerabilities Equities Processes Around the World, 4 January 2019, https://www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world.

199. Steven Herpig et al., The Encryption Debate in Germany, 30 May 2019, https://carnegieendowment.org/2019/05/30/encryption-debate-in-germany-pub-79215.

200. Global Partners Digital, World Map of Encryption Laws and Policies, https://www.gp-digital.org/world-map-of-encryption/.

201. Wolfgang Schulz et al., Human Rights and Encryption, 2016, https://www.ivir.nl/publicaties/download/human_rights_and_encryption.pdf.

202. Relevant laws are the Federal Information Security Modernization Act (FISMA) of 2014, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act (HIPAA) and also the Federal Trade Commission Act.

203. Bernstein v US Department of Justice, https://www.eff.org/cases/bernstein-v-us-dept-justice.

204. Kendall Howell, The Fifth Amendment, Decryption and Biometric Passcodes, Lawfare, 27 November 2017, https://www.lawfareblog.com/fifth-amendment-decryption-and-biometric-passcodes#:~:text=In%20contrast%20to%20a%20purely,an%20encryption%20case%2C%20Fisher%20v.&text=The%20defendants%20challenged%20the%20order,protected%20by%20the%20Fifth%20Amendment; See, for technical insight into fifth amendment protections, Aloni Cohen et al., Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries, Harvard Journal of Law & Technology, 2018, https://jolt.law.harvard.edu/assets/articlePDFs/v32/32HarvJLTech169.pdf.

205. Jack Karsten, et al., A Brief History of US Encryption Policy, Brookings, 19 April 2016, https://www.brookings.edu/blog/techtank/2016/04/19/a-brief-history-of-u-s-encryption-policy/.

206. S. 3398 (116th): EARN IT Act of 2020, https://www.govtrack.us/congress/bills/116/s3398.

207. Matthew Green, EARN IT Act is a direct attack on end-to-end encryption, 06 March 2020, https://blog.cryptographyengineering.com/2020/03/06/earn-it-is-an-attack-on-encryption/.

208. Trisha Anderson et al., Lawful Access to Encrypted Data Act Introduced, Inside Privacy, https://www.insideprivacy.com/surveillance-law-enforcement-access/lawful-access-to-encrypted-data-act-introduced/.

209. Mathew Waxman, Doron Hidin, How Does Israel Regulate Encryption?, 30 November 2015, https://www.lawfareblog.com/how-does-israel-regulate-encryption.

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

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

212. Kendall Howell, The Fifth Amendment, Decryption and Biometric Passcodes, Lawfare, 27 November 2017, https://www.lawfareblog.com/fifth-amendment-decryption-and-biometric-passcodes#:~:text=In%20contrast%20to%20a%20purely,an%20encryption%20case%2C%20Fisher%20v.&text=The%20defendants%20challenged%20the%20order,protected%20by%20the%20Fifth%20Amendment; See, for technical insight into fifth amendment protections, Aloni Cohen et al., Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries, Harvard Journal of Law & Technology, 2018, https://jolt.law.harvard.edu/assets/articlePDFs/v32/32HarvJLTech169.pdf.

213. *Id.*

214. *Id.*

215. Israel Basic Law: Human Dignity and Liberty, 1992, https://www.knesset.gov.il/laws/special/eng/basic3_eng.htm.

216. Government Access to Encrypted Communications: Israel, Library of Congress, last updated on 30 December 2020, https://www.loc.gov/law/help/encrypted-communications/israel.php.

217. Gili Cohen, Israel's High Court Rejects Warrantless Cellphone Searches, Haaretz, 19 June 2017, https://www.haaretz.com/israel-news/.premium-israel-s-top-court-rejects-warrantless-cellphone-searches-1.5485978.

218. Privacy International, Five Eyes, https://privacyinternational.org/learn/five-eyes.

219. United States, Department of Justice, International Statement: End-to-end Encryption and Public Safety, 11 October 2020, https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety.

220. Regulation of Investigatory Powers Act, 2000.

221. The Investigatory Powers Act, 2016.

222. Sections 252, 253, Investigatory Powers Act, 2016.

223. Bhairav Acharya et al., Deciphering The European Encryption Debate: United Kingdom, Open Technology Institute, June 2017, https://d1y8sb8igg2f8e.cloudfront.net/documents/Transatlantic_Encryption_UK__Final.pdf.

224. Alex Hern, UK government can force encryption removal, but fears losing, experts say, 29 March 2017, https://www.theguardian.com/technology/2017/mar/29/uk-government-encryption-whatsapp-investigatory-powers-act.

225. Open Rights Group, "Investigatory Powers Bill," Briefing for the House of Lords, https://www.openrightsgroup.org/assets/files/campaign_resources/investigatory_powers_bill/IPBill_briefing_Lords.pdf; Joint Committee on the Draft Investigatory Powers Bill, Written Evidence, 75-8.

226. Matt Burgess, "Home Office Will Make 'Major' Changes to Revised Surveillance Bill," Wired, 1 March 2016, https://www.wired.co.uk/article/home-office-investigatory-powers-bill.

227. Phillip Le Riche, "The Investigatory Powers Bill - It's Time to Take a Closer Look," 22 March 2016, https://www.grahamcluley.com/investigatory-powers-closer-look/.

228. Tim Hickman, Investigatory Powers Act 2016 becomes law, 12 December 2016, https://www.whitecase.com/publications/alert/investigatory-powers-act-2016-becomes-law.

229. *Id.*

230. Section 317C, Assistance and Access Bill 2018. Communication service provider is defined broadly. The full list runs for three pages, and includes everyone from the major telecommunications carriers down to an entity that "provides an electronic service that has one or more end-users in Australia," anyone who "develops, supplies or updates software used, for use, or likely to be used, in connection with" such a service, and "manufactures or supplies components for use, or likely to be used, in the manufacture of customer equipment for use, or likely to be used, in Australia.

231. Telecommunications and Other Legislation Amendment (Assistance and Access Bill, 2018, https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6195_aspassed/toc_pdf/18204b01.pdf;fileType=application/pdf.

232. Stilgherrian, The Encryption Debate in Australia, Carnegie Endowment for International Peace, 30 May 2019, https://carnegieendowment.org/2019/05/30/encryption-debate-in-australia-pub-79217.

233. Assistance and Access: A new industrial assistance framework, https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/assistance-and-access-industry-assistance-framework

234. *Id.*, See Technical Assistance Request.

