



The Dialogue™
INFORM . ENGAGE . IDEATE



ANALYSING THE NATIONAL SECURITY IMPLICATIONS OF WEAKENING ENCRYPTION



ANALYSING THE NATIONAL SECURITY IMPLICATION OF WEAKENING ENCRYPTION

Authors

Mr. Yashovardhan Azad, IPS (Retd.)

Chairman, DeepStrat

Mr. Anand Venkatnarayanan

Strategic Advisor, DeepStrat

Mr. Pranav Bhaskar Tiwari

Programme Manager, The Dialogue™

Mr. Sreyan Chatterjee

Senior Research Manager, The Dialogue™

Editor

Mr. Saikat Datta,

Designated & Founding Partner,
DeepStrat

Acknowledgement

We would like to thank Ambassador P. R. Chakravarty, IFS (Retd.), Former Secretary (Economic Relations), Ministry of Foreign Affairs, Mr. Amitabh Mathur, IPS (Retd.), Former Special Secretary, Research & Analysis Wing (R&AW), Vice Admiral Shekhar Sinha, Former FOC-in-C, Western Naval Command & Chief of Integrated Defence Staff and Mr. Navneet Rajan Wasan, IPS (Retd), Director General, Bureau of Police Research & Development for their support towards shaping this study.

Special thanks to the key discussants of all our consultations on encryption and cybersecurity, whose views have helped in shaping The Dialogue's research in this area. We express our sincere gratitude to Mr. Kazim Rizvi, Founding Director, The Dialogue without whose support, this report would not have been made possible. We also extend our gratitude to Ms. Avani Airan, Mr. Abhishek V., Mr. Bhavya Kapil Birla and Mr. Gyan Prakash Tripathi for their research assistance and Mr. Abhinav Kashyap for designing the report.

Glossary of Technical Terms

Term	Definition
APT	Advanced Persistent Threats are attacks from an adversary state with sophisticated resources and expertise that remains undetected in enemy computer servers for extended periods of time.
Asymmetric Encryption	Asymmetric Encryption is also known as Public-key encryption where the encryption key (public) and its decryption key (private key) are different. Only holders of the unique private key can decrypt messages sent using the public key.
BGP	Border Gateway Protocol is the postal service of the Internet. The BG protocol is responsible for finding the most efficient routes between autonomous systems for the data to travel from one point to the other.
CSAM	Child Sexual Abuse Material is the term used to define any content that depicts children involved in sexually explicit activity.
DNS	The domain name system is how computers convert human-readable domain names and hostnames to numerical IP addresses. When you type google.com into your web browser's address bar, your computer contacts its DNS server, and the DNS server replies with the numerical IP address of Google's server, which is what your computer connects to.
E2EE	The term 'end-to-end' signifies the two ends of a communication channel that are protected against snooping from anyone including the service provider.
Hashes	Hashing is the process used to assign a unique value to any particular content, so that it can be verified later for data integrity.
IP Layer	An IP address is a numerical address that corresponds to your computer on a network. When a computer wants to connect to another computer, it connects to that computer's IP address.
ISP	Internet Service Provider.
Key-Escrows	Key Escrows are an arrangement where encryption keys that provide access to plain text is stored and accessible by third parties (including government agencies).
LEA	Law Enforcement Agencies.
LDAP	Lightweight Directory Access Protocol is an open, vendor-neutral internet protocol that allows for data sets to be maintained in an organized manner that is often hierarchical. In a simplified sense, one can understand the LDAP as a database of information that can be used by authorized persons when needed.
Originator Traceability	Adding identifying information to any message that is sent to other parties using E2EE.

Term	Definition
Public Key Cryptography	Public Key Cryptography is an Asymmetric encryption technique.
SSL	Secure Sockets Layer is a protocol used to authenticate encrypted channels between computers. It is based on a certification format where SSL certified public keys are distributed widely and are matched with private keys to make an encrypted tunnel between the user and the software or website they wish to access. It was deprecated in 1999 being replaced by the Transport Layer Security (TLS) protocol.
SMTP/IMAP	<p>Simple Mail Transfer Protocol and Internet Message Access Protocol are used to transfer mails from the user through the server and to their destinations. SMT is also used for relaying or forwarding mail messages from one mail server to another which is necessary in cases where both ends of the transfer are on different platforms (Ex. Microsoft Outlook and Gmail).</p> <p>IMAP takes the SMT protocol to another level. It enables the storage of messages in a hierarchical order on the platform server (GMail's server) and allows for searchable contents across devices.</p>
The Signal Protocol	The Signal Protocol is a cryptographic scheme that allowed for E2EE messaging and other applications.
TCP	Transmission Control Protocol is a fundamental protocol in the Internet Protocol Suite and is responsible for sending data between the source and destination in a numbered and segmented format. TCP breaks the data being sent into small segments that are numbered and sequentially arranged at the destination so that the destination has the same data that was transferred from the source.
TLS	Transport Layer Security is the newer encryption layer built to be stronger than SSL. The 's' in Https indicates the presence of TLS encryption on the website. TLS authenticates the parties on either of the communication to verify they are who they claim to be.
UDP	User Datagram Protocol is a data transfer protocol that sends small data packages called 'Datagrams'. It sends packages of data very quickly but doesn't secure them as the transfer of packages between computers using UDP is done without establishing a connection. Thus, UDP although faster than TCP is less secure and is generally never used to transfer sensitive information.
VPN	Virtual Private Networks provide greater security online as they make private networks on a public network connection. They mask your IP address so that your actions are untraceable and thus, add a layer of security to your internet actions.

Introduction

In Prof. Balkin's Algorithmic societyⁱ, everyone seeks data, and not all want it legally, including both state and non-state actors. On an average day, India faces 375 cyberattacksⁱⁱ and the targets cover the entire spectrum from critical infrastructure, financial institutions, small businesses and individuals. In 2020ⁱⁱⁱ alone, there were 11,58,208 such incidents, a 3-fold increase from 2019. Given this reality, a robust approach where technical standards, laws and policies reinforce each other in the cyber domain is of utmost importance.

Encryption standards, laws and policies is one such area, where there is a vigorous debate, particularly on the topic of exceptional access to end-to-end encryption (hereinafter 'E2EE') private communications, used by applications based on the Signal protocol. While the current debate is framed as a binary of Privacy of users vs. Security of the State, in reality, it is a Security vs. Security debate, because any technology that has wide spread adoption becomes a critical infrastructure by itself, whether operated by the state or private entities.

The widespread adoption of E2EE across a wide variety of applications around the world thus becomes a universal critical infrastructure (standard), the shaping and protection of which is important for ensuring national security. This report assesses the E2EE debate from the Security vs. Security perspective, lays out the issues on both sides of the debate and also recommends a set of technical and policy measures to resolve them.

The first section examines the age-old encryption debate and how the technology has evolved over the years. It sets the context for the debate and discusses how dual-use encryption technology interacts with our constitutional ideals, national security, and economy.

The second section gives a qualitative and quantitative analysis on the importance that Indian citizens give to E2EE and documents how E2EE is no more a technology for secure messaging alone, but is the foundation to ensure security. The third section breaks down the key aspects of the E2EE technology for the reader to appreciate a holistic picture of the developments in the area of Encryption.

After setting this contextual foundation, the fourth chapter discusses the contours of the Indian surveillance regime. It documents the key challenges posed by E2EE to the existing surveillance capabilities, which data sets are already available and by following a process outlined in the report what more can be achieved. The experimental meta data analysis has been discussed with veterans from law enforcement agencies (hereinafter 'LEAs') and their views on the encryption debate and existing capabilities have also been highlighted.

It is on the basis of this extensive research that we recommend four key steps to ensure a progressive cybersecurity regime in India.

ⁱ Balkin. J.M. (2017, Sept. 20) Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation, UC Davis Law Review (2018), Yale Law School, Public Law Research paper No. 615, accessible from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3038939

ⁱⁱ India sees 375 cyberattacks everyday (Nov.17, 2020), PTI, <https://www.thehindu.com/business/india-sees-375-cyberattacks-everyday/article33110725.ece>

ⁱⁱⁱ Lok Sabha Starred Question No: 393 regarding Cyber Attacks (2021, Mar. 23) Answered by Shri. G. Kishan Reddy , Minister of State for Home Affairs. Accessible from <http://loksabhapublications.nic.in/questions/QResult15.aspx?qref=23441&lsno=17>

Table of Content

Executive Summary	1
Background	3
Cryptography and Warfare	3
Evolution of E2EE	4
What is the Debate?	5
Dual Use and Equity Processes	7
User Perspective – E2EE	9
Natural Experiments	9
Quantitative Studies	10
E2EE – Technology View.....	11
Law Enforcement View.....	14
Encryption as Law Free Zone	14
Analysis of Existing Capabilities Pre-E2EE	15
CMS	15
NETRA	15
NATGRID	16
LIMS	16
Investigations in an Encryption enabled society	16
What Metadata Analysis can reveal	17
Insights from Law Enforcement Interviews	21
Encryption Regulations.....	24
Technical measures and Categorization	24
Around the World	25
China	25
Australia	25
Belgium	26
Russia	27
Canada	27
Netherlands	28
Indian Laws Before IT Rules	29

The Law Matrix	30
Section 69 and Decryption rules	30
Section 91 of the Code of Criminal Procedure	31
IT Rules 2021	31
Traceability and the Puttaswamy Test	31
Backdoors and Traceability	32
Recommendations	33
Create an action plan for reducing encryption debt	33
Pause encryption hostile laws	33
Commit to surveillance reforms	33
A nationwide study to gauge the requirements of the LEAs & Intelligence Agencies	33

Executive Summary

Encryption in today's increasingly interconnected world is perhaps the only technology that provides us a sense of safety online. It is the most important enabler of free speech and indirectly thus, allows for the internet enabled communication to provide the same privacy we expect within the confines of what a physical conversation with another person offers, but in the digital world. Despite its pivotal importance in maintaining individual privacy, it does indeed hamper the state's ability to fulfil legitimate state security actions in certain cases. Most debates seem to address the topic in a Privacy vs. Security binary. We reached out to key stakeholders to get a more nuanced perspective of this debate. Post that we hosted semi-structured interviews with veterans from intelligence and law enforcement agencies to appreciate the challenges they faced in investigating cybercrimes and its interaction with end-to-end encryption technology. Our findings are listed below:

Firstly, weakening encryption technology through backdoors has short term benefits with long term consequences as the States cannot be secure if their citizens are not. Mandating backdoors either through legal or other means, has short term advantages for the intelligence agencies intent on targeting bad actors, but in the long term impacts their own citizens, thus not only nullifying the short term gains, but also creating exponential long term costs.

Secondly, in our interactions with former and serving members of India's intelligence community, we learnt that there is a significant lack of capacity on part of our intelligence infrastructure to analyze meta data as well as effectively use any decrypted content that even a backdoor may provide, should the state go through with such a legislation. In such a

scenario we recommend capacity building, preferably one without compromising E2EE, especially, when studies indicate that E2EE does not need to be done away with or weakened to achieve state objectives. It is thus crucial to stop legislating encryption hostile laws.

Thirdly, a net importer of weapons with no indigenous capability to build, maintain and service them, cannot be a credible military power. Correspondingly, a net importer of encryption technologies with no capability to build, break and maintain them, cannot be a credible cyber power. Given that more and more weapon systems and critical infrastructure are getting digitalized, a Nation-State which has encryption debt (like India) will always be vulnerable.

Similar to how a country in debt cannot hope to come out of it, by going deeper into debt, encryption debt cannot be reduced by becoming more hostile to encryption, as it erodes whatever cyber capabilities that exist, across the spectrum. Hence an action plan for reducing encryption debt is a must, and developing a E2EE stack offers a faster way to get there.

Fourthly, Indian Surveillance projects need to be reformed in order to abide by the Puttaswamy mandate while increasing their technical expertise to use meta data for meeting state security goals. This is recommended considering that making backdoors into E2E encrypted platforms is largely futile as it will only push illegal chats to other platforms offering encrypted communication.

Fifthly, while lawmakers globally have cracked down on E2E encryption as the key enabler of illegal and terrorist activities, this perspective is dismissive of the data available that speaks to the contrary. The SIRIUS EU Digital Evidence Situation Report wherein 325 experts from law enforcement agencies were interviewed, concluded that the key challenge was to access even the basic information on users owing to lengthy processes and varied cooperation

mechanisms of different companies. Accordingly, it is recommended that process and personnel for accessing meta data on presentation of legal warrant be defined for seamless investigations in India.

Sixthly, while the State's interest in regulating the spread of CSAM and fake news online are legitimate, the State shall endeavour to limit their actions within the confines of the Puttaswamy mandate and the proposed data protection framework. This requires adherence of data minimisation principle and passing a four fold test to put any valid restriction on an individual's privacy.

