CONCEPTUALISING INTERACTION BETWEEN CRYPTOGRAPHY AND LAW

Pratik Prakash Dixit[*]

The modern form of cryptography has pervaded nearly all levels of everyday technological use. It is used to secure online commercial transactions, ATM transactions, all modern technological devices like mobile phones and laptops, and instant messaging applications like WhatsApp. Though encryption provides a zone of privacy to users, it also presents the challenge of "going dark" before law enforcement agencies. Recently, there has been a growing debate in countries like the United States and India, to regulate the use of encryption so that the law enforcement agencies can have access to the encrypted data. However, the governments have not been able to figure out the modalities to do so. Since encryption is the most potent tool at the disposal of an individual to protect his or her privacy, any government policy which seeks to regulate its use must also take into consideration its potential impact on the privacy of citizens. This paper argues that a greater focus must be laid on adopting stronger encryption standards rather than weakening them. Empirical facts also prove that the binary of 'privacy versus security' is fallacious because the gains accrued from using strong cryptography easily outweigh the losses.

I. INTRODUCTION

Cryptography, derived from the Greek *kryptos* (hidden) and *logos* (word), is the science and art of code-making and code-breaking.[1] Cryptography, in more elaborate and simpler terms, is the art of "creating and using methods of disguising messages, using codes, ciphers, and other methods" so that only the intended persons can receive the information.[2] Cryptography makes sure that secrecy is maintained between the sender and the receiver.[3] The desire to keep

[*] Third year student of National Law School of India University, Bengaluru. I would like to thank Mr. Apar Gupta for his valuable inputs and suggestions. I would also like to thank the editors of the NUJS Law Review for their comments on the draft. All mistakes remain mine.

[1] The Information Technology Rules, 2000, Schedule V. (It defines cryptography as:

"(i) The mathematical science used to secure the confidentiality and authentication of data by replacing it with a transformed version that can be reconverted to reveal the original data only by someone holding the proper cryptographic algorithm and key.

(ii) A discipline that embodies the principles, means, and methods for transforming data in order to hide its information content, prevent its undetected modification, and/or prevent its unauthorised uses.")

[2] A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip and the Constitution*, 143 UNIVERSITY OF PENNSYLVANIA LAW REVIEW, 709, 713 (1995).

[3] *Id.*, 72. (Michael Froomkin vividly describes secrecy as:

> "[a] form of power. The ability to protect a secret, to preserve one's privacy, is a form of power. The ability to penetrate secrets, to learn them, to use them, is also a form of power.

personal information secret has long pervaded human history.[4] Humans have been using codes and ciphers for thousands of years in order to protect trade secret and diplomatic communication.[5] With the advent of new technology and a greater need to protect them, the use of cryptography has increased exponentially and pervaded every part of human existence.

Cryptography, as we know today, developed in the United States in the 1970s with the arrival of computers. Initially, it was mostly viewed as a discipline of interest to military organisations and surveillance agencies.[6] However, the development of computers and growth of the internet in the 1990's paved the way for general use of strong cryptography. With the emergence of electronic communication on personal computer networks, people needed a sure way to communicate and transact freely, securely, and anonymously. On one hand, cryptography allowed users to authenticate documents and transact in a bubble of secrecy;[7] on the other hand, government agencies like the NSA saw the use of encryption for personal and commercial use as a threat to national security.[8] Therefore, cryptography was also called a 'double-edged' sword.[9]

Recently, a committee headed by Retd. Justice B.N. Srikrishna submitted a draft of the Personal Data Protection Bill, 2018, to the government.[10] This law will regulate how the personal information of Indian citizens is used by public and private organizations.[11] In addition to the data protection law, India also urgently needs a comprehensive encryption policy so as to secure the information technology architecture of India's digital economy.[12] We already have the skeletal

Secrecy empowers, secrecy protects, [and] secrecy hurts. The ability to learn a person's secrets without her knowledge- to pierce a person's privacy in secret- is a greater power still.")