235. *Id.*, See Technical Assistance Notice.

236. *Id.*, See Technical Capability Notice.

237. *Id.*

238. Section 317ZG, Australian Telecommunications Act 1997.

239. Stilgherrian, "Australia's encryption laws will fall foul of differing definitions", 11 December 2018, https://www.zdnet.com/article/australias-encryption-laws-will-fall-foul-from-differing-definitions/.

240. See full report of the INSLM here: https://www.inslm.gov.au/sites/default/files/2020-07/INSLM_Review_TOLA_related_matters.pdf.

241. Philip Catania et al., Australia's security monitor recommends changes to controversial 'anti-encryption' legislation, Corrs Chambers Westgarth, July 2020, https://corrs.com.au/insights/australias-security-monitor-recommends-changes-to-controversial-anti-encryption-legislation.

242. Art. 24, Law regarding Confidence in the Digital Economy (LCEN), 2004-575, 21 June 2004. According to this law, the use of means of cryptology are free and are not subject to prior approval if such deployment is exclusively for the functions of authentication or control of integrity.

243. Articles 60-1 and 60-2, French Criminal Procedure Code, 1958.

244. Article 230-1, French Criminal Procedure Code, 1958.

245. Bhairav Acharya et al., Deciphering the European Encryption Debate: France, Open Technology Institute, July 2017, https://na-production.s3.amazonaws.com/documents/France_Paper_8_8.pdf.

246. Article 434-15-2, French Penal Code.

247. Article L871-1, Intelligence Act, 2015.

248. For a more comprehensive review of France's legal framework for hacking, see European Parliament Directorate-General for Internal Policies, "Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices," March 2017, http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf.

249. Bhairav Acharya et al., Deciphering the European Encryption Debate: France, Open Technology Institute, July 2017, https://na-production.s3.amazonaws.com/documents/France_Paper_8_8.pdf.

250. Ross Schulman et al., Deciphering the European Encryption Debate: France, 31 July 2017, https://www.newamerica.org/oti/blog/deciphering-european-encryption-debate-france/.

251. Articles 60-1 and 60-2, French Criminal Procedure Code, 1958.

252. Bhairav Acharya et al., Deciphering the European Encryption Debate: France, Open Technology Institute, July 2017, https://na-production.s3.amazonaws.com/documents/France_Paper_8_8.pdf.

253. Zunyou Zhou, China's Comprehensive Counter Terrorism Law, 23 January 2016, https://thediplomat.com/2016/01/chinas-comprehensive-counter-terrorism-law/.

254. Covington, China Enacts Encryption Law, 31 October 2019, https://www.cov.com/-/media/files/corporate/publications/2019/10/china_enacts_encryption_law.pdf.; Lorand Laskai et al., The Encryption Debate in China, Carnegie Endowment for International Peace, 30 May 2019. https://carnegieendowment.org/2019/05/30/encryption-debate-in-china-pub-79216.

255. Lindsey Sheppard et al., The Spectrum of Encryption: Safety and Security Considerations, Centre for Strategic & International Studies, August 2020, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200831_Encryption_Full_WEB.pdf.

256. Jack Nicas, Raymond Zhong, and Daisuke Wakabayashi, Censorship, Surveillance and Profits: A Hard Bargain for Apple in China, New York Times, 17 May 2021, https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html.

257. Article 12 of the Russian Federal Law No. 128-FZ, 2001, On Licensing Specific Types of Activities.

258. European Commission for Democracy Through Law, Federal Law on the Federal Security Service of the Russian Federation, 24 February 2012, https://policehumanrightsresources.org/content/uploads/2016/08/Federal-Law-on-Federal-Security-Service-Russia-1995.pdf?x96812.

259. Rishabh Bailey et al., Backdoors to Encryption: Analysing an intermediary's Duty to Provide Technical Assistance, Data Governance Network Working Paper, February 2020, https://datagovernance.org/files/research/1615814633.pdf.

260. Information Technology and Innovation Foundation, Unlocking Encryption: Information Security and Rule of Law, March 2016, http://www2.itif.org/2016-unlocking-encryption.pdf.

261. Filings related to In Re Order Requiring Apple, Inc. To Assist In The Execution Of A Search Warrant Issued By This Court, No. 15-MC-1902, 9 October 2015.

262. Carlos Liguori, Exploring Lawful Hacking as a Possible Answer to the "Going Dark" Debate Dark", 2020, https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1019&context=mtlr.

263. Claiming that widespread encryption would be disastrous for law enforcement, the United States government proposed the use of the 'Clipper Chip' on devices, an encryption tool that contained a master key held by the government. This would give the government access to encrypted communications.

264. Harold Abelson et al., Keys under doormats: Mandating insecurity by requiring government access to all data and communications, 2015, https://www.schneier.com/wp-content/uploads/2016/09/paper-keys-under-doormats-CSAIL.pdf.

265. James A. Lewis et al., The Effect of Encryption on Lawful Access to Communications and Data, February 2017, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/encryption/csis_study_en.pdf.

266. Lindsey R. Sheperd et al., The Spectrum of Encryption: Safety and Security Considerations, August 2020, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200831_Encryption_Full_WEB.pdf.

267. Hemani Sheth, India joins global call on tech companies to allow encryption backdoors for law enforcement, 13 October 2020, https://www.thehindubusinessline.com/info-tech/india-joins-global-call-on-tech-companies-to-allow-encryption-backdoors-for-law-enforcement/article32840898.ece.

268. United States, Department of Justice, Lawful Access Policy Brief, https://www.justice.gov/olp/lawful-access.

269. This is a cryptographic feature that ensures that a new key is created for each communication between the sender and the recipient. This ensures that an attacker who gains access to keys can only decrypt data from the time of the breach; historic and future data remains safe.

270. Rishabh Bailey et al., Backdoors to Encryption: Analysing an intermediary's Duty to Provide Technical Assistance, Data Governance Network Working Paper, February 2020, https://datagovernance.org/files/research/1615814633.pdf.

271. James A. Lewis et al., The Effect of Encryption on Lawful Access to Communications and Data, February 2017, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/encryption/csis_study_en.pdf.

272. *Id.*

273. Information Technology and Innovation Foundation, Unlocking Encryption: Information Security and Rule of Law, March 2016, http://www2.itif.org/2016-unlocking-encryption.pdf.