Seventhly, the State's proposed originator traceability requirement is not only contrary to the Puttaswamy mandate, but also is technically infeasible without fundamentally breaking E2E encryption. E2E encrypted messaging tools and applications are now being used by at least 400 million users in India, which is 25% of the population. Hence mandating 'originator traceability' which cannot be implemented without breaking E2E encryption, puts each of these users at risk.

Eighthly, there is a pressing need for routine sensitization as well as upskilling of all stakeholders in the criminal justice system about the complex dual-use dynamics that form the basis of encryption technology.

Lastly, there is a need to understand where our intelligence and law enforcement agencies are facing challenges, more importantly in terms of access. A study should be commissioned to assess the need of modern technology required by the said institutions. The need for advanced technology for lawful hacking and meta data analysis must be assessed and catered to all while adhering to the standards ruled by the Puttaswamy case. This is a key step towards increasing our capabilities to keep our citizens secure while ensuring that E2E encryption protect individual privacy the way it does currently.

1 Background

1.1 Cryptography and Warfare

The need for a formal discipline of cryptography pre-dates even the invention of the written word.¹ While the written word needs to follow a system of rules that allows others to learn to read and write, the spoken word is much more flexible and explains the proliferation of dialects, which may be hard for speakers from other dialects to understand. Hence creation of a new dialect to transmit messages was a common technique. One could simply prefix or suffix or insert a known syllable while speaking and create a dialect that is hard to comprehend when spoken rapidly (e.g. Pig Latin, Spanish Jerigonza, South Indian language dialects etc.).

Coded writing to convey instructions to armies and other agents of the state was normal practice and even finds mentions in the Greek epic poem, Iliad, where the hero Bellerophon was sent with a secret tablet, which contained a message to get rid of the bearer. Use of other approaches towards encryption such as the ‘Spartan Scytale’ and other simple substitution ciphers (replacing a character in a written language with some other character) existed even as far back as 7th Century B.C.

The first systematic cryptography treatment was done by the Arabs, particularly Abu Al Kindi.² The Tudor period in England was involved in active development of cryptography based on the work of the Arabs, but the first major

milestone of cryptography determining the outcome of war, happened in 1628, in the battle of Réalmont in 1628, where the defenders' message of dwindling supplies was broken, which resulted in their surrender.³

The invention of telegraph also created fertile grounds for further development of cryptography, as messages were sent via a broadcast medium than via specific targeting approaches. During the Napoleon era, multiple ciphers were used based on message priority with increasing complexity, but almost all of them were broken by the British.

The book ‘La Cryptographie Militaire’ was written in 1883, which detailed basic rules that any cryptographic system has to be follow, some of which are relevant even today. The invention of radio (another broadcast medium) created further need for the development of cryptography, just like telegraph a few decades earlier. MI-8, the American code breaking organization was formed to analyse and break all types of codes during WW-I but in the year 1929, it was shut down by Herbert Hoover, who said ‘Gentlemen do not read other Gentlemen’s mail’.⁴

WW-II also saw further development on cryptography, where words from hard to learn Navajo language were used for operational key words to phrases . This allowed the creation of unbreakable code that could translate three lines of English text in 20 seconds compared to 30 minutes, which was the norm with code breaking machines⁵. These code breakers played a critical role in the victory of the Iwo Jima

¹ Kahn, D. (1967). *The Code breakers*. The MacMillan Company.

² Smith, D. J. (2003, January). Codes and Ciphers in History, Part 1 - To 1852 . Retrieved from <https://web.archive.org/web/20050309020549/http://www.smithsriska.demon.co.uk/crypto-ancient.html>

³ Cohen, F. (1990). A Short history of Cryptography (Chapter 2). Retrieved from Istanbul Technical University: <https://web.itu.edu.tr/~orssi/dersler/cryptography/Chap2-1.pdf>

⁴ National Security Agency. (n.d.). The Black Chamber. Retrieved from <https://www.nsa.gov/about/cryptologic-heritage/center-cryptologic-history/pearl-harbor-review/black-chamber>

⁵ Office of the Director of National Intelligence. (n.d.). 1942: Navajo Code Talkers. Retrieved from <https://www.intelligence.gov/index.php/people/barrier-breakers-in-history/453-navajo-code-talkers>

battle.⁶

1.2 Evolution of E2EE

Given the deep association of cryptography with warfare, cryptographic algorithms were considered to be munitions and were tightly regulated by the Allied states, as it determined their technological superiority. The first dent on these regulations was made by cryptographers Whitefield Diffie and Martin Hellman, who proposed asymmetric encryption.⁷ Asymmetric encryption was a unique breakthrough because it not only allowed the algorithms to be public, but some portion of the key too.

Diffie and Hellman also note in the last paragraphs of the paper⁸ that “Skill in production cryptanalysis has always been heavily on the side of the professionals, but innovation, particularly in the design of new types of cryptographic systems, has come primarily from the amateurs” and hoped that “this will inspire others to work in this fascinating area in which **participation has been discouraged in the recent past by a nearly total government monopoly**” (*sic*).

The shift towards Public key cryptography led to the gradual weakening of the munitions regulations, as they were increasingly unenforceable and led to difference of opinion between law enforcement and civil society organizations in the United States and is often referred to as “Crypto Wars” of the 1990s. The then, FBI Director, Louis J Freeh, called for “responsible encryption”⁹ and “balanced

encryption” and pushed for “key-escrows” where law enforcement or a trusted third party holds the encryption keys and cited how “terrorists, spies and violent gangs” will use encryption products to carry out their activities in impunity.

What had changed was not the nature of the debate, but the public participation. This increased public focus ultimately made the Crypto-Wars unwinnable in the short-term for law enforcement agencies in the United States. The wide-spread adoption of encryption by the general public was made possible through the introduction of and user-friendly product for day-to-day encryption needs called the Pretty Good Privacy (hereinafter ‘PGP’) by cryptographer and civil liberties icon Phil Zimmerman.

The shake-up that was the 90s for the world of encryption can be best summed up in Zimmerman’s own words¹⁰ – “Advances in technology will not permit the maintenance of the status quo, as far as privacy is concerned. The status quo is unstable. If we do nothing, new technologies will give the government new automatic surveillance capabilities that Stalin could never have dreamt of. **The only way to hold the line on privacy in the information age is strong cryptography**” (*sic*).

The crypto-wars had been a stalemate with most of the export-control regulations going away, but the 9/11 attacks brought forth the Patriot Act¹¹, which allowed expanded surveillance powers for law enforcement including sneak and peak

⁶ Even more fascinating accounts about how cryptography swayed battle outcomes, can be found in the book by David Kahn, *The Code breakers*.

⁷ Whitefield, D., & E. M. H. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6), 644-654.

⁸ Ibid.

⁹ Freeh, L. J. (1996, July 25). Regarding Impact of Encryption on Law Enforcement and Public Safety. Retrieved from <https://nsarchive.gwu.edu/document/22248-document-02-louis-j-freeh-director-federal>

¹⁰ Zimmermann, P. (1991, June). Why I wrote PGP. Retrieved from <https://www.philzimmermann.com/EN/esays/WhyIWrotePGP.html>

¹¹ Government, U. (2001). The Patriot Act. Retrieved from <https://www.govinfo.gov/content/pkg/PLAW-107publ56/html/PLAW-107publ56.htm>

warrants, roving wiretaps, pen registers, trap and trace devices and allowed subpoenas to be issued to all service providers for data access.

The extent of this wide range access to technology resulted in mass surveillance programs that touched many service providers, as revealed by Edward Snowden.¹² It revealed that there are programs such as XKeyscore that collected all data that any user does online, Prism which allowed the National Security Agency (hereinafter ‘NSA’) access to any non-US citizen’s data in companies such as Google, Microsoft, Yahoo. The depth of access resulted in more user demands for privacy, which the government of the day cannot break by leaning into the service provider.

The renewed user demand for service provider immunity was achieved by embracing another cryptographic innovation – The Signal Protocol.¹³ By combining public key cryptography, symmetric encryption and ephemerality, it allows full control of encryption keys to the end users (or devices) without the intermediary or service provider knowing about them and only playing the role of a dumb message forwarder.

1.3 What is the Debate?

Given the close association of encryption with warfare, the debate on encryption is always framed as Security vs Privacy, where Security means Security of the State, while Privacy means Individual Privacy. Once put in this frame, the resolving mechanism for the tension between these two aspects becomes one of balancing. The framework of balancing hinges on a three-legged stool:

- a. The assumption of rational actors who will always think about long term impact of their actions, guided

by a deliberative approach, created, nurtured and supervised through institutions which take the long term view.

- b. There is always a technical solution or capability that allows the balancing, where harm in one area will not necessarily overrun any benefits that accrue in other area.
- c. A policy framework that is transparent to all the actors with scrutiny on results which in turn allow further evolution of the framework.

With this frame in place, it is easier to understand the various approaches that have been attempted so far as described below:

- i. A technical architecture in the form of a ‘back-door’ access or introduction of ability to remove anonymity for law enforcement agencies on major communications platforms is then proposed with access control measures on who gets to use it with various oversight mechanisms which may or may not include judicial oversight.
- ii. User-side checking at the device level through automated means or through a reporting mechanism.
- iii. Compelled disclosure by the User by unlocking the device on a case by case basis with judicial oversight.

The fundamental assumption about the back-door approach is that once built, no one else can use it because there are robust safeguards through access control. However this assumption does not hold in the cyber domain because all back-doors are simply thought structures expressed in programmatic form and hence can be reverse engineered by any motivated adversary having sufficient resources to

¹² Ball, J. (2013, August 13). The NSA Files. Retrieved from <https://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations>

¹³ Mirlinspike, M. (2013, November 13). Advanced cryptographic ratcheting. Retrieved from <https://signal.org/blog/advanced-ratcheting/>

find the back-door.

Consider an example of how exceptional access systems can be built using ‘key escrow’, where law enforcement or intelligence agencies have the master key. There are few distinct problems with this approach¹⁴:

1. Risk of Security incident – Any organization that holds the keys can be subject to a security incident which means that exceptional access is no longer exceptional.
2. Certainty of exploitation – All known key escrow systems have had known vulnerabilities and increase operational complexity as the number of moving parts increase exponentially.
3. Cost overruns – Both the above factors increase operational costs and hence fall apart once these costs could not be borne by the entities or not cross subsidized by the state.

Another approach proposed by law enforcement to handle the issue of forbidden content [e.g. Child Sex Abuse Material (hereinafter ‘CSAM’)] freely exchanged via encrypted applications such as messaging is client side scanning. This typically involves creating a capability where a set of hashes are sent to the device and message content is compared against these hashes and authorities are informed if there is a match. The risks involved in this approach are very obvious:

- a. Anyone can reverse engineer the scanning application and hence obtain the hashes, which enables them to side step the scanning by creating images that do not match the scans. This means, the only way to avoid the side step is locked-in devices, which do not allow inspection. Given that inspection is important to security research this would further curtail defensive

measures against vulnerabilities.

- b. The management of the hash database and access control to it is both a policy and technical issue, as it will keep growing in size. Given that we know that such a database can never be protected fully from malicious access, the risk of it being used by adversaries to understand content exchanged within the country always exists.

Both these above examples indicate that the balancing exercise between Privacy vs Security is deeply flawed and hence untenable in the cyber domain. It is in fact a balancing exercise between Security vs Security, where the context of Security is the Security of the Nation State.

¹⁴ Abelson, H., Anderson, R., Bellovin, S. M., Benolah, J., Blaze, M., Whitfield, D., . . . Landau, S. (2015, July 6). Keys Under Doormats: Mandating insecurity by requiring government access to all data and communication. Retrieved from <http://dspace.mit.edu/handle/1721.1/97690>

1.4 Dual Use and Equity Processes

All tools and technology in the cyber domain are dual use. The term ‘dual use’ in cyber domain has multiple inter-related meanings. In trading terminology¹⁵, it means “goods, software and technology that can be used for both civilian and military applications” and are typically under export control. Encryption however is also both an offensive and defensive weapon and can be deployed by any state or non-state actor in both forms.

The simultaneous binary nature of encryption also implies that any attempt to weaken or restrict encryption to enable data collection or spying on foreign adversaries by state actors also weakens defensive capabilities of the state, as it allows adversaries to use these techniques on their own residents. This dual nature creates fault lines and incoherence in policy making, as it requires a complex equity process to weigh the long term impact of policy interventions.

For instance, consider the Juniper networks breach.¹⁶ This was made possible because the NSA leaned on the company to add an encryption algorithm in their routers in the year 2008, that had a known back-door, if they had to qualify for future contracts with military and intelligence services. The incorporation of the algorithm, allowed the NSA to decrypt communications of foreign targets who used Juniper’s products, but in 2012, this was spotted and hijacked by the Chinese APT (Advanced Persistent Threat) group APT-5, which changed the algorithm’s parameters that allowed it to bypass encryption and was used to

target other companies and even the US government later.