[4] James Graham et al., Cyber Security Essentials 6 (2011).

[5] Kaveh Waddell, *The Long and Winding History of Encryption*, The Atlantic, January 13, 2016 available at https://www.theatlantic.com/technology/archive/2016/01/the-long-and-winding-history-of-encryption/423726/ (Last visited on June 6, 2018).

[6] Ivars Peterson, *Encrypting Controversy*, 143 Science News, 394 (1993).

[7] M. Leigh MacDonald, *Internet Regulation: An Inter-American Plan*, 32 The University Of Miami Inter-American Law Review, 83, 95 (2001).

[8] John Deutch, *Terrorism*, The Foreign Policy (Washington), (1997), 108; (The National Security Agency (NSA) is an intelligence agency of the United States established in 1952. The NSA was created with an objective to provide cryptologic support to U.S. military operations during cold war and beyond. *See* National Security Agency), *Mission & Values*, available at https://www.nsa.gov/about/mission-values/ (Last visited on June 21, 2018).

[9] Maura Conway, *Terrorist Use of the Internet and the Challenges of Governing Cyberspace* in Power And Security In The Information Age 95 (Myriam Dun Cavelty, Victor Mauer et al., 2007).

[10] The Hindu, *Protect critical personal data of citizens: draft Bill*, July 27, 2018, available at https://www.thehindu.com/news/national/srikrishna-committee-report-recommends-penalties-for-misuse-of-data/article24532466.ece (Last visited on October 14, 2018).

[11] The Hindu, *Protecting our data*, March 23, 2018, http://www.thehindu.com/opinion/op-ed/protecting-our-data/article23325493.ece (Last visited on June 18, 2018).

[12] Bedavyasa Mohanty, *Encryption Policy 2.0: Securing India's Digital Economy* May 4, 2017, https://www.orfonline.org/research/encryption-policy-2-0-securing-indias-digital-economy/ (Last visited on June 21, 2018).

framework in the form of the Information Technology Act, 2000, and various rules framed thereunder. However, the exponential development in the field of encryption technology has made the provisions therein redundant.

The aim of this paper is to conceptualise the interaction between law and a dichotomous technology like cryptography. The object of this paper is to understand cryptography, its applications, and national security threats and perceptions. Based on this descriptive analysis, the paper critiques the present and proposed laws in India with regards to regulating encryption and accessing encrypted data. Most of the discourse on regulating the use of encryption has been framed in the binary of 'privacy versus security'.[13] This paper argues that this binary is false because decryption of necessary and accessible data can be lawfully achieved to further criminal and national security investigations without debilitating the privacy of citizens. This paper further argues that use of strong encryption must be promoted with an aim to secure the sacrosanct constitutional rights of citizens and remedying the power imbalance between the citizen and the state.

This paper begins with a general overview of cryptography. Part II explains the technical details as to the workings of cryptography and its applications. It also delineates the challenges perceived by law enforcement agencies because of cryptography's profuse use in nearly all kinds of electronic devices. Part III delves into various regulations adopted or proposed in the United States, European Union, and India to access encrypted data. Part IV explains the Indian government's response to the problem of 'going dark'. In this part the Draft National Encryption Policy, 2015, and the regulations that were proposed thereunder are dissected. Part V attempts to rationalize the use of cryptography with the right to privacy. In this part the recent developments in privacy jurisprudence in India, the United States and Canada is discussed in the context of regulating cryptography. Part VI proffers various suggestions that the government could take into consideration while formulating a new encryption policy. The final part concluded that any new encryption policy must be tempered and tailored to reflect the recent developments in legal and constitutional philosophy so as to secure the constitutional rights of citizens.