274. Cloudflare, Policy Primer: The Encryption Conundrum, 2017, https://www.cloudflare.com/media/pdf/cloudflare-whitepaper-policy-primer-the-encryption-conundrum.pdf; James A. Lewis et al., The Effect of Encryption on Lawful Access to Communications and Data, February 2017, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/encryption/csis_study_en.pdf.

275. United States Courts, Wiretap Reports, https://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports; Erin Kelly, FBI can't unlock 13% of password-protected phones it seized, official says, https://www.usatoday.com/story/news/politics/2016/04/19/fbi-cant-unlock-13-password-protected-phones-seized-official-says/83224860/.

276. Europol, Transnational access to electronic evidence for criminal cases: trends and latest developments within the EU and beyond, Press Release, 01 December 2020, https://www.europol.europa.eu/newsroom/news/transnational-access-to-electronic-evidence-for-criminal-cases-trends-and-latest-developments-within-eu-and-beyond.

277. *Id.* Under this study, LEAs cited basic subscriber information (52.9%) and traffic data (32.4%) as the most often needed types of data in investigations. LEAs also identified short data retention periods (70.6%), difficulty in identifying how and where to send requests (55.9%) and a lack of standardization in companies' processes (41.2%) as the three main problems when trying to access evidence from service providers -- i.e. not encryption.

278. G. Weimann, The Terrorist Migration to the Darkweb, June 2016, https://www.jstor.org/stable/26297596?seq=1#metadata_info_tab_contents.

279. Rukmini Callimachi, How ISIS Built the Machinery of Terror under Europe's Gaze, 29 March 2016, https://www.nytimes.com/2016/03/29/world/europe/isis-attacks-paris-brussels.html?_r=0.

280. Bruce Scheiner et al., Don't Panic. Making Progress on the Going Dark Debate, 1 February 2016, https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

281. Information Technology and Innovation Foundation, Unlocking Encryption: Information Security and Rule of Law, March 2016, http://www2.itif.org/2016-unlocking-encryption.pdf.

282. Bruce Scheiner et al., Don't Panic. Making Progress on the Going Dark Debate, 1 February 2016, https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

283. Amnesty International, Encryption: A Matter of Human Rights, 2017, https://www.amnestyusa.org/wp-content/uploads/2017/04/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf.

284. UNESCO, Keystones to foster inclusive Knowledge Societies, Access to information and knowledge, Freedom of Expression, Privacy, and Ethics on a Global Internet, 2015, https://unesdoc.unesco.org/ark:/48223/pf0000232563.

285. David Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression A/HRC/29/32, 22 May 2015, https://sflc.in/sites/default/files/wp-content/uploads/2017/10/2015-David-Kaye-Encryption-Anonymity.pdf.

286. K.S. Puttaswamy v Union of India, (2017) 10 SCC 1.

287. UNESCO, Keystones to foster inclusive Knowledge Societies, Access to information and knowledge, Freedom of Expression, Privacy, and Ethics on a Global Internet, 2015, https://unesdoc.unesco.org/ark:/48223/pf0000232563.

288. Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of expression, , UN Doc. A/HRC/23/40, 17 April 2013.

289. *Id.*

290. Neil Richards, Intellectual Privacy, 87 TEXAS L. REV 387, 389 (2008).

291. Global Partners Digital, Travel Guide to the Digital World: ENCRYPTION POLICY FOR HUMAN RIGHTS DEFENDERS, 2017, https://www.gp-digital.org/wp-content/uploads/2017/09/TRAVELGUIDETO-ENCRYPTIONPOLICY.pdf.

292. https://www.forbesindia.com/article/take-one-big-story-of-the-day/facebook-whatsapp-sue-indian-government-over-traceability-requirement/68175/1

293. Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on the right to privacy, REFERENCE:OL IND 8/2021, 11 June 2021, https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=26385.

294. Stefanie Pell, Jonesing for a Privacy Mandate, Getting a Technology Fix—Doctrine to Follow, 14 N.C. J. L. & TECH. 489, 2013; Neil Richards, Don't let US government read your e-mail, CNN, 18 August 2013, https://edition.cnn.com/2013/08/18/opinion/richards-lavabit-surveillance/ index.html.

295. Bedvyasa Mohanty, "GOING DARK' IN INDIA: The Legal and Security Dimensions of Encryption, December 2016, https://www.orfonline.org/wp-content/uploads/2016/12/ORF_Occasional_Paper_102_Encryption.pdf.

296. United States v Jones, 565 US 400 (Sotomayor J., concurring).

297. Woodrow Hartzog and Evan Selinger, Surveillance as Loss of Obscurity, 72 WASH. & LEE L. REV. 1343, 2015.

298. James Comey, Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?, Federal Bureau of Investigation, 2014, https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

299. Access Now, Human Rights in the Digital Era: An International Perspective on Australia 2018, https://www.accessnow.org/cms/assets/uploads/2018/07/Human-Rights-in-the-Digital-Era-an-international-perspective-on-Australia.pdf.

300. Lex Gill, Law, Metaphor, and the Encrypted Machine, 2018.

301. Harold Abelson et al., Keys under doormats: Mandating insecurity by requiring government access to all data and communications, 2015, https://www.schneier.com/wp-content/uploads/2016/09/paper-keys-under-doormats-CSAIL.pdf.

302. Chris Jaikaran, Encryption: Frequently Asked Questions, Congressional Research Service, 28th September 2016, https://fas.org/sgp/crs/misc/R44642.pdf.

303. *Id.*

304. James A. Lewis et al., The Effect of Encryption on Lawful Access to Communications and Data, February 2017, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/encryption/csis_study_en.pdf.

305. Amazon Web Services, Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, 4 July 2019.

306. This is discussed in greater detail in Chapter 6 of this Whitepaper.

307. Article 32, GDPR.

308. Clause 24, PDP Bill.

309. Wolfgang Schulz, Joris van Hoboken, Encryption and Human Rights, 2016 https://www.ivir.nl/publicaties/download/human_rights_and_encryption.pdf.

310. *Id.*

311. *Id.*

312. This is discussed in detail in Chapter 3 of this Whitepaper.

313. Dara Kerr, NSA reportedly installing spyware on US-made hardware, 12 May 2014, https://www.cnet.com/news/nsa-reportedly-installing-spyware-on-us-made-hardware/.