Mandating back-doors either through legal or other means, as this incident reveals, has short term advantages for the intelligence agencies intent on targeting foreign subjects, but in the long term, it impacts their own citizens, thus not only nullifying the short term gains, creating exponential long term costs.

A similar argument applies for a spate of proposed laws and regulations that have been introduced recently world-wide¹⁷. Broadly these could be classified as:

1. Mandatory minimum or maximum strength of keys or algorithms.
2. Licensing or registration of algorithms.
3. Obligations on providers to assist decryption and/or identification.
4. Obligations on Individuals to assist decryption.

While the first 3 policy interventions are broad based and affect every resident within a jurisdiction, the last intervention only affects specific individuals and is targeted. However none of the first 3 interventions are backed by an equity process that carefully weighs the pros and cons across a longer time frame.

The need for an equity process is further reinforced by a working paper,¹⁸ put out by the Encryption Working Group, which argues that “Security can be defined in a variety of ways, such as national security and public safety, cybersecurity and privacy, or security from hostile or oppressive state actors. These interests are all priorities. All parties—including

¹⁵ European Commission. (2021, July 14). Dual-use trade controls . Retrieved from https://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/index_en.htm

¹⁶ Jordan, R. (2021, September 2). Juniper Breach Mystery Starts to Clear With New Details on Hackers and U.S. Role. Retrieved from <https://finance.yahoo.com/news/juniper-breach-mystery-starts-clear-130016591.html>.

¹⁷ Global Partners Digital. (n.d.). World map of encryption laws and policies. Retrieved from <https://www.gp-digital.org/world-map-of-encryption/>

¹⁸ Carnegie Endowment Encryption Working Group. (2019, September 10). Moving the Encryption Policy Conversation Forward. Retrieved from <https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573>

those who typically make rights-based arguments and those who typically make national security-and law enforcement-based arguments—are concerned with thwarting malicious actors, criminals, terrorists, and foreign agents, and investigating and preventing crime and threats to public safety. Encrypted technologies also support and enhance not only the speech and communications of individuals and communities but also the missions and operations of national security and law enforcement. “**The key is determining how we can jointly figure out how to weigh competing security responsibilities based on factual analysis and more informed cost/benefit assessments.**” (*sic*)

However, not every jurisdiction engages in this complex process before passing laws or notifying regulations on encryption, but instead circumvent the process by framing it as a simple problem of choosing between binaries.¹⁹ For instance, the 2018 statement of the Five eyes alliance,²⁰ exhorts service providers to voluntarily establish lawful access solutions in their products and on failing it warns that they may pursue technological, legislative and other measures to achieve the same. The statement however is not signed by the intelligence agencies of the Five Eyes alliance,²¹ thus illustrating that at least one key Stakeholder does not agree to it, as it does not conform to the equity process.

¹⁹ Venkatnarayanan, A. (2021, Mar.10) Stopping the encryption tsunami with legal straws does not make a cyber power, The Print. Retrieved from <https://theprint.in/theprint-valuead-initiative/stopping-the-encryption-tsunami-with-legal-straws-does-not-make-a-cyber-power/618929/> See also Azad,Y. & Venkatnarayanan,A. (2021, Nov.24) For investigations, metadata is enough. Uphold privacy, Hindustan Times. Retrieved from <https://www.hindustantimes.com/opinion/for-investigations-metadata-is-enough-uphold-privacy-101637769624433.html>

²⁰ Department of Home Affairs, Australian Government. (2018). Statement of Principles on Access to Evidence and Encryption. Retrieved from <https://web.archive.org/web/20180925154820/https://www.homeaffairs.gov.au/about/national-security/five-country-ministerial-2018/access-evidence-encryption>

²¹ Landau, S. (2018, September 26). The Five Eyes Statement on Encryption: Things Are Seldom What They Seem. Retrieved from <https://www.lawfareblog.com/five-eyes-statement-encryption-things-are-seldom-what-they-seem>

2 User Perspective -E2EE

E2EE is slowly becoming the benchmark of secured communication and data transfer to protect both business and private communications. This section analyses how users view it and how their thinking has evolved over time, as it creates a baseline that will inform the success of any policy intervention.

2.1 Natural Experiments

User adoption of any technology including E2EE is governed by societal factors, where a large number of participants engage in activities that include pushing out commercial standards, creating new products, creating legal regimes and engaging in advocacy. While the short term impact of these activities might be negligible on their own, taken together they create a baseline over time, that becomes more dominant and entrenched.

For instance, the debate in India about privacy was largely due to the rolling out of the Aadhaar project, which envisaged an outcome, where all aspects of the residents' life is connected to a single identifier, which would be issued based on biometric deduplication of finger prints and IRIS scans.

The union government argued in the Supreme court, that there is no fundamental right to privacy in the early hearings on the Aadhaar matter.²² The

issue was then referred to a nine-judge constitutional bench, which then ruled that privacy is indeed a fundamental right.²³

The court then heard the original Aadhaar issue again for a period of over four months that brought forth more debates on the public forum about privacy and other facets such as consent. The final judgement had an interesting and controversial take on the issue of consent - It allowed holders of Aadhaar numbers that were issued before the promulgation of the Aadhaar act, the right to apply for deletion and deactivation, but made that right infructuous as the majority held that the Aadhaar numbers are required for many services.

Post the Aadhaar experience, it is evident that at least some sections of the Indian citizenry has a significantly altered baseline on how they view privacy issues. This was why even a perceived threat to their privacy, owing to misinformation around WhatsApp's new Privacy Policy that personal texts can also be accessed by the platform, led many to join other platforms like Signal.²⁴

Recent events indicate that this altered baseline on privacy also creates resistance on projects rolled out by the government. When the Covid pandemic struck, the government created a new app called 'Aarogya Setu' for contact tracing and made it mandatory for services,²⁵ using the playbook it adopted for Aadhaar. It even urged smart phone makers to pre-install it. However privacy concerns forced it to open source the app, but it was immediately

²² Pahwa, N. (2015, August 6). "Violation of privacy doesn't mean anything because privacy is not a guaranteed right" – Gol. Retrieved from <https://www.medianama.com/2015/08/223-privacy-india-aadhaar/>

²³ Krishnan, M. (2017, August 24). Puttaswamy: Right to Privacy is a Fundamental Right under Article 21, Supreme Court. Retrieved from <https://www.barandbench.com/news/right-privacy-fundamental-right-supreme-court>

²⁴ Mathi, S. (2021, July 9). WhatsApp puts new privacy policy on hold until data protection bill comes into force: Report. Retrieved from <https://www.medianama.com/2021/07/223-whatsapp-privacy-policy-on-hold/>

²⁵ Indian Express Tech Desk. (2020, May 3). Aarogya Setu mandatory: Who all must download the app right away. Retrieved from <https://indianexpress.com/article/technology/social/aarogya-setu-app-mandatory-contact-tracing-app-6389284/>

analysed and shown as not genuine,²⁶ as the repository has not been updated after that. Public litigation petitions were then filed against mandating the use of the app, which led the courts to rule that it cannot be mandatory for service access.²⁷

Qualitative studies also affirm the fact that people value privacy as a priceless right contrary to common perception and want to keep their messaging history and switch to other messaging applications, if the providers are not trustworthy.²⁸

2.2 Quantitative Studies

The most detailed analysis of user perception around the specific problem of use of E2EE in messaging applications was done by CUTS International.²⁹ Its key findings are reproduced below as it is:

1. Out of a sample size of 2,113 WhatsApp users, only 1 in 250 users or a total of 8 users (0.37%) understood the role of E2EE in securing their messages.
2. Only 61% of the respondents believed that their chats are E2EE.
3. 57% of the respondents were under the misconception that they get personalised ads on digital platforms, based on their chats on E2EE Instant Messaging services.
4. Respondents were likely to reduce exchanging different information with different contacts by 19%, if E2EE is removed.
5. Respondents were 27% more likely to

completely stop exchanging different information with different contacts, if E2EE is removed.

While it may be possible to conclude that E2EE is under possible threat because only 0.37% of the survey respondents understand its significance, that would be an oversimplification, because many of these users ported to Signal, after being subjected to a barrage of misinformation that WhatsApp's E2EE was being meddled. This clearly demonstrates that people are now very sensitive about E2EE.

Hence one way to understand the figures of 19% (reduce information exchange) and 27% (stop information exchange) if E2EE was outlawed is that, it represents a latent demand for the option of having private communications without being snooped upon, even though only a handful understand the technology that underpins it. The survey further shows that given an option between E2EE and non E2EE on messaging, close to 78% chose E2EE and a large percentage are even willing to pay for it.

As almost all the respondents of this survey are of voting age, the 78% preference on E2EE, thus represents a barrier that any elected government must pass through to outlaw E2EE usage.

²⁶ Pandharipande, N. (2020, June 15). Aarogya Setu not 'open source' in real sense, claim cybersecurity activists, say server code must be made public. Retrieved from <https://www.firstpost.com/tech/news-analysis/aarogya-setu-not-open-source-in-real-sense-claim-cybersecurity-activists-say-server-code-must-be-made-public-8480011.html>

²⁷ Agarwal, A. (2020, October 19). Without law, govt cannot deny services for not installing Aarogya Setu: Karnataka High Court. Retrieved from <https://www.medianama.com/2020/10/223-govt-cannot-denry-services-aarogya-setu-karnataka-hc/>

²⁸ Dvara Research. (2017, November 16). Privacy on the Line. Retrieved from <https://www.dvara.com/research/wp-content/uploads/2017/11/Privacy-On-The-Line.pdf>

²⁹ CUTS International. (2021, March). Understanding Consumers Perspective on Encryption in India. Retrieved from <https://cuts-ccier.org/pdf/survey-finding-understanding-consumers-perspective-on-encryption.pdf>

3 E2EE- Technology View

Technology stacks in the networking space are commonplace because they are not only easier to represent hierarchically, but also make implementation simpler. The layering allows multiple applications to be developed at a rapid pace over time. The interesting aspect is that for the above stack to work, many layers of intermediaries are essential, even at the application level.

Consider Email which runs over the Simple Mail Transfer Protocol/Internet Message Access Protocol (hereinafter ‘SMTP/IMAP’) or Voice calls which runs over SIP protocol. All these require intermediaries for either end points or users to discover each other. Intermediaries in this digital ecosystem hence perform the following functions:

1. Route packets on Internet Protocol Layer (hereinafter ‘IP layer’).
2. Discover information about other parties (Border Gateway protocol (hereinafter ‘BGP’) at IP layer, Mail Exchanger (hereinafter ‘MX’) records via Domain Name System (hereinafter ‘DNS’), Address information via Lightweight Directory Access Protocol (hereinafter ‘LDAP’) etc.)
3. Provide the required services for a particular operation (Voice Over Internet Protocol (hereinafter ‘Voip’) Service, Calendar Service, Contact Service, Email Service, Storage etc.)

As a result of providing these functions, intermediaries collect data and meta data about networks, systems, and participating users and can either use such collected data to improve the quality of their services they provide or build additional services that use this data or can provide this data to others. The addition of Secure

Sockets Layer (hereinafter ‘SSL’) and Transport Layer Security (hereinafter ‘TLS’) (commonly referred to as encryption) into this mix, only changes the connectivity pattern, but does not alter the data and meta data collection by the intermediaries.

Hence even when SSL/TLS is implemented between the user/systems and the intermediaries, there is always a possibility that, they may turn rogue and hand over user data to others for commercial reasons or may be asked to do so by sovereign States exercising state power over them.

E2EE is one way to design the network stack so that, the intermediary is a hostile entity and only does the forwarding of packets from a known source to a known destination (IP layer) and nothing else. In this design, the intermediary only provides the transport layer at an infrastructure level and other applications are built on top of this layer by collaborating clients, without the intermediary knowing anything about these applications.

To understand the E2EE stack, it is necessary to understand the network stack before E2EE in some detail. Most of the applications use the network stack as shown below and are only aware of the transport layer (SSL/TLS, Transmission Control Protocol (hereinafter ‘TCP’)/ User Datagram Protocol (hereinafter ‘UDP’ etc.)