II. HOW CRYPTOGRAPHY WORKS

Before going into the details of the workings of cryptography, it is necessary to understand certain terms associated with it. A 'plaintext' is the original message. A 'cipher-text' is an encrypted message. 'Encryption' is any procedure to convert plaintext into cipher-text.[14] 'Decryption' is any procedure to

[13] Derek Bambauer, *Privacy versus Security*, 103(3) Journal Of Criminal Law And Criminology 667, 668 (2013).

[14] The Information Technology (Certifying Authorities) Rules, 2000, Schedule V. (It defines encryption as "[t]he process of transforming plaintext data into an unintelligible form (cipher text) such

convert cipher-text into plaintext.[15] An 'algorithm' is a mathematical function used to encrypt and decrypt messages.[16] Modern algorithms use a 'key' to encrypt and decrypt messages.[17] Based on the type of key[18] used, cryptography can be divided into two parts, *viz*. conventional or symmetric cryptography and public-key or asymmetric cryptography.

A. THE WORKINGS OF CRYPTOGRAPHY

1. Conventional or Symmetric Cryptography

In symmetric cryptography,[19] both the sender and the receiver of the information use the same key. The sender uses a key to encrypt the message and the receiver uses the same key to decrypt the message.[20] For this to happen, the sender and the receiver must generate, share, and store the key in advance. However, there are four main difficulties or inadequacies of the symmetric cryptosystems, especially that of key-management:[21] first, since most transactions over the internet occur between parties that do not have an established prior relationship, they cannot share the key in advance; second, exchange of keys will lead to

that the original data either cannot be recovered (one-way encryption) or cannot be recovered without using an inverse decryption process (two-way encryption).")

[15] The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 2(d). (It defines decryption as "[t]he process of conversion of information in non-intelligible form to an intelligible form via a mathematical formula, code, password or algorithm or a combination thereof.")

[16] Dr. Farooq Ahmad, Cyber Law in India 33 (4th ed., 2011). (Modern cryptography is based on the mathematical properties of prime numbers. Prime numbers have only two factors- one and the number itself. However, the third number obtained by multiplying two prime numbers is not a prime number. It has the factors of the two prime numbers, save for itself and one. It is mathematically difficult to obtain the original two prime factors from the product. At present, all cryptosystems rely on the difficulty of reversing encryption computations based around prime number mathematics.)

[17] William A. Hodkowski, *The Future of Internet Security: How New Technologies Will Shape the Internet and Affect the Law*, 13(1) Santa Clara High Technology Law Journal 217, 225 (1997). (All the information like text, pictures, or sounds is converted into binary digits or bits (0 or 1). A 'key' changes all these digits of information into an unintelligible form, *i.e.* encrypts it. A 'key', either similar or different, also has to be used on the receiver's side to change the information back into intelligible form, *i.e.* decrypt it.)

[18] The Information Technology (Certifying Authorities) Rules, 2000, Schedule V. (It defines 'key' as a "sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification).")

[19] The Draft National Encryption Policy, 2015, Annexure. (It defined Symmetric Encryption/ Cryptography as "a method of encryption where the same key is used for both Encryption and Decryption. The key must be kept secret, and is shared by the message sender and recipient.")

[20] Simon A. Price, *Understanding Contemporary Cryptography and Its Wider Impact upon the General Law*, 13 International Review of Law Computers and Technology, 95, 97 (1999).

[21] The Information Technology (Certifying Authorities) Rules, 2000, Schedule V. (It defines Key Management as "[t]he administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy.")

deferments of transactions; third, each person will have to retain a different key for each person he or she wishes to communicate or transact with; and fourth, it will become difficult for the parties to securely exchange the keys.[22] This key management problem was effectively solved by asymmetric or public key cryptography.