314. Dan Goodin, Chinese hackers who breached Google reportedly targeted classified data, 21 May 2013, https://arstechnica.com/information-technology/2013/05/chinese-hackers-who-breached-google-reportedly-targeted-classified-data/.

315. Alexa Wainscott, A "Golden Key" to Pandora's Box: The Security Risks of Government-Mandated Backdoors to Encrypted Communications, 2017.

316. Chad Perrin, The danger of complexity: More code, more bugs, 1 February 2020, https://www.techrepublic.com/blog/it-security/the-danger-of-complexity-more-code-more-bugs/.

317. Stephanie K. Pell, You Can't Always Get What You Want: How Will Law Enforcement Get What it Needs in a Post-CALEA, Cybersecurity-Centric Encryption Era?, 2016, https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1306&context=ncjolt.

318. In re An Apple Phone Seized During the Execution of a Search Warrant on a Black Lexus IS300, No. ED 15-0451M, 2016 U.S. Dist. LEXIS 20543 (C.D. Cal. Feb. 16, 2016), https://www.clearinghouse.net/detail.php?id=15497.

319. *Id.*

320. James A. Lewis et al., The Effect of Encryption on Lawful Access to Communications and Data, February 2017, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/encryption/csis_study_en.pdf.

321. Joseph Lorenzo Hall, The NSA's Split-Key Encryption Proposal is Not Serious, 20 April 2015, https://cdt.org/insights/the-nsas-split-key-encryption-proposal-is-not-serious/.

322. Harold Abelson et al., Keys under doormats: Mandating insecurity by requiring government access to all data and communications, 2015, https://www.schneier.com/wp-content/uploads/2016/09/paper-keys-under-doormats-CSAIL.pdf.

323. Andy Greenberg, Hacker Lexicon: What Is Perfect Forward Secrecy?, 28 November 2016, https://www.wired.com/2016/11/what-is-perfect-forward-secrecy/.

324. Harold Abelson et al., Keys under doormats: Mandating insecurity by requiring government access to all data and communications, 2015, https://www.schneier.com/wp-content/uploads/2016/09/paper-keys-under-doormats-CSAIL.pdf.

325. Matthew Green, How do we build encryption backdoors, April 2016, https://blog.cryptographyengineering.com/2015/04/16/how-do-we-build-encryption-backdors/.

326. *Id.*

327. Harold Abelson et al., Keys under doormats: Mandating insecurity by requiring government access to all data and communications, 2015, https://www.schneier.com/wp-content/uploads/2016/09/paper-keys-under-doormats-CSAIL.pdf.

328. Parker Higgins, On the Clipper Chip's Birthday, Looking Back on Decades of Key Escrow Failures, Electronic Frontier Foundation, 16 April 2015, https://www.eff.org/deeplinks/2015/04/clipper-chips-birthday-looking-back-22-years-key-escrow-failures.

329. Matt Blaze, Key Escrow From A Safe Distance: Looking Back at the Clipper Chip, https://www.mattblaze.org/escrow-acsac11.pdf.

330. Standing Committee, National People's Congress of the PRC, Cryptography Law of the PRC, 14th Meeting of the 13th Congress (Beijing: China People's Congress, 26 October 2019). http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.shtml

331. European Commission for Democracy Through Law, Federal Law on the Federal Security Service of the Russian Federation, 24 February 2012, http://www.icla.up.ac.za/images/un/use-of-force/eastern-europe/Russia/Federal%20Law%20on%20Federal%20Security%20Service%20Russia%201995.pdf.

332. Jay Stowsky, Secrets or Shields to Share? New Dilemmas for Dual Use Technology Development and the Quest for Military and Commercial Advantage in the Digital Age, 2003, https://escholarship.org/uc/item/89r4j908.

333. Draft National Encryption Policy, Department of Electronics and Information Technology, https://info.publicintelligence.net/IN-DraftEncryptionPolicy.pdf.

334. Electronic Frontier Foundation, Secure Messaging Scorecard, https://www.eff.org/node/101713/.

335. Aaron F. Brantley, Banning Encryption to Stop Terrorists: A Worse than Futile Exercise, August 2017, https://ctc.usma.edu/wp-content/uploads/2017/08/CTC-Sentinel_Vol10Iss7-10.pdf.

336. See this leaked European Commission report: https://www.politico.eu/wp-content/uploads/2020/09/SKM_C45820090717470-1_new.pdf.

337. Mallory Knodel, New Technical Report Brings Together Experts to Tackle Encryption Myths, November 2020, https://cdt.org/insights/the-global-encryption-coalition-breaks-encryption-myths/.

338. Rule 4(4), 2021 Intermediaries Guidelines; S. 3398 (116th): EARN IT Act of 2020, https://www.govtrack.us/congress/bills/116/s3398.

339. The Economic Times, Facebook encryption threatens public safety, Priti Patel tells Zuckerberg, 04 October 2019, https://economictimes.indiatimes.com/news/international/world-news/facebook-encryption-threatens-public-safety-priti-patel-tells-zuckerberg/articleshow/71445166.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

340. Internet Society, Breaking encryption myths: What the European Commission's leaked report got wrong about online security, https://www.globalencryption.org/wp-content/uploads/2020/11/2020-Breaking-Encryption-Myths.pdf.

341. Internet Society, Fact Sheet: Client-Side Scanning, https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/.

342. Erica Portnoy, Why Adding Client-Side Scanning Breaks End-To-End Encryption, Electronic Frontier Foundation, November 2019, https://www.eff.org/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption.

343. *Id.*

344. Matthew Green, EARN IT Act is a direct attack on end-to-end encryption, 6 March 2020, https://blog.cryptographyengineering.com/2020/03/06/earn-it-is-an-attack-on-encryption/.

345. *Id.*

346. Erica Portnoy, Why Adding Client-Side Scanning Breaks End-To-End Encryption, Electronic Frontier Foundation, November 2019, https://www.eff.org/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption.

347. Ian Levy et al., Principles for a More Informed Exceptional Access Debate, 29 November 2018, https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate.

348. Susan Landau, Exceptional Access: The Devil is in the Details, 26 December 2018, https://www.lawfareblog.com/exceptional-access-devil-details-0.

349. Kevin Townsend, Inside GCHQ's Proposed Backdoor Into End-to-End Encryption, 3 June 2019, https://www.securityweek.com/inside-gchqs-proposed-backdoor-end-end-encryption.