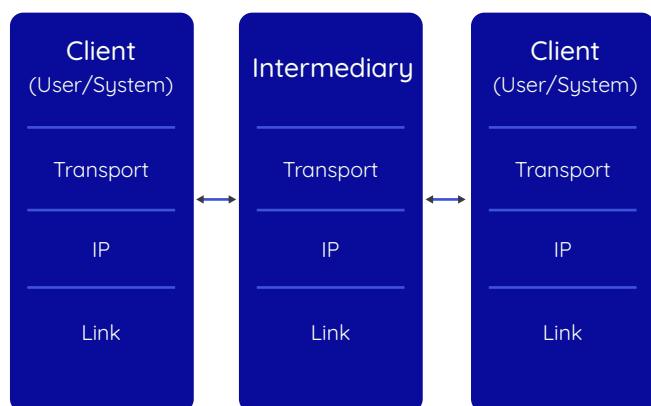


Figure No. 1

This holds true even when solutions like Virtual Private Networks (hereinafter ‘VPN’) and anonymizing solutions like The Onion Router (hereinafter ‘Tor’) are used. If the intermediary were a VPN

provider, all packets are intercepted at the IP layer by a VPN client and is routed via the intermediary to the destination. In the case of Tor, the application package also contains the network stack and does not use the default network stack that ships with the Operating system, as this is the only way to deliver on the promise of full anonymity. The recently announced update by Apple,³⁰ which provides two relays that assign a random IP and a proxy which then fetches the content from the destination and delivers it to Safari browser can be viewed as a “TOR” service for Apple users. However, unlike TOR, which uses a different network stack packaged along with the application, Apple has embedded the privacy-preserving network stack into its devices, as it has full control on the operating system that ships with the device.

These services offer a framework for us to think about E2EE applications in terms of network stack. By merely changing the transport layer of the network stack, new applications can be built, which offer privacy protection features, where even the intermediary is not aware of the data that passes through them. In the case of messenger applications like Signal, WhatsApp and Threema, the client applications create a new transport stack (E2EE) on top of existing transport stack (TCP, UDP) and overlay the applications on top of this stack such as instant messages, video calling, voice calling, live locations as shown below:

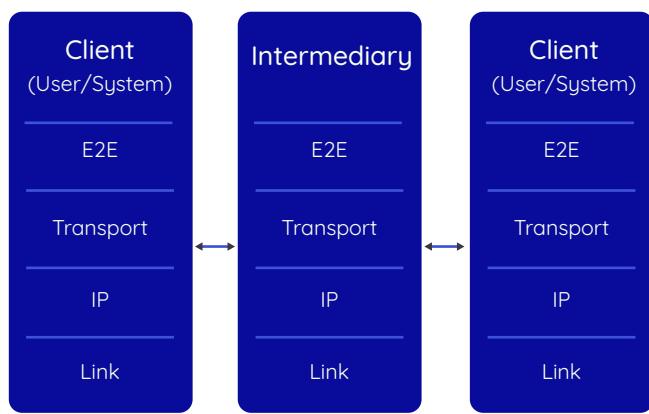


Figure No. 2

³⁰ Apple. (2021, June 7). Apple advances its privacy leadership with iOS 15, iPadOS 15, macOS Monterey, and watchOS 8 . Retrieved from Apple News room: <https://www.apple.com/newsroom/2021/06/apple-advances-its-privacy-leadership-with-ios-15-ipados-15-macos-monterey-and-watchos-8/>

³¹ See <https://github.com/ockam-network/ockam>

The functionality offered by the E2EE layer is the Signal protocol that allows applications on both sides to send encrypted message payloads to other clients, by merely specifying a destination, where the encryption key per payload (or a session) is rotated continuously to allow Perfect Forward security. The E2EE intermediary (network) layer hence is application blind and can allow any number of custom applications at a rapid pace without the involvement of the intermediary.

There are already custom libraries that allow any application to incorporate the E2EE network stack.³¹

These libraries provide the required code for both the intermediaries and the users/services/clients and even support multiple intermediaries (via hops) just like the IP layer, thus allowing federated and decentralized service providers, all forming a web of intermediaries but are still privacy oriented and application blind. The evolution of these libraries that provide a network stack layer that allows E2EE is the next logical development of the internet stack and would be based on a business model that offers privacy by design (e.g., Apple) as a premium offering.

It is possible to envisage Internet of Things (hereinafter ‘IoT’) and smart home devices embracing this stack where devices can be controlled by smart phones via apps, without any personal data ever kept or stored by the intermediary, thus obviating the need to invest on data protection and data management technologies, which are at best mitigating strategies. E2EE thus offers immediate ROI in terms of cost savings for device vendors, who can run a lean intermediary infrastructure without having to comply onerous data protection regulations.

Workaround to E2EE Technology

Solution	Definition	Disadvantages
 Traceability	Enables the government/intermediary to identify the first originator of an illegal communication.	<ul style="list-style-type: none"> Absolute first originators cannot be traced via this method. Against the fundamental nature of E2EE. Leads to architectural vulnerabilities which can be exploited by bad actors. Is not perfect and can be circumvented by savvy criminals.
 Backdoor	Change to an encrypted system to allow exceptional access to encrypted communication when needed.	<ul style="list-style-type: none"> Once weakened for LEAs, even bad actors (including foreign states) will learn to adapt and exploit.
 Key Escrow	Keys to encrypted communication are kept by a company, Government or a third party for safekeeping and ready to access when needed.	<ul style="list-style-type: none"> Renders the company and its users susceptible to cyber vulnerabilities owing to creation of 'honeypots'. Features like perfect forward secrecy wherein the key is changed after every transaction will lose its essence. It will be too onerous for the company to maintain keys.
 Client Side Scanning	Scanning a client's data and flagging content that is determined to be objectionable	<ul style="list-style-type: none"> Can be misused to micro target advertisements, or surveil message content. A slippery slope to a China Model (Refer to section 5.2.1). Mass Surveillance tool as every message is reviewed instead of a targeted one.
 Ghost Proposal	Where a third party is silently added as a participant to a communication.	<ul style="list-style-type: none"> Will lead to a chilling effect on speech as their presence is never intimated to the other two parties. Against the very nature of E2EE.
 Digital Signatures	Authenticates the exchange of messages between two parties & prevents tampering of messages.	<ul style="list-style-type: none"> Sender of a particular communication may be identified but that sender may not necessarily be the 'first originator'. Identity theft/digital impersonation may hinder investigation. Inter-platform traceability through digital signatures is complex
 Metadata Analysis	Metadata contains information about the communication, but not the contents of the communication itself.	<ul style="list-style-type: none"> Metadata if compromised, can give deeper insights into people than actual message content sometimes. Use of metadata should be governed by the data minimization principle and the test ruled in the Puttaswamy case.

Table No. 1
Analysing the National Security Implications of Weakening Encryption

4 Law Enforcement View

4.1 Encryption as Law Free Zone

LEA tasked with maintaining national security (or a narrower mandate of cyber-security) have approached the problem of encryption from the urgent perspective of “going dark”³² on the critical surveillance fronts. Arguing that E2EE makes it systematically impossible to predictably access the content of individual messages, LEA have highlighted the rise in use of E2EE communication tools as a critically important trend hampering the effectiveness of their surveillance ambit and thus endangering public safety.

Investigative agencies³³ and parliamentary committees (in India)³⁴ have advanced arguments that cite an increasing number of investigations or cases that are running into use of E2EE communication tools by criminal actors.

Encryption tools being used by fundamentalist groups is often a core concern for counter-terrorism operations, but the futility of trying to regulate encryption, when tools for using PGP and other open source software that already exists, in which back-door insertion can

³² Comey, J. (2014, October 16). Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? Retrieved from <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course>

³³ Ibid.

³⁴ Adhoc Committee Rajyasabha. (2020, January 25). 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. Retrieved from https://rajyasabha.nic.in/rsnew/Committee_site/Committee_File/Report-File/71/140/0_2020_2_16.pdf

³⁵ Graham, R. (2016). How Terrorists Use Encryption. CTC Sentinel, 9(6), 20-26.

³⁶ Dearden, L. (2015, September 16). British Isis jihadists 'had phones hacked by GCHQ' before they were killed by drone strikes. Retrieved from <https://www.independent.co.uk/news/uk/home-news/british-isis-jihadists-had-phones-hacked-gchq-they-were-killed-drone-strikes-10503076.html>

³⁷ Australian Federal Police. (June, 8). AFP-led Operation Ironside smashes organised crime. Retrieved from <https://www.afp.gov.au/news-media/media-releases/afp-led-operation-ironside-smashes-organised-crime>

³⁸ Supra at 35.

³⁹ Duckett, C., & Barbaschow, A. (2017, July 14). The laws of Australia will trump the laws of mathematics: Turnbull. Retrieved from <https://www.zdnet.com/article/the-laws-of-australia-will-trump-the-laws-of-mathematics-turnbull/>

be easily spotted by anyone, has been acknowledged.³⁵ While encryption may be unbreakable, it does not mean there are no choices but to give up, as actors often commit operational security mistakes, that allows end points to be compromised.

End point hacking is always available as an option and in some cases has been quite effective against single targets.³⁶ There is also an option of infiltration, where a compromised encryption application is successfully marketed as safe, has widespread adoption within the criminal network, and is then used to reel in the entire network.³⁷

However, the prevailing view within law enforcement is that, widely available ready-to-use encryption tools often operate outside the legal framework and needs to be reined in, as it increases the cost of performing investigations and also reduces their effectiveness in obtaining convictions.³⁸ This is why the Australian Prime Minister, Malcolm Turnbull, remarked “The laws of Australia will trump the laws of mathematics”.³⁹

4.2 Analysis of Existing Capabilities Pre-E2EE

There are at least 4 known surveillance projects that the Indian government runs

within its jurisdiction⁴⁰.

- Centralized Monitoring System (hereinafter ‘CMS’)
- Network Traffic Analysis System (hereinafter ‘NETRA’)
- National Grid (hereinafter ‘NATGRID’)
- Lawful Intercept and Monitoring Project (hereinafter ‘LIM’)

4.2.1 CMS

The CMS project was first announced in the Year 2009 and was extensively discussed in the Department of Telecom’s annual reports in the Years 2011⁴¹ and Years 2012-13.⁴² The surveillance platform covers all the Internet Service Providers (hereinafter ‘ISPs), Telecom Service Providers (hereinafter ‘TSPs’) and even Private leased lines providers (used for connecting geographically distant offices) and allows surveillance to be carried out by both the state governments and central agencies.

It is capable of intercepting voice calls, SMS, MMS and Faxes sent via 2G, 3G, 4G networks across any two parties once configured and allows targets to be monitored automatically once a warrant is issued and verified by a DoT official without any involvement of the ISPs, TSPs or others. The design hence purposefully reduces the chance of anyone but the officials knowing if the target is under surveillance.

It also offers full spectrum search options including SMS, calling/called parties, time duration and call types and can perform advanced analysis capabilities, which include:

- Day night pattern analysis - Map if a target’s calls is distributed towards the time of the day.
- Chain reflection - Trace through a call sequence and map if it leads to more calls from the called party.
- Link analysis - Map the entire network of the target and the phone numbers of every contacted party.
- Threshold analysis - Determine suspicion profiles based on number of calls made.

CMS also allows call graph analysis to be combined with location, tower and other data to derive intelligence about the targets using metadata only.

It however suffers from a critical issue – most of the calls and messages are now moving towards E2EE and hence surveillance is only viable, if targets do not use E2EE. Thus the surveillance platform built at great cost is effective, only if the targets can be downgraded to the pre-internet era with 2G networks and voice calls.

4.2.2 NETRA

NETRA’s stated purpose is to analyse network traffic and derive intelligence.⁴³ For that purpose, it uses pre-set key word filters to analyse traffic and flag suspicious network flows. With known limits for traffic storage at 300 GB for analysis, it was never going to be sufficient to keep up with the ever increasing traffic growth, even in an era (2014), where TLS encryption was not near universal.

With the growth of TLS and E2EE, the utility

⁴⁰ Tiwari, U. (2017, January 20). The Design & Technology behind India’s Surveillance Programmes. Retrieved from <https://cis-india.org/internet-governance/blog/the-design-technology-behind-india2019s-surveillance-programmes>

⁴¹ Department of Telecom. (2012). Annual Report, 2011-12. Retrieved from https://dot.gov.in/sites/default/files/AR%20English%2011-12_0.pdf

⁴² Department of Telecom. (2013). Annual Report 2012-13. Retrieved from [https://dot.gov.in/sites/default/files/Telecom%20Annual%20Report-2012-13%20\(English\)%20_For%20web%20\(1\).pdf](https://dot.gov.in/sites/default/files/Telecom%20Annual%20Report-2012-13%20(English)%20_For%20web%20(1).pdf)

⁴³ Gupta, R., & Matoo, S. (2017, January). Internet Traffic Surveillance & Network Monitoring in India: Case Study of NETRA. Retrieved from https://www.researchgate.net/publication/312380082_Internet_Traffic_Surveillance_Network_Monitoring_in_India_Case_Study_of_NETRA

of NETRA for broad based surveillance diminishes significantly to the point of being irrelevant, when coupled with its known scaling issues.