350. Nate Cardozo, Give up the Ghost: A Backdoor by Another Name, 4 January, 2019, https://www.justsecurity.org/62114/give-ghost-backdoor/; Ross Schulman, Why the Ghost Keys Solution to

Encryption is No Solution, 18 July 2019, https://www.justsecurity.org/64968/why-the-ghost-keys-solution-to-encryption-is-no-solution/.

351. *Id.*

352. Rowena Johansen, Ethical Hacking Code of Ethics: Security, Risk & Issues, March 2017, http://panmore.com/ethical-hacking-code-of-ethics-security-risk-issues#:~:text=The%20legal%20risks%20of%20ethical,it%20is%20not%20performed%20properly.

353. *Id.*

354. EC-Council, 5 Vulnerabilities that ethical hacking can uncover, https://blog.eccouncil.org/what-is-ethical-hacking/.

355. Ben Buchanan, Bypass encryption: 'Lawful hacking' is the next frontier of law enforcement technology, Boston Business Journal, March 2017, https://www.bizjournals.com/boston/news/2017/03/17/viewpointbypassing-encryption-lawful-hacking-is.html.

356. European Parliament, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf).

357. *Id.*

358. Privacy International v. The Secretary of State for Foreign and Commonwealth Affairs, [2016] UKIP Trib 14_85-CH, https://www.ipt-uk.com/docs/Privacy_Greennet_and_Sec_of_State.pdf.

359. Riana Pfefferkorn, The FBI is mad because it keeps getting into locked iPhones without Apple's help, 23 May 2020, https://techcrunch.com/2020/05/22/the-fbi-is-mad-because-it-keeps-getting-into-locked-iphones-without-apples-help/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAE6qtM81RJRAuLgGVIiDZ5EFE_otFC2l6U0KkVhz4QUlZuzE8-vWERf2NtFfH4HSzaa_4LRRIHgQSGhaI-1nNUN_wrehMYyRzO1hE70O15XhhehUAD8AIFzmpwsksBdrrHUx0AUZkWo-AhkY81ThwTNtmtD1TyEQyZogf14YYYtD.

360. Simrit Chhabra et al., Framework for Regulating Encryption in India, August 2019, https://thequantumhub.com/wp-content/uploads/2020/08/Regulation-of-Encryption-TQH-Updated-08Apr19-Final.pdf.

361. Sven Herpig et al., The Future of Vulnerabilities Equities Process Around the World, 4 January 2019, https://www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world.

362. Rowena Johansen, Ethical Hacking Code of Ethics: Security, Risk & Issues, 24 March 2017, http://panmore.com/ethical-hacking-code-of-ethics-security-risk-issues.

363. Susan Landau, Law Enforcement Is Accessing Locked Devices Quite Well, Thank You, LawFare, 7 December 2020, https://www.lawfareblog.com/law-enforcement-accessing-locked-devices-quite-well-thank-you.

364. Logan Koepke et all, Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones, Upturn, October 2020, https://www.upturn.org/reports/2020/mass-extraction/.

365. Committee to Protect Journalists, Spyware and Press Freedom, https://cpj.org/spyware/.

366. Times of India, Pegasus 'snooping': Several prominent names on the 'list', 19 July 2021, https://timesofindia.indiatimes.com/india/pegasus-snooping-several-prominent-names-on-the-list/articleshow/84554139.cms.

367. Business Standard, Pegasus scandal: Defence Ministry says 'no transaction' with NSO Group, 9 August 2021, https://www.business-standard.com/article/current-affairs/pegasus-scandal-defence-ministry-says-no-transaction-with-nso-group-121080901294_1.html.

368. Yashovardhan Azad, Pegasus: India needs urgent surveillance reform, Hindustan Times, 10 August 2021, https://www.hindustantimes.com/opinion/pegasus-india-needs-urgent-surveillance-reform-101628602162097.html.

369. The procedure for ordering surveillance under Indian law is discussed in detail in Chapter 2 of this Whitepaper.

370. Aihik Sur, Pegasus spyware: How do we rein in State surveillance? Here's what experts had to say, Medianama, 21 July 2021, https://www.medianama.com/2021/07/223-pegasus-state-surveillance-experts-opinions/.

371. Harvard Law Review, Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance, April 2018, https://harvardlawreview.org/2018/04/cooperation-or-resistance-the-role-of-tech-companies-in-government-surveillance/.

372. ICT for Peace Foundation & Counter-Terrorism Committee Executive Directorate, Private Sector Engagement in Responding to the use of the internet and ICT for Terrorist Purposes, 2014, https://www.un.org/sc/ctc/wp-content/

uploads/2016/12/Private-Sector-Engagement-in-Responding-to-the-Use-of-the-Internet-and-ICT-for-Terrorist-Purposes.pdf.

373. Europol, Fighting Cybercrime in a Connected future, 11 October 2019, https://www.europol.europa.eu/newsroom/news/fighting-cybercrime-in-connected-future.

374. Peter Swire & Kenesa Ahmad, 'Going Dark' Versus a 'Golden Age for Surveillance', 28 November 2011, https://fpf.org/wp-content/uploads/Going-Dark-Versus-a-Golden-Age-for-Surveillance-Peter-Swire-and-Kenesa-A.pdf.

375. *Id.*

376. Harold Abelson et al., Keys under doormats: Mandating insecurity by requiring government access to all data and communications, 2015, https://www.schneier.com/wp-content/uploads/2016/09/paper-keys-under-doormats-CSAIL.pdf.

377. Claiming that widespread encryption would be disastrous for law enforcement, the United States government proposed the use of the 'Clipper Chip' on devices, an encryption tool that contained a master key held by the government. This would give the government access to encrypted communications.

378. Byron Tau, The FBI Secretly Ran the Anom Messaging Platform, Yielding Hundreds of Arrests in Global Sting, Wall Street Journal, 8 June 2021, https://www.wsj.com/articles/fbi-sting-using-anom-platform-leads-to-global-round-up-of-suspects-11623165556?st=7ddl6ijysz446l3&reflink=article_whatsapp_share.

379. Lily Hay Newman, The FBI's Anom Stunt Rattles the Encryption Debate, WIRED, 11 June 2021, https://www.wired.com/story/fbi-anom-phone-network-encryption-debate/.