4.2.3 NATGRID

The NATGRID project aims to create a single intelligence network by combining data sources from various sources ranging from existing government databases from welfare delivery, tax databases, immigration records, travel databases and state-wide crime databases. The idea behind the NATGRID is that the quality of intelligence increases, when data from various sources can be combined using Master Data Management (hereinafter 'MDM') techniques, normalized and analysed.

Even normal encryption changes the dynamics of NATGRID, if service providers and other government organizations start encrypting data, as it makes MDM techniques obsolete. Even Key escrow mechanisms make it complex to manage the data sources, as every data source needs to be decrypted and then analysed. For a project that has already seen multiple bureaucratic delays and cost overruns, encryption hence is an additional hurdle.

Perhaps that is one reason, why the draft encryption policy envisaged all service providers to always keep a plain text copy of any encrypted data for LEA access.⁴⁴

4.2.4 LIMS

The Lawful Intercept and Monitoring systems (LIM) refer to legally approved systems installed and managed by ISPs in order to monitor and track communications

online by select people, sections of people, or any communications that use a certain phrase or terminology as decided and provided to the TSP/ISPs to highlight and produce for further governmental perusal. It is primarily run by the Centre for Development of Telematics (hereinafter 'C-DoT') in the Ministry of Telecom since 2011. However, LIMs are dependent on ISPs to manage and implement real-time monitoring of the Indian Internet Traffic for certain interactions as the government may notify them.

These Systems provide for intercepting any communication lines that use Indian servers whether telecommunication or internet based. They also allow for key word searches of all data that flows in through Indian servers.⁴⁵

While the interceptions are only allowed when requirements under section 69 of IT Act and section 5 of the Indian Telegraph Act read with section 419A of the same act are fulfilled, reportedly, these guidelines are not always followed, and ascertaining an exact number is impossible due to there being no legally mandated record-keeping of such data.⁴⁶ However, the rapid adoption of E2EE across sectors have gravely damaged the effectiveness of LIMs as they have made it harder for such monitoring services to snoop in when needed.

4.3 Investigations in an encryption enabled society

Encryption technology is by its very nature dual-use. The phone used for connecting families and friends can also be used to hatch conspiracies or to harass another. Transitioning from a pre-E2EE age to a world with ubiquitous access to E2EE technology, many have raised concerns on the challenges faced in lawful interception

⁴⁴ Pahwa, N. (n.d.). Updated: India's draft encryption policy puts user privacy in danger. Retrieved from Medianama: <https://www.medianama.com/2015/09/223-india-draft-encryption-policy/>

⁴⁵ Tiwari, U. (2017, Jan. 20) The Design & Technology behind India's Surveillance Programmes, Centre for Internet & Society, accessible from https://cis-india.org/internet-governance/blog/the-design-technology-behind-india2019s-surveillance-programmes#_ftnref19

⁴⁶ Singh, S. (2013, Sept. 08) Govt. violates privacy safeguards to secretly monitor Internet traffic, The Hindu, accessible from <https://www.thehindu.com/news/national/govt-violates-privacy-safeguards-to-secretly-monitor-internet-traffic/article5107682.ece>

of encrypted communications.

On the other end, use of E2EE has been found not only crucial for user privacy but also for national security. A pertinent question is whether E2EE obviates LEAs from fulfilling their duty? The SIRIUS EU Digital Evidence Situation Report wherein 325 experts from law enforcement agencies were interviewed opines otherwise. It concluded that the key challenge was to access even the basic information on users owing to lengthy processes and varied cooperation mechanisms of different companies.

The report highlights that in most cases plaintext is not required and access to meta data is sufficient. Among key challenges faced by LEAs per the EUROPOL report is that of the tedious process from accessing even meta data.⁴⁷ Project Trojan Shield conducted jointly by USA, along with LEAs from other countries led to over 500 arrests without weakening encryption for all.⁴⁸ Herein the LEA turned a known criminal to sell a compromised encrypted platform in criminal syndicates which ultimately lead to multiple arrests. This is testamentary to what LEA's ingenuity can achieve.

Access to more data is not always the answer, as it only worsens finding the needle in the haystack, by making the haystack bigger and the needle smaller. The credence of NSA's all-encompassing phone surveillance was questioned, when the only success was in tracing of a wire transfer of \$8500.⁴⁹

⁴⁷ EUROPOL (2020, Dec.01) Transnational Access to electronic Evidence for Criminal Cases: Trends and Latest Developments within the EU and Beyond, Press Release accessed from <https://www.europol.europa.eu/newsroom/news/transnational-access-to-electronic-evidence-for-criminal-cases-trends-and-latest-developments-within-eu-and-beyond>

⁴⁸ Department of Justice, U.S. Attorney's Office Southern District of California, FBI's Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown (June 8, 2021) <https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive>

⁴⁹ The Washington Post, Is this \$8500 wire transfer really the NSAs best case for tracking American Phone Records, <https://www.washingtonpost.com/news/worldviews/wp/2013/08/09/is-this-8500-wire-transfer-really-the-nsas-best-case-for-tracking-americans-phone-records/>

⁵⁰ Mitchell, B. (2017, October). Going Dark: Impact To Intelligence And Law Enforcement And Threat Mitigation. Retrieved from https://www.dni.gov/files/PE/Documents/10---2017-AEP_Going-Dark.pdf See also US District Court. (2015, September). WhatsApp Pen Order Kansas. Retrieved from <https://www.documentcloud.org/documents/3335507-WhatsApp-Pen-Trap-Order.html>

4.4 What meta data analysis can reveal

One option that is available for Intelligence agencies and LEAs, when confronted with E2EE is using meta data analysis and other data procured from commercial entities that they may offer to the government for monetary considerations.⁵⁰ The value of meta data derived intelligence is however poorly understood, and hence there is always more demand from LEA for full access.

While the textbook definition of meta data is data about data, in practice meta data is activity records. For instance, when two people call each other, the conversation generates meta data as shown below:

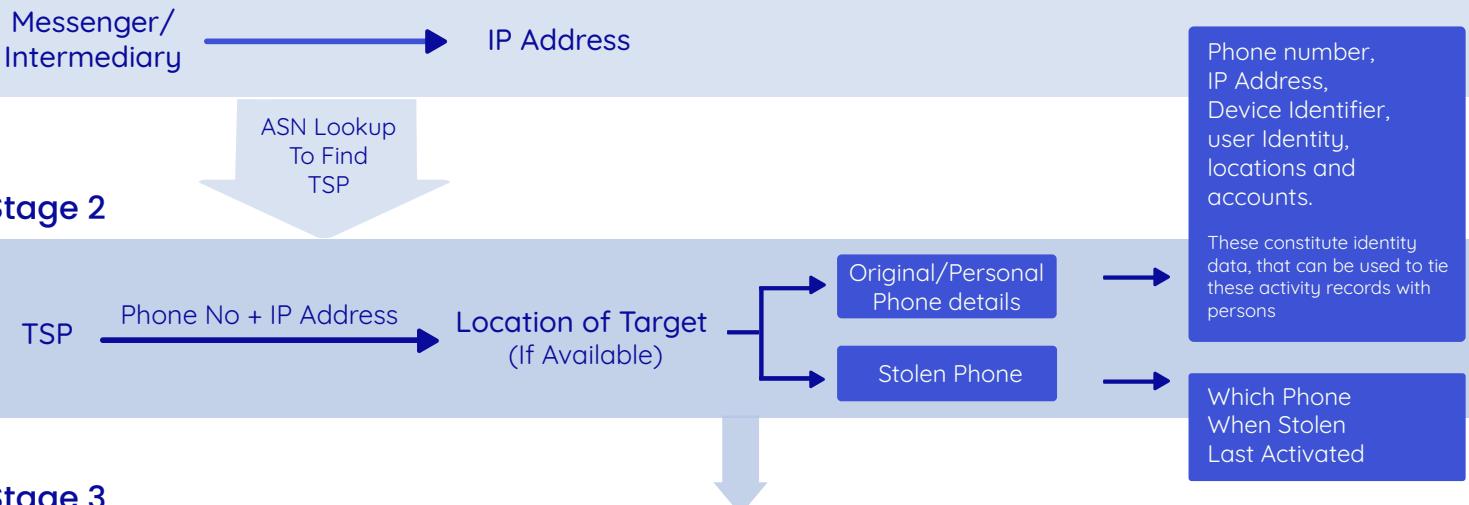
Session ID	Start Time	Duration
S1	10/02/2019, 00:30:40	150 seconds
S1	15/02/2019, 15:20:20	120 seconds
S2	19/03/2019, 16:40:00	190 seconds

Table No. 2

Further, service providers also collect other related data such as Phone number, IP Address, Device Identifier, and these constitute identity data, that can be used to tie these activity records with persons. For instance, consider consumer grade spying apps that attempt to gauge if two people are talking to each other via WhatsApp

Meta Data Analysis Based Surveillance Model

Stage 1



Stage 3



Activation date;
Device Serial number;
Device Type and feature list;
Care plan status and Warranty status;
If device is loaner, replacement or
refurbished;
Warranty expiry date; &
Sold by (works for common device
manufacturers).

Stage 4.1

Based on
Target Profile
purchase
details

NATGRID

Activation date;
Device Serial number;
Device Type and feature list;
Care plan status and Warranty status;
If device is loaner, replacement or
refurbished;
Warranty expiry date; &
Sold by (works for common device
manufacturers).

Stage 4.2

Disclosure
of Call data
records from
TSP

CDR Disclosed

Call Chain
Analysis

Call Chain Analysis (A talked to B, and
then B talked to C, thus establishing A,
B, C all belong to the same chain of
command).

Stage 4.3

Social
Media
Tracking

By mapping the IP Addresses with
well-known applications (Twitter,
Facebook, WhatsApp etc.), it is possible
to outline the online activity profile of
a user.

Stage 5

Location information about given number(s) can be enhanced further, particularly when the number is an Indian number. For Indian numbers, T/ ISPs can be contacted to give other metadata information such as

- DNS Queries made.
- IP Addresses contacted by target's device.

Stage 6

- The target's movements can be obtained from telecom providers within a 50-meter range and existing location databases available for sale from service providers can be used to reconstruct the Wi-Fi networks that the target possibly connects to and the ISP that serves the broadband connection.
- Requests can then be made to the ISP to provide activity records of the target based on the IP Address records obtained from messaging providers.

Stage 7

- List of applications that the target uses often; and
- Combined with activity records from CMS and the messaging provider, LEAs can make a reasonably accurate picture that can be later developed into a detailed profile of the target.

Figure No. 3

status. It involves the following steps:

1. Obtain the phone numbers of the two people, whom you need to surveil.
2. Add them to your contact list.
3. Monitor their “Online” status using the known public Application Programming Interface (hereinafter ‘API’).⁵¹
4. And then estimate probability that they talked to each other, when both are seen online at the same time, since talking requires both coming online together at the same time.

The consumer grade apps estimate probability if the two targets talked to each other by generating activity records as shown below:

Target	Online when	Duration
T1	00:30:40	50 seconds
T2	00:30:42	45 seconds
T1	15:00:23	180 seconds
T2	15:00:28	120 seconds

Table No. 3

This is then matched to generate intersection records as shown below:

Intersection Point	From	To
I1	00:30:42	00:31:27
I2	15:00:28	15:02:28

Table No. 4

To estimate the probability that these intersection records indicate either genuine conversation or simply a random match (since it is possible that these two targets may be talking to others during this time). What then is the probability of two

intersection records being unconnected random events? It is $P(I1) * P(I2)$ which is lesser than $P(I1)$. Applying this logic, the more intersection records 2 targets generate, more likely that they are indeed talking to each other as the probability that it is random becomes quite low.

Unlike consumer grading spying apps which must estimate probability, intelligence agencies however can demand access of meta data from service providers, thus allowing them to bypass the activity creation record phase and directly go to the analysis phase. There had been a lot of existing precedence that service providers do share meta data with law enforcement agencies.⁵² Further in an investigation into ISIS in 2014, Federal Bureau of Investigation (hereinafter ‘FBI’) Agents sought identities, locations and telephone numbers or accounts, and these were executed as well.

As the court records indicate⁵³ sharing of meta data is sufficient to identify the parties in a conversation without revealing the message content.

“Cellular phones can connect to the Internet via the cellular network. When connecting through the cellular network, Internet communications sent and received by the cellular phone each contain the same unique identifier that identifies cellular voice communications, such as an Equipment Serial Number (hereinafter ‘ESN’), Mobile Equipment Identifier (hereinafter ‘MEID’), Mobile Identification Number (hereinafter ‘MIN’), Subscriber Identity Module (hereinafter ‘SIM’), International Mobile Subscriber Identity (hereinafter ‘IMSI’), Mobile Station Integrated Services Digital Network (hereinafter ‘MSISDN’),

⁵¹ See <https://wacheck.online/>

⁵² US District Court. (2016, May). Pen Register Device. Retrieved from <https://www.documentcloud.org/documents/3391606-WhatsApp-Pen-Trap-Order-May-2016.html>, see also: US District Court. (2014, June). Trap and Trace Installation. Retrieved from <https://www.documentcloud.org/documents/3335223-Fox-Brewster-Usa-Whatsapp-Order-for-Trape-and.html>, See also US District Court. (2014, August). WhatsApp meta data Request. Retrieved from <https://www.documentcloud.org/documents/3335504-WhatsApp-Metadata-Request-2014.html>

⁵³ Ibid.

or International Mobile Equipment Identity (hereinafter ‘IMEI’). Internet communications from a cellular phone also contain the IP address associated with that cellular phone at the time of the communication. Each of these unique identifiers can be used to identify parties to a communication without revealing the communication’s contents.” (*sic*)

Further the Pen-trap orders also ask for the following information:

- IP addresses associated with the cell phone device or devices used to send or receive electronic communications.
- Any unique identifiers associated with the cell phone device or devices used to make and receive communications with cell phone number 52 33 3724 5939, or to send or receive other electronic communications, including the ESN, MEIN, IMSI, IMEI, SIM, MSISDN, or MIN
- IP addresses of any websites or other servers to which the cell phone device or devices connected
- Source and destination telephone numbers and email addresses

The IMEI database⁵⁴ can be queried for more information on

1. Activation date.
2. Device Serial number.
3. Device Type and feature list.
4. Care plan status and Warranty status (for most of the common device manufacturers)
5. If device is loaner, replacement or refurbished.
6. Warranty expiry date.
7. Sold by (works for common device manufacturers).

Message contact information allows agencies to create intersection records easily as shown below:

Contact number	From	To
+91 45678 12121	00:30:42, 5 th April 2020	00:31:27, 5 th April 2020
+41 3245 555 444	15:00:28, 20 th June 2020	15:02:28, 20 th June 2020

Table No. 5

Further, meta data requests would also allow them to create a list of other numbers the target regularly interacts with, thus allowing them to perform call chain analysis (A talked to B, and then B talked to C, thus establishing A, B, C all belong to the same chain of command). When combined the data from CMS (Central Monitoring system), location information about given number(s) can be enhanced further, particularly when the number is an Indian number.

For Indian numbers, telecom providers and ISPs can be contacted to give other meta data information such as

- DNS Queries made.
- IP Addresses contacted by target’s device.

By mapping the IP Addresses with well-known applications (Twitter, Facebook, WhatsApp etc.), it is possible to outline the online profile of the target as shown below:

⁵⁴ Run windows on Mac, IMEI.info, <https://www.imei.info>

Application	From	To	IP Addresses
Twitter	00:30:42, 5 th April 2020	00:31:27, 5 th April 2020	X.Y.Z.W, Y.Z.W.P
Face-book	15:00:28, 20 th June 2020	15:02:28, 20 th June 2020	A.B.C.D A1.B1. C1.D1
Google Hangout	12:43:21, 19 th July 2020	12:49:21, 19 th July 2020	B.A.C.D
Chat forum visited by Drug dealers	12:59:21, 19 th July 2020	13:59:21, 19 th July 2020	Y.A.B.D

Table No. 6

While obtaining such information from the telco that serves the phone numbers is usually trivial, obtaining the ISP, if Wi-Fi is used, it is somewhat more involved, as it involves figuring out which Wi-Fi networks are near to the target and mapping them to a particular broadband connection.

The target's movements can be obtained from telecom providers within a 50-meter range and existing location databases available for sale from service providers can be used to reconstruct the Wi-Fi networks that the target possibly connects to and the ISP that serves the broadband connection, and requests can then be made to the ISP to provide activity records of the target based on the IP Address records obtained from messaging providers.

Further, ISPs can also be requested to enable Deep Packet Inspection (hereinafter 'DPI') that can identify the list of applications that the target uses often and when combined with activity records from CMS and the messaging provider, can provide a reasonably accurate picture that can be allowed to build a detailed profile of the target. This could be then used as an input for requesting device seizure via a judicial warrant.

None of this requires putting back-doors in messaging applications or in other service provider networks but can simply done by exercising powers that the agencies already have.

4.5 Insights from Law Enforcement Interviews

To understand why even after having access to data from a variety of sources, LEAs and intelligence agencies have reservations with E2EE, qualitative interviews were conducted with current and former officials at the central and state level including those from Indian Foreign Services, Indian Police Services and Indian Armed Forces. The key points discussed are summarized below:

1. Storage of data outside India is a major challenge for access given the tedious Mutual Legal Assistance Treaty (hereinafter 'MLAT') process. Police officers often approach the official at the Indian office of the technology company. Officers are not sure whom to approach and the India head of the companies shift compliance burden on the foreign office where they are headquartered.
2. Access to information is sought majorly in two broad scenarios. First, when a crime is suspected to be perpetrated. Second, when the crime is suspected to take place. The process for accessing crucial information via the MLAT process is so time-consuming that:
 - i. In the first scenario, information is often shared long after the perpetration of the crime;
 - ii. In the second scenario, information is shared so late that if the police request it (and all such requests have to be disclosed during trial) then the accused endeavours

to use the non-availability of the report as a mitigating circumstance (and at times to cast reasonable doubt) which delays the trial.

3. It is only in a handful of cases where cybersecurity or technology experts are part of the investigation team from the beginning. Most police officers have to solve cybercrimes without the assistance of experts. Even if the police officer makes effort to educate oneself, then a savvy criminal who is an expert in this domain can find a way to outsmart the police. Access to technical experts as part of the investigation team is a major challenge.
4. It has been noticed that even when the LEAs know where to look, judges refrain from giving favourable orders owing to their inability to appreciate technology.
5. LEAs ask for broad data sets from companies because most of the times LEAs do not have access to experts to guide them on what exactly to ask for. Thus they ask for everything, this is more concerning because of their inability to draw patterns from meta data because of lack of access to technical experts. (*sic*)
6. Unlike countries like the US, Indian LEAs are not able to unleash the potential of surveillance via meta data. There is an need to build capacity on this front, currently only specialised agencies of certain members with such expertise while we need one in every police station. (*sic*)
7. The Navy runs sensitization programs regularly with fishing communities across all the States in the western theatre. This approach allows them to cover

entire communities in a span of a year repeatedly, as river inlets and estuaries can also be used to launch attacks. In this context, it is critical to appreciate that the ambit of surveillance operations is so vast that widespread use of military-grade E2EE, which is nearly unbreakable, represents a significant worry for intelligence planners. Its use creates a problem for counterintelligence and surveillance operations.

8. India is far different from the Chinese surveillance regime. Given the wide canvass, mass surveillance in India is almost impossible, as it does not have the wherewithal for the same. To prevent attacks, LEAs have to act on inconclusive proofs, which at times leads to abrasive surveillance. Better technical support for intercepting and analysing digital communications will be immensely useful here. This said, there is a need for institutionalized checks and balances via appropriate surveillance reforms. (*sic*)
9. Despite efforts from the International Telecommunications Union to address the global encryption debate, no solution has been arrived at. With the presence of autocratic States like China and Russia any global cooperation is difficult to achieve. Moreover India has banned Chinese Telecom hardware owing to suspected back-doors raising concerns of espionage.
10. While savvy criminals might shift to different encrypted platforms if they get to know that the platform has been compromised. But access to E2EE is not the sole factor, reach and user-friendliness is also an important consideration. Many rely on code language even on encrypted platforms as an additional layer of security.

11. While consultation with foreign experts maybe helpful, given the sensitivities involved, India needs to build its own surveillance and cybersecurity architecture. Afterall friendly nations also spy on each other in the age where information is power.

5 Encryption Regulation

5.1 Technical measures and Categorization

Encryption regulations typically stand on a two-legged stool – Mandating or utilizing existing capabilities (technical measures) and a policy framework that outlines how these capabilities will be used.

Broadly technical measures to regulate encryption fall within these categories:

- a. **Algorithm Selection** – Encryption algorithms are bucketed into either a black list or a whitelist or both. The list of algorithms could span across all of Hashing, Message Authentication, Asymmetric Key signature and Symmetric Key encryption and be applicable for certain sectors and use cases (Data at rest, Data at motion etc.). Algorithms prescribed by regulators are typically expected not to contain backdoors, but the Dual EC PRNG⁵⁵ incident shows, there are known exceptions.
- b. **Key Escrow** - In the Key escrow approach, a decryption key to a user or for a device is held in an escrow account by a third party which could either be a government or private entity, and access is given to this escrow key, based on a well-defined process, which may involve the judiciary. While it is easier to build, the problem of how to restrict access to the decryption key to only the right set of parties is considered a hard

problem and not possible to solve.⁵⁶

- c. **Client-Side Scanning** – When content is encrypted at the edges, and centralized scanning is hence not possible, one approach is to mandate edge scanning or client scanning of content. In this model, a set of hashes are either sent to the edge devices or is stored in a central repository and when any content is sent out, it is searched against these hashes and flagged if it exceeds a certain threshold. As the natural experiment of Apple's implementation of CSAM indicates, it was easy to reverse engineer and break it on edge devices to by-pass this process.⁵⁷
- d. **Ghost Users** – In this approach, a third party is silently added to a conversation between two users without their knowledge,⁵⁸ as these services depend upon an identity provider. As Greene observes, this approach forces a known vulnerability to never be fixed by providers, and becomes “an ossifying influence that holds ancient flaws in place”.
- e. **Watermarks** – Watermarks may be mandated to be added within content to defeat anonymity. The watermarks can be overt (Digital signatures for contracts) or covert (hidden meta data). One known issue when hidden meta data was prescribed to defeat anonymity is that, it assumes that clients will always be legitimate and will not be reverse engineered to create forgeries, an assumption that does not hold on practice.

⁵⁵ Zetter, K. (2013, September 24). How a Crypto 'Back-door' Pitted the Tech World Against the NSA. Retrieved from Wired: <https://www.wired.com/2013/09/nsa-back-door/>

⁵⁶ Greene, M. (2021, August 01). Thinking about “traceability”. Retrieved from <https://blog.cryptographyengineering.com/2021/08/01/thinking-about-traceability/>

⁵⁷ Ygvar, A. (2021, August). Neural Hash. Retrieved from Git Hub: <https://github.com/AsuharietYgvar/Apple-NeuralHash2ONNX>

⁵⁸ Greene, M. (2018, December 17). On Ghost Users and Messaging Back-doors. Retrieved from Cryptography Engineering: <https://blog.cryptographyengineering.com/2018/12/17/on-ghost-users-and-messaging-back-doors/>

5.2 Around the World

State policy on encryption in various jurisdictions covers the entire spectrum from banning encryption or mandating severe restrictions upon the public access to strong encryption tools (e.g. China, Turkey) to legal protection for public access to encryption (e.g. Netherlands) and interim measures such as diluting public access to encryption. This is achieved through a range of restrictions including - regulations on key length, local storage of data and meta data storage and export control.

5.2.1 China

China's state policy on encryption is one of stubborn isolationism, focused on building domestic capacity and finally establishing a splinternet triggered by events in the last decade. Following the disclosures by Edward Snowden in 2013, Chinese policy on encryption targeted self-sufficiency as infrastructure built on products and services supplied by US companies was seen as a national security risk.

The culmination of the rejig of policy focus was with the coming into force of the Encryption Law in January 2020. Beijing's encryption policy is driven by the intertwined interests of political control and commercial development.⁵⁹

With an intention to redress user concerns of vulnerability of their personal data on digital platforms and in a bid to nurture the Chinese digital economy, with a focus on encryption dependent blockchain technology, the Chinese officials have liberalised the commercial encryption

regime.

The encryption law⁶⁰ envisages a 3-tiered structure – Core, Common and Commercial. While core and common tiers are controlled and used to protect state secrets, the law allows more freedom and openness for commercial cryptography. The law however is silent about key management and by specifying inspection and control structure by the State Cryptography Administration (hereinafter 'SCA') eventually ensures that cryptographic keys will be made available to the state agencies,⁶¹ thus ensuring that E2EE would be effectively outlawed.

The access to encryption keys by state agencies was further illustrated in the case of Apple. They moved all their iCloud keys to China where it is managed by a local company.⁶² This along with state mandated use of a different device which stores these keys (Hardware Security Modules are special devices that store cryptographic keys). This device is unlike those made by Thales Corporation which Apple uses elsewhere.