380. McKinsey Global Institute, Internet matters: The Net's sweeping impact on growth, jobs, and prosperity, May 2011, https://www.mckinsey.com/~/media/McKinsey/Industries/Technology%20Media%20and%20Telecommunications/High%20Tech/Our%20Insights/Internet%20matters/MGI_internet_matters_full_report.pdf.

381. Bruce Scheiner, et al., Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications, 7 July 2015, https://www.schneier.com/wp-content/uploads/2016/09/paper-keys-under-doormats-CSAIL.pdf.

382. Ryan Hagemann et al., Encryption, Trust, and the Online Economy: An Assessment of the Economic Benefits Associated with Encryption, Niskanen Center, 9 November 2015, https://www.niskanencenter.org/wp-content/uploads/old_uploads/2015/11/RESEARCH-PAPER_EncryptionEconomicBenefits.pdf.

383. *Id.*

384. George Barket et al., The Economic Impact of Laws that Weaken Encryption, Internet Society, 05 April 2021, https://www.internetsociety.org/wp-content/uploads/2021/05/The_Economic_Impact_of_Laws_that_Weaken_Encryption-EN.pdf.

385. International Telecommunication Union, Powering the digital economy: Regulatory approaches to securing consumer privacy, trust and security, 2018, https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.POW_ECO-2018-PDF-E.pdf

386. Omar Abbosh et al., Securing the Digital Economy: Reinventing the Internet for Trust, Accenture Strategy, 2019, https://www.accenture.com/_acnmedia/Thought-Leadership-Assets/PDF/Accenture-Securing-the-Digital-Economy-Reinventing-the-Internet-for-Trust.pdf.

387. Stephen Burmester, The rising cost of a data breach in 2020, IBM, 6 August 2020, https://www.ibm.com/blogs/ibm-anz/the-rising-cost-of-a-data-breach-in-2020/.

388. Andy Greenberg, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, Wired, 22 August 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.

389. Anandi Chandrashekhar, Cost of data breach for India Inc rose by 9.4% in 2020: IBM Data Breach Report, The Economic Times, 29 July 2020, https://economictimes.indiatimes.com/tech/internet/cost-of-data-breach-for-india-inc-rose-by-9-4-in-2020-ibm-data-breach-report/articleshow/77235007.cms.

390. Stephen Burmester, The rising cost of a data breach in 2020, IBM, 6 August 2020, https://www.ibm.com/blogs/ibm-anz/the-rising-cost-of-a-data-breach-in-2020/.

391. Omar Abbosh & Kelly Bissell, Securing the Digital Economy: Reinventing the internet for trust, Accenture Strategy, at 4 (2019), https://www.accenture.com/_acnmedia/Thought-Leadership-Assets/PDF/Accenture-Securing-the-Digital-Economy-Reinventing-the-Internet-for-Trust.pdf.

392. George Barket et al., The Economic Impact of Laws that Weaken Encryption, Internet Society, 05 April 2021, https://www.internetsociety.org/wp-content/uploads/2021/05/The_Economic_Impact_of_Laws_that_Weaken_Encryption-EN.pdf.

393. *Id.*

394. National Institute of Standards and Technology, The Economic Impacts of the Advanced Encryption Standard, 1996-2017, September 2018, https://csrc.nist.gov/publications/detail/white-paper/2018/09/07/economic-impacts-of-the-advanced-encryption-standard-1996-2017/final.

395. Caleb Chen, Losing the Right to Encryption Means Losing Business, Internet Society, 29 September 2020, https://www.internetsociety.org/blog/2020/09/losing-the-right-to-encryption-means-losing-business/.

396. In 2019,18% of those who distrust the Internet responded that they make fewer online purchases. See https://www.internetsociety.org/wp-content/uploads/2019/06/CIGI-Ipsos-Trust-User-Privacy_Report_2019_EN.pdf).

397. International Telecommunication Union, Powering the digital economy: Regulatory approaches to securing consumer privacy, trust and security, 2018, https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.POW_ECO-2018-PDF-E.pdf.

398. Bedavyasa Mohanty et al., Framing Multi-stakeholder Conversations on Encryption, ORF Special Report, at 9 December 2016, https://www.orfonline.org/wp-content/uploads/2016/12/ORF_SpecialReport_29_Encryption_FinalForUpload.pdf.

399. Alison Grace Johansen, What is encryption and how does it protect your data?, Norton, 24 July 2020, https://us.norton.com/internetsecurity-privacy-what-is-encryption.html#:~:text=Encryption%20is%20the%20process%20of,a%20network%20like%20the%20internet.

400. Cyber Talk, Security breach exposes data of millions of Telefonica customers, 18 July 2018, https://www.cybertalk.org/2018/07/18/security-breach-exposes-data-millions-telefonica-customers/.

401. Istvan Lam, How to restore trust in the digital economy, Tresorit Blog, 18 July 2018, https://tresorit.com/blog/eprivacy-and-e-evidence/.

402. Kathy Brown, Encryption and Security our Digital Economy, CircleID, 7 April 2017, https://www.circleid.com/posts/20170407_encryption_and_securing_our_digital_economy/.

403. Bedavyasa Mohanty & Alexander Spalding, Framing Multi-stakeholder Conversations on Encryption, ORF Special Report, at 9, December 2016, https://www.orfonline.org/wp-content/uploads/2016/12/ORF_SpecialReport_29_Encryption_FinalForUpload.pdf.

404. Micheala Curry, What has cybersecurity got to do with innovation?, Deloitte, 09 June 2020, https://www2.deloitte.com/au/en/blog/innovation-blog/2020/what-cybersecurity-do-with-innovation.html.

405. Mohamad Ali, Backdoor Government decryption hurts my business and yours, Harvard Business Review, 15 September 2016, https://hbr.org/2016/09/backdoor-government-decryption-hurts-my-business-and-yours#:~:text=Market%20research%20suggests%20that%20the,to%20%244.82%20billion%20in%202019.&text=Fifteen%20years%20later%2C%20encryption%20increasingly,effectively%20and%20create%20economic%20growth.

406. Nate Lord, Startups and Data Breaches: How a startup can protect itself from a data breach in 2014 and beyond, Data Insider, 25 September 2020, https://digitalguardian.com/blog/startups-data-breaches-how-startup-can-protect-itself-data-breach-2014-beyond.

407. eGuard Technology Services, 9 ways encryption protects your business, https://www.eguardtech.com/9-ways-encryption-protects-your-business/.