5.2.2 Australia

The Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, (hereinafter 'TOLA Act') provides wide surveillance powers to access encrypted communication to Australian LEAs and intelligence agencies without any judicial or legislative oversight. To ensure that the notices under the TOLA Act are targeted, the law prohibits the creation of 'systemic weakness' or 'systemic vulnerability', as a safeguard, without understanding that it is impossible to do

⁵⁹ Laskai, L., & Segal, A. (2021, March). The Encryption Debate in China: 2021 Update. Retrieved from Carnegie Endowment for International Peace: https://carnegieendowment.org/files/202104-China_Country_Brief.pdf

⁶⁰ Huaxia. (2019, October 26). China Focus: China adopts law on cryptography. Retrieved from Xinhua: http://www.xinhuanet.com/english/2019-10/26/c_138505655.htm

⁶¹ Dickenson, S. (2019, November 7). China's New Cryptography Law: Still No Place to Hide . Retrieved from Harris Bricken: <https://harrisbricken.com/chinalawblog/chinas-new-cryptography-law-still-no-place-to-hide/>

⁶² Nellis, S., & Cadell, C. (2018, February 24). Apple moves to store iCloud keys in China, raising human rights fears. Retrieved from Reuters: <https://www.reuters.com/article/us-china-apple-icloud-insight/apple-moves-to-store-icloud-keys-in-china-raising-human-rights-fears-idUSKCN1G8060>

so.⁶³

The legislation, without specifically outlawing encryption, provides a framework of three notices to ensure that whenever there is a need for legal assistance to decrypt a communication, the technology companies comply viz:

- **Technical Assistance Requests (hereinafter ‘TARs’):** for the ‘designated communication provider’ to voluntarily provide decrypt or provide access assuming they already have the capability to comply.
- **Technical Assistance Notices (hereinafter ‘TANs’):** envisage a compulsory order to decrypt or provide access assuming they have the capability to comply.
- **Technical Capability Notices (hereinafter ‘TCNs’):** is a compulsory notice to develop capabilities to facilitate TARs and TANs. A TCN would be death knell for E2EE, though per the Parliamentary Joint Committee on Intelligence and Security (hereinafter ‘PJCIS’) no TCNs have been issued⁶⁴ as of August 2020.

The legislation uses a catch-all approach with the definition of ‘designated communication provider’, all of whom are bound to respond to the notices. While the law weakens encryption, and appears targeted, it does not have judicial oversight mechanisms.

Lack of judicial oversight, makes Australia an outlier⁶⁵ amidst the Five Eyes wherein all other members need judicial authorisation for intrusive surveillance.

5.2.3 Belgium

Belgians have long had privacy focussed laws even before the European Union General Data Protection Regulations (hereinafter ‘EU GDPR’) in the form of the Belgian Data Protection Act of 1992⁶⁶ and the Electronic Communications (the Electronic Communications Act) of 2005⁶⁷ backed by Article 22 of the Belgian Constitution⁶⁸. It provides for constitutionally backed individual privacy. Post implementation of the GDPR, the Belgian government had a law namely, the Act of 3 December 2017 on the establishment of the Data Protection Authority⁶⁹ that established the Belgian Data Protection Authority.

⁶³ Stillgherian. (2018, December 11). Australia’s encryption laws will fall foul of differing definitions. Retrieved from ZDNet: <https://www.zdnet.com/article/australias-encryption-laws-will-fall-foul-from-differing-definitions/>

⁶⁴ Official Committee. (2020, August 7). PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY. Retrieved from Commonwealth of Australia: https://parlinfo.aph.gov.au/parlInfo/download/committees/commjnt/30904d8b-7cfb-4ef0-99fb-fba2299b57bf/toc_pdf/Parliamentary%20Joint%20Committee%20on%20Intelligence%20and%20Security_2020_08_07_7954_Official.pdf

⁶⁵ Law Council of Australia. (2020, December 4). Richardson Review: Law Council deeply concerned by recommendation to cut judiciary out of warrant approval. Retrieved from <https://www.lawcouncil.asn.au/media/media-releases/richardson-review-law-council-deeply-concerned-by-recommendation-to-cut-judiciary-out-of-warrant-approval>

⁶⁶ Belgian Data Protection Act of 8th December 1992, accessed from https://www.legislationonline.org/download/id/2638/file/Belgium_Protection_Privacy_Processing_Data_Act_1992upd2008.pdf

⁶⁷ Electronic Communications Act, 13 of 2005, accessed from http://www.ejustice.just.fgov.be/cgi_loi/loi_a1.pl?DETAIL=2005061332/F&caller=list&row_id=1&numero=1&rech=2&cn=2005061332&table_name=LOI&n=m=2005011238&la=F&chercher=t&dt=LOI&language=fr&fr=f&choix1=ET&choix2=ET&fromtab=loi_all&sql=dt+-contains++%27LOI%27+and+dd+=+date%272005-06-13%27and+actif+=+%27Y%27&ddda=2005&tri=d-d+AS+RANK+&trier=promulgation&dddj=13&dddm=06&imgcn.x=46&imgcn.y=8#LNK0001

⁶⁸ Article 22, Belgian Constitution, English Translated version accessed from https://www.dekamer.be/kvvcr/pdf_sections/publications/constitution/GrondwetUK.pdf

⁶⁹ Belgian DPA Act, accessed from http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=n-l&la=N&cn=2018073046&table_name=wet

While Belgium has historically been at the forefront of protecting their citizen's privacy, recent legislations have taken a different path. The Belgian government attempted to pass a Data Retention Act in 2016 which mandated telecom and internet companies retaining large amounts of Data on all users for up to 12 months, in case LEAs need access. The law was struck down firstly by the European Court of Justice (hereinafter 'CJEU')⁷⁰ on grounds that mass storage of personal data, as a general and preventive measure, is not in line with EU law and then by the constitutional court of Belgium itself⁷¹.

The CJEU however allowed such retention insofar that they meet objective criteria that establish a connection between the data retained and the objective pursued.⁷²

Belgian legislators have since drafted a new law⁷³ that allows for encryption to be offered but requires back-doors into encrypted systems if needed by the LEAs. The law has been heavily criticised for having a lack of understanding of how encryption cannot be weakened for law enforcement without jeopardizing the entire

network as well as it being called the "most dangerous law being considered by any European Union Member state" in an open letter signed by 100 organisations calling for a halt on the draft law.⁷⁴

5.2.4 Russia

The Russian Federal Law on Information, Information Technology and Protection of Information⁷⁵ mandates messaging service providers to retain 'content data' for up to six months and provide decryption keys to LEAs on demand if the messages are encrypted. Though E2EE is not outlawed, the Yarovaya Law (a telecom law- known for enhancing surveillance capacity of the government) ensures that the Government has carte blanche power to compel access.⁷⁶

5.2.5 Canada

The Canadian Government has historically taken a pro-encryption position. The commitment towards strong encryption was near-ubiquitous as discerned from the 2017 Statement⁷⁷ of the Minister for Public Safety Ralph Goodale, "In Canada's

⁷⁰ Court of Justice of the European Union, (2020, Oct. 06) Judgments in Case C-623/17, C-511/18, La, C-512/18, and C-520/18, Press Release No. 123/20, accessed from <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123en.pdf>

⁷¹ Belgian Constitutional Court judgement dt. April 22, 2021, accessed from <https://www.const-court.be/public/n/2021/2021-057n.pdf>

⁷² Waem, H. & Fraeyman,G.J. (2021,May. 18) The Belgian Constitutional Court annuls Data Retention Act, DLA Piper, accessed from <https://blogs.dlapiper.com/privacymatters/the-belgian-constitutional-court-annuls-data-retention-act/>

⁷³ Belgian Parliament, The Draft law on the collection and storage of identification, traffic and location data in the electronic communications sector and their access by the authorities' accessed from <https://ibpt.be/index.php/operateurs/publication/annexe-1-dispositif>

⁷⁴ Global Encryption Coalition (2021, Sept. 28) Open Letter: 100 organizations and cybersecurity experts call on the Belgian Government to halt legislation to undermine end-to-end encryption, GEC, accessed from <https://www.globalencryption.org/2021/09/open-letter-48-organizations-and-cybersecurity-experts-call-on-the-belgian-government-to-halt-legislation-to-undermine-end-to-end-encryption/>

⁷⁵ Khayryuzov, V. (2020, October 21). The Privacy, Data Protection and Cybersecurity Law Review: Russia. Retrieved from The Law Reviews: <https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/russia>

⁷⁶ World Intermediary Liability Map . (2016, July 7). Yarovaya Law. Retrieved from World Intermediary Liability Map : <https://wilmap.stanford.edu/entries/federal-law-374-fz-amending-federal-law-combating-terrorism-and-certain-legislative-acts>

⁷⁷ Parsons, C. (2019, August 21). Canada's New and Irresponsible Encryption Policy. Retrieved from Citizen Labs: <https://citizenlab.ca/2019/08/canadas-new-and-irresponsible-encryption-policy-how-the-government-of-canadas-new-policy-threatens-charter-rights-cybersecurity-economic-growth-and-foreign-policy/>

view, while encryption poses challenges for Canadian law enforcement investigators, it also safeguards our cybersecurity and our fundamental rights and freedoms. Canada has no intention of undermining the security of the internet by impeding the use of encryption.”

This position has however shifted recently in light of the Communique released by Five Eyes to provide exceptional access. While Canada does not have any law in place to weaken encryption this policy shift has however raised serious concerns.⁷⁸

5.2.6 Netherlands

The Netherlands legislated a national data protection law implementing the ideals of the GDPR. Their commitment towards strong encryption was reiterated in the 2016 statement which opposed interference with encryption methods which

noted,⁷⁹ “Encryption supports respect for privacy and the secret communication of citizens by providing them a means to communicate protected data confidentially and with integrity. This is also important for the exercise of the freedom of expression. For example, it enables citizens, but also empowers important democratic functions like journalism by allowing confidential communication.”

The Criminal Procedure Code of Netherlands, under Article 126 allows an investigating judge to order someone (although not a suspect) to decrypt any encrypted data, or to provide information on how to do so. This provision is not enforceable against a suspect who enjoys protection against self-incrimination.

⁷⁸ Ibid.

⁷⁹ Brook, C. (2016, January 5). Dutch Government Embraces Encryption, Denounces Back-doors. Retrieved from Threat Post: <https://threatpost.com/dutch-government-embraces-encryption-denounces-back-doors/115778/>

5.3 Indian Laws Before IT Rules

1999	<p>Kargil Review Committee Recommended the use of encryption and decryption by intelligence agencies.</p>
2000	<p>Department of Telecommunications Prohibited the use of 40-bit key length without prior authorisation. The ISP's were expected to obtain permission and submit decryption keys to the government.</p>
2001	<p>Information Technology (Certifying Authorities) Rules, 2000 Introduced the use of Public Key Infrastructure (PKI) for encrypting, signing and authenticating transactions in order to increase online security.</p>
2001	<p>SEBI's Report on Internet Trading Recommended that a 64/128-bit encryption standard to secure transactions and online trading must be available for free use.</p>
2008	<p>Reserve Bank of India Internet Banking Guidelines Recommended the use of 128-bit Secure Socket Layer (SSL) encryption as an alternative to PKI for increased browser security.</p>
2008	<p>Information Technology Act Amendment (Section 69) Authorised the Central and State governments to intercept, monitor or decrypt information necessary for the security and/ or sovereignty of the country, for preserving public order or investigating crime.</p>
2009	<p>Information Technology Act Amendment (Section 84A) Provided for the modes and methods for encryption to promote e-governance and e-commerce.</p>
2009	<p>Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (Rule 9) Allowed decryption orders to relate to any information sent to or from "a person or class of persons" or "relate to any subject matter".</p>
2010	<p>SEBI circular on "Securities Trading using Wireless Technology" Provided that the Department of Telecom will govern mandatory use of encryption for internet-based trading.</p>
2011	<p>Information Technology (Intermediary Guidelines) Rules, 2011 Mandated that intermediaries must trace the originator of information on their platform when ordered to do so by an authorised government agency.</p>
2015	<p>Draft National Encryption Policy, 2015 Permitted the use of encryption subject to several obligations imposed on businesses and citizens alike. Ensured LEA's and other authorities had the power to enforce decryption.</p>
2018	<p>Draft Information Technology (Intermediary Guidelines) Rules, 2018 Mandated proactive monitoring of illegal content and ensure traceability of originator of the content.</p>
2019	<p>Personal Data Protection Bill, 2019 (Clause 24) Mandated the use of encryption by every data fiduciary and processor, among other measures, to secure personal data.</p>
2020	<p>Report of the Ad hoc Committee in the Rajya Sabha Recommended breaking end to end encryption to avail safe harbour as a result of the Committee's examination of pornography on social media and its effect on children and society as a whole.</p>
2020	<p>POCSO Rules on Child Safety, 2020 Listed the types of information to be shared by intermediaries with LEA's to check CSAM.</p>
2020	<p>A communique released by Five Eyes along with India and Japan Recommended the Big Tech to ensure traceability in end-to-end encrypted platforms.</p>
2020	<p>TRAI Recommendations on Regulatory Framework for Over-The-Top (OTT) Communication Services Recommended that no regulatory intervention was required in the security architecture of end to end encrypted platforms, as meddling with the same may lead to cyber vulnerabilities.</p>
2021	<p>Janani Krishnamurthy v. Union of India Transferred to the Supreme Court, the case deals with the extent of liability of the Intermediaries to provide information regarding user generated content.</p>
2021	<p>Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 Rule 4(2) mandated Originator Traceability for Significant Social Media Intermediaries.</p>

Figure No. 4

5.3.1 The Law Matrix

India, like most countries, has tried to find a way around encryption by providing exceptional access, i.e. the power to request or demand interception on content that would otherwise stay encrypted on the different platforms. The relevant provisions of the laws include Section 69 of the Information Technology Act, 2000 read with the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 ('Decryption Rules'), Section 91 of the Code of Criminal Procedure, and Rule 4(2) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ('IT Rules, 2021').