408. Alex Loo, Can cybersecurity be a competitive edge, Echo Worx, 15 February 2019, https://www.echoworx.com/blog-can-cyber-security-be-a-competitive-edge/.

409. Deloitte, Industry 4.0 and cybersecurity, Managing risk in an age of connected production, 2017, https://www2.deloitte.com/content/dam/insights/us/articles/3749_Industry4-0_cybersecurity/DUP_Industry4-0_cybersecurity.pdf

410. Information Technology & Innovation Foundation, ITIF Technology Explainer: What is Encryption, 6 March 2020, https://itif.org/publications/2020/03/06/itif-technology-explainer-what-encryption.

411. *Id.*

412. Christian Dawson, Opinion: Encryption backdoors are killers of the innovation economy, The Christian Science Monitor, 18 December 2015, https://www.csmonitor.com/World/Passcode/2015/1218/Opinion-Encryption-backdoors-are-killers-of-the-innovation-economy.

413. Bedavyasa Mohanty, 'Going Dark' in India: The Legal and Security Dimensions of Encryption, ORF Occasional Paper, December 2016, https://www.orfonline.org/wp-content/uploads/2016/12/ORF_Occasional_Paper_102_Encryption.pdf.

414. BSA, Encryption: Why it matters, 2019, https://encryption.bsa.org/.

415. Ryan Hagemann et al., Encryption, Trust, and

the Online Economy: An Assessment of the Economic Benefits Associated with Encryption, Niskanen Center, 9 November 2015, https://www.niskanencenter.org/wp-content/uploads/old_uploads/2015/11/RESEARCH-PAPER_EncryptionEconomicBenefits.pdf.

416. https://www.weforum.org/agenda/2020/08/covid-19-has-accelerated-india-s-digital-reset/

417. Ryan Hagemann et al., Encryption, Trust, and the Online Economy: An Assessment of the Economic Benefits Associated with Encryption, Niskanen Center, 9 November 2015, https://www.niskanencenter.org/wp-content/uploads/old_uploads/2015/11/RESEARCH-PAPER_EncryptionEconomicBenefits.pdf.

418. Ryan Hagemann et al., Encryption, Trust, and the Online Economy: An Assessment of the Economic Benefits Associated with Encryption, Niskanen Center, 9 November 2015, https://www.niskanencenter.org/wp-content/uploads/old_uploads/2015/11/RESEARCH-PAPER_EncryptionEconomicBenefits.pdf.

419. Ministry of Family Health and Welfare, Telemedicine Practice Guidelines, https://www.mohfw.gov.in/pdf/Telemedicine.pdf.

420. National Digital Health Mission, https://ndhm.gov.in/.

421. Emmanuel de Roquefeuil, Tech-enabled healthcare solutions: The answer to the problem of Covid-19, Economic Times, 23 September 2020, https://cio.economictimes.indiatimes.com/news/next-gen-technologies/tech-enabled-healthcare-solutions-the-answer-to-the-problem-of-covid-19/78267889.

422. James Lewis, Denise Zheng, & William Carter, The Effect of Encryption on Lawful Access to Communications and Data, Centre for Strategic and International Studies, February 2017, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/170221_Lewis_EncryptionsEffect_Web.pdf.

423. Lindsey Shephard, Brian Katz et al, The Spectrum of Encryption: Safety and Security Considerations, Centre for Strategic and International Studies, August 2020, https://www.csis.org/analysis/spectrum-encryption-safety-and-security-considerations

424. Google, About client-side encryption, https://support.google.com/a/answer/10741897?hl=en; Tom Warren, Microsoft Teams is getting end-to-end encryption support, https://www.theverge.com/2021/3/2/22308915/microsoft-teams-end-to-end-encryption-support-e2ee.

425. PWC, Creating cyber secure smart cities, September 2018, https://www.pwc.in/assets/pdfs/publications/2018/creating-cyber-secure-smart-cities.pdf

426. Cyber Security Requirement for Smart City – Model Framework, National Security Council Secretariat, 19 May 2016, http://mohua.gov.in/pdf/58fd92b5545b85821b621a862dCyber_Securitypdf.pdf.

427. Soumik Ghosh, The biggest data breaches in India, CSO India, 13 March 2021, https://www.csoonline.com/article/3541148/the-biggest-data-breaches-in-india.html.

428. Gus Tomlinson, GBG State of Digital Identity: 2020, GBG, 2020, https://www.gbgplc.com/the-gbg-state-of-digital-identity-2020/.

429. Kazim Rizvi et al., The future is encrypted, The Daily Guardian, 12 November 2020, https://the-dailyguardian.com/the-future-is-encrypted/.

430. Shailender Kumar, A new India needs a new approach to data security, Economic Times, 3 October 2019, https://cio.economictimes.indiatimes.com/news/digital-security/a-new-india-needs-a-new-approach-to-data-security/71416379.

431. Scientific Analysis Group, Defence Research and Development Organisation, Ministry of Defence, https://www.drdo.gov.in/labs-and-establishments/scientific-analysis-group-sag.

432. Press Trust of India, DRDO Successfully Demonstrates Quantum Communication Between Two Labs, Hindustan Times, 9 December 2020, https://www.hindustantimes.com/india-news/drdo-successfully-demonstrates-quantum-communication-between-two-labs/story-8IiVkcPtgXAB9QpHFdwBRO.html

433. Joint Cipher Bureau, Global Security, https://www.globalsecurity.org/intell/world/india/jcb.htm.

434. Guidelines for Protection of Critical Information Infrastructure, 2015, https://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf

435. Section 84A, IT Act.

436. Section 1.3 (e), National Digital Communications Policy, 2018, https://innovate.mygov.in/ndcp_chapter/chapter5-secure-india/.

437. NITI Aayog, Blockchain - The India Strategy, January 2020, https://niti.gov.in/sites/default/files/2020-01/Blockchain_The_India_Strategy_Part_I.pdf.

438. Draft Blockchain Policy, 2019, Government of Telangana, https://it.telangana.gov.in/wp-content/uploads/2019/05/Telangana-Blockchain-Policy-Draft-May-2019.pdf.

439. Section 4, Cloud Security Best Practices, Ministry of Electronics and Information Technology, https://www.meity.gov.in/writereaddata/files/WI3_Cloud%20Security%20Best%20Practices_06112020.pdf.