All these laws, through a number of approaches, put an obligation on the platforms operating in India to follow decryption of content upon a request made in line with these rules, and levy penalties for failure to comply with the same.

5.3.2 Section 69 and Decryption rules

Section 69 of the IT Act was amended in 2008 to crystallise an obligation of decryption on service providers. As per this provision, government authorities specified in subsection (1) and (3) shall have the power to compel "subscriber or intermediary person in charge of computer resource" to assist in intercepting and decrypting the content on their platforms for the purposes laid down in the subsection (1) of the provision, including cases of a threat to national security, national integrity, public order and decency, or prevention or investigation of crimes.

These conditions for decryption are often considered to be broadly worded with vague terms that increase the chances of

decryption manifold. Accordingly, certain procedural safeguards have also been provided under subsection (2), which provides that the orders may only be passed by the concerned authorities must comply with.

It was in exercise of the power to prescribe such safeguards under Section 69(2) that the Decryption Rules⁸⁰ were put in place. Through these rules the protocol and the parameters of decryption were defined. For instance, Rule 3 deals with the passing of the specific directions for interception or monitoring or decryption of any information, and states that the competent authority can issue an order for the decryption "of any information generated, transmitted, received or stored in any computer resource."

Additionally, Rule 8 places an obligation on the authority directing decryption to ensure that no alternative to collecting the information exists. It is also important to note Rule 13, enforces an obligation for assisting with decryption to the extent possible, thus keeping the service providers open to maintain end-to-end encryption on their platforms.

One of the most controversial of the rules however, is Rule 9 allowing for decryption for specific information exchanged between any "person or class of persons" and related to "any subject matter." This provision broadens the scope of decryption requests and raises the risk of targeting vulnerable groups.

Section 69 and the Decryption Rules are important points of discussion in the encryption debate considering the penalty provisions which provide for fines and imprisonment for up to seven years for instances of non-compliance by any person, including an intermediary.

⁸⁰ MeITY notification, Rules under S.69 IT Act, 27th November, 2009, <https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Procedure%20and%20Safeguards%20for%20Interception%2C%20Monitoring%20and%20Decryption%20of%20Information%29%20Rules%2C%202009.pdf>

5.3.3 Section 91 of the Code of Criminal Procedure

This section contains the most basic provisions for governmental right to summons and producing documents or other things, held physically on technological and internet platforms by private entities. The section states that “whenever any Court or any officer in charge of a police station considers that the production of any document or other thing is necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding under this Code by or before such Court or officer, such Court may issue a summons, or such officer a written order, to the person in whose possession or power such document or thing is believed to be, requiring him to attend and produce it, or to produce it, at the time and place stated in the summons or order.”

It should be noted that this section authorises not just the courts, but also executive bodies to approach private-sector organizations for gaining access to communication information. This section can therefore be used by governmental bodies to access basic subscriber information and other meta data, especially from telecom and internet companies, without much judicial oversight.

However, the jurisprudence on this section has evolved overtime to develop certain safeguards on the use of this section such as the judgement in **State of Orissa v. Debendra Nath Padhi**,⁸¹ which restricted the use of this Section ‘roving and fishing’ enquiries, and the one in **Suresh Kumar v. C Sandhumani**,⁸² which places an obligation on the police authorities to show that the

person against whom such summons are issued hold records that are important for the case at hand.

5.4 IT Rules 2021

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (hereinafter ‘IT Rules 2021’) were introduced to tackle the emerging challenges in the digital space. This section seeks to discuss its cybersecurity implications and interaction with the Puttaswamy judgement.

5.4.1 Traceability and the Puttaswamy Test

The growing challenge of fake news and CSAM on messaging platforms has been a concern for the State for a while, and the legal solution for this issue is, IT Rules 2021 Rule 4 (2)⁸³ of which mandates enabling originator traceability (the identity of the person who generated a message) on significant social media messaging platforms. While the rules clarify that the provision is supposed to be used only in cases of serious offences, most of the categories of offences mentioned are open ended and can easily be subjected to abuse.

The rule also mentions that in doing so the intermediary shall not be required to disclose the content of the message, however when read alongside the decryption rules, the State authorities have the power to demand not just the content of the message but the details of all the recipients of the said message and not just its originator.⁸⁴

⁸¹ State of Orissa v Debendranath Padhi, 497 of 2001 (Supreme Court Of India November 29, 2004).

⁸² Suresh Kumar v C Sandhumani, Crl. OP No.20741 of 2015 and M.P.No.1 of 2015 (Madras High Court October 18, 2015).

⁸³ Government of India. (2021, February 25). Intermediary Guidelines and Digital Media Ethics Code. Retrieved from The Gazette of India: https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf

⁸⁴ Rodriguez, K. (2021, June 2). Why Indian Courts Should Reject Traceability Obligations. Retrieved from EFF: <https://www.eff.org/deeplinks/2021/06/why-indian-courts-should-reject-traceability-obligations>

These provisions will be the end of E2EE as it is technically impossible to introduce traceability without breaking encryption. Further traceability is an ineffective tool for LEAs given that it can be easily spoofed leading to innocent citizens being falsely incriminated.⁸⁵

The provision also fails to satisfy the Puttaswamy mandate⁸⁶ wherein the Supreme Court proposed a four-fold test to determine the validity of restrictions on privacy, which calls for the existence of a legitimate aim, suitability or rational nexus, necessity, and proportionality.

The aim of preventing threat to national security is too broad and vague given that there does not exist any precise clear definition of national security either under these rules or anywhere else. The solution is not suitable given that cybercriminals can easily shift to unregulated encrypted platforms⁸⁷ which implies that the government will not even get meta data, from platforms that currently provide them.

The argument of necessity also fails to stand due to the existence of less restrictive measures like meta data analysis and development of traditional surveillance technologies. Further, given that undermining E2EE not just makes the platform even more vulnerable to attack by cybercriminals but also to foreign espionage and hence the proposed solution would lead to far greater national security threats, thereby defeating the argument of proportionality as well.

5.4.2 Back-doors and Traceability

Developing capabilities for originator traceability on E2EE platforms is the same as building a back-door. Traceability is simply another way to find who ‘sent’ the message. Rule 4(2) of the new Rules does not merely enforce a policy but mandate development of technical capabilities to enforce a policy. The risks with ‘originator traceability’ remain exactly the same as with ‘back-doors’ viz:

- Can be repurposed and abused;
- Can be accessed illegally;
- Is not fool-proof; and
- Not useful.

Another crucial concern is that Rule 4(2) of the new Rules does not prescribe the technical architecture to enforce traceability. In the absence of any known technology that can ensure traceability without severely weakening privacy, the mandate is impossible to implement to the extent it conflicts with Article 21 of the Constitution.

⁸⁵ The Hindu Business Line. (2021, May 26). WhatsApp drags Govt to court on new message tracing rules . Retrieved from Business Line: <https://www.thehindubusinessline.com/companies/whatsapp-drags-govt-to-court-against-new-it-rule-on-tracing-message-originator/article34646461.ece>

⁸⁶ Grover, G., Rajwade, T., & Katira, D. (2021, July 14). THE MINISTRY AND THE TRACE: SUBVERTING END-TO-END ENCRYPTION. NUJS Law Review. See also Rizvi,K. & Singh,S. (2021, Mar 15) Does The Traceability Requirement Meet The Puttaswamy Test?, Live Law. Retrieved from <https://www.livelaw.in/columns/the-puttaswamy-test-right-to-privacy-article-21-171181>

⁸⁷ Graham, R. (2016). How Terrorists Use Encryption. CTC Sentinel, 9(6), 20-26. Dearden, L. (2015, September 16). British Isis jihadists ‘had phones hacked by GCHQ’ before they were killed by drone strikes. Retrieved from <https://www.independent.co.uk/news/uk/home-news/british-isis-jihadists-had-phones-hacked-gchq-they-were-killed-drone-strikes-10503076.html>

6 Recommendations

6.1 Create an action plan for reducing encryption debt

A net importer of weapons with no indigenous capability to build, maintain and service them, cannot be a credible military power. Correspondingly, a net importer of encryption technologies with no capability to build, break and maintain them, cannot be a credible cyber power. Given that more and more weapon systems and critical infrastructure are getting digitized, a nation-state which has encryption debt (like India) will always be vulnerable.

Similar to how a country in debt, cannot hope to come out of it, by going deeper into debt, encryption debt cannot be reduced by becoming more hostile to encryption, as it erodes whatever cyber capabilities that exist, across the spectrum. Hence an action plan for reducing encryption debt is a must, and developing a E2EE stack, offers a faster way to get there.

6.2 Pause encryption hostile laws

The draft encryption policy of 2015 was withdrawn after wide spread criticism, that it will worsen the existing cyber vulnerabilities, as it would have reduced protection across all sectors, including critical infrastructure.

E2EE messaging tools and applications are now being used by at least 400 million users in India, which is 25% of the population. Hence mandating ‘originator traceability’ which cannot be implemented without breaking E2EE, puts every one of these users at risk. It also further dissuades anyone else in working on furthering the field of encryption within India, thereby disrupting the potential to offer better products and services, and harms national interests, given the well-known encryption debt.

National security simply cannot mean, security and data access for the intelligence agencies and LEAs and vulnerability for everyone else. Hence hostile encryption laws, must be paused and better ways to address the issues needs to be evolved.

6.3 Commit to surveillance reforms

LEAs and intelligence agencies have serious capability issues to monitor domestic threats, who are increasingly relying on digital tools for communications, as interviews indicate. This results in passing of laws that are encryption hostile, which further worsens the encryption debt and increases vulnerabilities of everyone, thus worsening national security issues.

One way to stop this worsening spiral is simultaneous and co-ordinated actions on strengthening oversight mechanisms on data collection and interception tools, techniques and procedures used by LEAs and intelligence agencies, coupled with investment on enhancing data analysis capabilities, from data sources that already exist.

This also implies that all stakeholders in the criminal justice system must be sensitized about the complex dual-use dynamics that form the basis of encryption technologies. Further judicial and other officers having the power to order disclosure of data must be regularly upskilled on technology and cybersecurity issues. Given that many LEA officials face challenges owing to lack of technical expertise by the adjudicating officer having the power to issue legal warrants for disclosure of information, such periodic training is extremely crucial.

6.4 A nationwide study to gauge the requirements of the LEAs & Intelligence Agencies

It is not always a question of access to plaintext but that of access to even basic subscriber information from transnational

companies. There is a need for a study which aims to understand where our LEAs and Intelligence Agencies are facing challenges, more importantly in terms of access. The study should also assess the need of modern technology required by the said institutions. The need for advance technology for lawful hacking and meta data analysis must be assessed and catered to. While acquiring technology or building technical capabilities, one must ensure that the technology itself or its use does not violate the Puttaswamy Test and the Data Minimization requirement envisaged in the Personal Data Protection Bill, 2019. Similar studies to understand the requirements of the LEAs and intelligence agencies in EU have been very useful in having an informed legal and policy debate on the next steps to ensure national security.

Imprint
© 2022 The Dialogue™ and DeepStrat
www.thedialogue.co
www.deepstrat.in

Recommended citation: Yashovardhan Azad et al. (2022, January 12). *Analysing the National Security Implications of weakening encryption*. New Delhi. The Dialogue and DeepStrat.

The Dialogue™ is a public-policy think-tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue™ has been ranked as the world's Top 10 think-tanks to watch out for, by the Think-Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

DeepStrat LLP is a New Delhi-based Think Tank and Strategic Consultancy. It was founded with the vision to combine rich experience in government with the best talent available in the private sector to produce sustainable solutions. At DeepStrat we focus on a broad spectrum of issues – from National Security to Technology, Sustainability, Governance, Capacity Building, Foreign Policy, Defence and Public Policy