440. Press Trust of India, Aadhaar protected by high-tech encryption, authentication: UIDAI Chairman, Economic Times, 24 May 2018, https://economictimes.indiatimes.com/news/politics-and-nation/aadhaar-protected-by-high-tech-encryption-authentication-uidai-chairman/articleshow/64308769.cms?from=mdr.

441. Section 6, Security in the UIDAI System, UIDAI, https://uidai.gov.in/my-aadhaar/about-your-aadhaar/security-in-uidai-system.html.

442. National Digital Health Blueprint, 2019, Ministry of Health and Family Welfare, https://www.nhp.gov.in/NHPfiles/National_Digital_Health_Blueprint_Report_comments_invited.pdf.

443. Kartik Bommakanti, China's cyberattack on Maharashtra power grid was to improve PLA's bargaining position, https://theprint.in/opinion/chinas-cyberattack-on-maharashtra-power-grid-was-to-improve-plas-bargaining-position/620274/.

444. Report of the Expert Group: Review of the Indian Electricity Grid Code, January 2020, http://www.cercind.gov.in/2020/reports/Final%20Report%20dated%2014.1.2020.pdf.

445. *Id.*

446. *Id.*

447. John Downing, Low Latency Encryption Will Secure the US Electrical Grid, https://www.cyberdefensemagazine.com/low-latency-encryption/.

448. Cathy Brown, Encryption and Securing Our Digital Economy, CircleID, 07 April 2017, https://www.circleid.com/posts/20170407_encryption_and_securing_our_digital_economy/.

449. George Barket et al., The Economic Impact of Laws that Weaken Encryption, Internet Society, 05 April 2021, https://www.internetsociety.org/wp-content/uploads/2021/05/The_Economic_Impact_of_Laws_that_Weaken_Encryption-EN.pdf.

450. What is perfect forward secrey?, Wired, 18 November 2021, https://www.wired.com/2016/11/what-is-perfect-forward-secrecy/.

451. Anand Venkatanarayanan, Dr. Kamakoti's Solution for WhatsApp Traceability Without Breaking Encryption Is Erroneous and Not Feasible, Medianama, 13 August 2019, https://www.medianama.com/2019/08/223-kamakoti-solution-for-traceability-whatsapp-encryption-madras-anand-venkatanarayanan/.

452. *Id.*

453. Carnegie Encryption Working Group, Moving the Encryption Policy Conversation Forward, Carnegie Endowment for International Peace, September 2019, https://carnegieendowment.org/files/EWG__Encryption_Policy.pdf.

454. *Id.*

455. Abhinav Sekhri, Mobile Phones and Criminal Investigations in India, SSRN, 25 June 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3590996.

456. Anand Venkatanarayanan, Dr. Kamakoti's Solution for WhatsApp Traceability Without Breaking Encryption Is Erroneous and Not Feasible, Medianama, 13 August 2019, https://www.medianama.com/2019/08/223-kamakoti-solution-for-traceability-whatsapp-encryption-madras-anand-venkatanarayanan/.

457. Traceability and Cybersecurity – Experts' Workshop Series on Encryption in India, Internet Society, November 2020, https://www.internetsociety.org/resources/doc/2020/traceability-and-cybersecurity-experts-workshop-series-on-encryption-in-india/.

458. Rishab Bailey et al., Backdoors to Encryption: Analysing an intermediary's duty to provide 'technical assistance', DGN Working Paper 15, February 2020, https://datagovernance.org/files/research/1615814633.pdf.

459. Carnegie Encryption Working Group, Moving the Encryption Policy Conversation Forward, Carnegie Endowment for International Peace, September 2019, https://carnegieendowment.org/files/EWG__Encryption_Policy.pdf.

460. Nasscom-DSCI Discussion Paper: The Road Ahead for Encryption in India, 4 September 2020, https://community.nasscom.in/communities/policy-advocacy/nasscom-dsci-discussion-paper-the-road-ahead-for-encryption-in-india.html.

461. Daniel Castro et al., Unlocking Encryption: Information Security and the Rule of Law, March 2016, http://www2.itif.org/2016-unlocking-encryption.pdf.

462. Sven Herpig et al., The Future of Vulnerabilities

Equities Processes Around the World, Lawfare, 4 January 2019, https://www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world.

463. Simrit Chhabra et al., Framework for Regulating Encryption in India, The Quantum Hub, August 2019, https://thequantumhub.com/wp-content/uploads/2020/08/Regulation-of-Encryption-TQH-Updated-08Apr19-Final.pdf.

464. Bedavyasa Mohanty, 'Going Dark' in India: The legal and security dimensions of encryption, 13 December 2016, https://www.orfonline.org/research/going-dark-in-india-the-legal-and-security-dimensions-of-encryption/.

465. Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (Retd.), A Free and Fair Digital Economy: Protecting Privacy, Protecting Indians, July 2018, https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf.

466. Sections 69A, 69B, Information Technology Act, 2000.

467. Rishab Bailey et al., Backdoors to Encryption: Analysing an intermediary's duty to provide 'technical assistance', DGN Working Paper 15, February 2020, https://datagovernance.org/files/research/1615814633.pdf.

468. Rules 17, 13(3), Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

469. Rule 13, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

470. Rule 19, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

471. Internet Freedom Foundation v Union of India, W.P. (C) No. 44/2019.

472. Bedavyasa Mohanty, 'Going Dark' in India: The legal and security dimensions of encryption, 13 December 2016, https://www.orfonline.org/research/going-dark-in-india-the-legal-and-security-dimensions-of-encryption/.

473. Pranesh Prakash et al., How India Regulates Encryption, Centre for Internet & Society, 30 October 2015, https://cis-india.org/internet-governance/blog/how-india-regulates-encryption.

Acknowledgement

On behalf of DSCI, we would like to extend our heartfelt gratitude to all the organizations and individuals for their valuable time and support without which this whitepaper would not have been possible. We also extend our special thanks to the Ikigai law team (Sreenidhi Srinivasan & Vijayant Singh) for their support in the creation of this whitepaper.

A NASSCOM® Initiative

DATA SECURITY COUNCIL OF INDIA

NASSCOM CAMPUS, 4th Floor, Plot. No. 7-10, Sector 126, Noida, UP - 201303

For any queries, contact:

E: info@dsci.in | W: www.dsci.in

DSCI_Connect dsci.connect dsci.connect data-security-council-of-india dscivideo