2. Asymmetric or Public Key Cryptography

Public key cryptography ('PKC') was developed in 1976 by Whitfield Diffie and Martin Hellman.[23] In PKC, two keys are used, public key and private key.[24] In this form, the recipient's public key, which is made known to the world at large, is used by the sender to encrypt the message, while the private key, known only to the recipient, is used to decrypt the message.[25] PKC serves a dual purpose, *viz*. authentication and encryption. PKC allows the recipient of information to confirm that the information came from a certain sender. Digital signature is the principal way by which identities of parties in electronic transactions are authenticated.[26] Digital signing is usually done through a public key system.[27] The sender encrypts the information with his or her private key, thereby signing the document, and sends the information to the recipient, who decrypts the information with the sender's public key, thereby verifying the authenticity of the sender.[28]

The aforementioned two types of cryptosystems are essentially designed to solve different problems.[29] Symmetric cryptography is best suitable for encrypting data, whereas PKC is best suitable for key management.[30] However, PKC's ability to initiate a secure communication channel between two parties who have never communicated before has made the growth of e-commerce possible on

[22] Price, *supra* note 20, 98.

[23] Shafi Goldwasser & Mihir Bellare, Lecture Notes on Cryptography, 206 (2008).

[24] The Information Technology (Certifying Authorities) Rules, 2000, Schedule V.

[25] The Information Technology (Certifying Authorities) Rules, 2000, Schedule V. (It defines Public Key Cryptography as a:

> "type of cryptography that uses a key pair of mathematically related cryptographic keys. The public key can be made available to anyone who wishes to use it and encrypt information or verify a digital signature; the private key is kept secret by its holder and can decrypt information or generate a digital signature.")

[26] Anjali Singhal, *The Piracy of Privacy? A Fourth Amendment Analysis of Key Escrow Cryptography*, 7 Stanford Law And Policy Review, 189, 191 (1996). (Digital signatures are unique identifier codes that provide a way to mathematically and legally determine an authentic document. Each digital signature is a string of bits attached to an electronic document and created from the documents content and the sender's private key.)

[27] The Information and Technology Act, 2000, §3.

[28] Stewart A. Baker, *Decoding OECD Guidelines for Cryptography Policy*, 31 The International Lawyer, 729, 730 (1997).

[29] Martin Hogg, *Secrecy and Signatures- Turning the Legal Spotlight on Encryption and Electronic Signatures*, Law And Internet, 39 (Lilian Edwards & Charlotte Waelde, 2nd ed., 2000). (Symmetric key cryptography is faster than asymmetric key cryptography because it uses smaller number of bits in the key. However, the speed can be mitigated by using a combination of symmetric and asymmetric encryption. In practice RSA (public key cryptosystem) is combined with DES (symmetric key cryptosystem) for encrypting data.)

[30] *Id*.

the Internet.[31] The increase in the use of cryptography in the 1990s was coincident with the rise of the Internet.[32] Cryptography made it possible for individuals to engage in online banking, e-commerce, and communicate freely and securely via emails, text messages, and voice communications.

B. CRYPTOGRAPHY: APPLICATIONS AND CHALLENGES

The modern form of encryption has pervaded nearly all levels of everyday technological use. In the present day and age, encryption is deployed to secure online commercial transactions, Automated Teller Machines ('ATM'), all modern technological devices like laptops and smartphones, wireless networks, information database[33] and even smart cars.[34] Though the focus of this paper is mainly on the encryption used for securing data in transmission and data stored in devices like a laptop or a smartphone, an encryption policy must take all aspects and applications of cryptography into consideration. A laptop or a smartphone makes use of encryption in multiple ways. This includes the hardware, the firmware that connects the hardware and the operating system, and a large number of softwares that operates on the device.[35]

Encryption is used to protect the data contained in mobile phones and laptops by using a device locking mechanism. Data which is not moving from device to device but is physically stored in a device like a mobile phone or a hard drive is known as 'data at rest'.[36] Whenever a smartphone is locked, the data therein is encrypted which can only be decrypted by the key[37] specified by the user.[38] Encryption is also used to secure data that moves across the internet or within

[31] Nathan Saper, *International Cryptography Regulation and the Global Information Economy*, 11 Northwestern Journal Of Technology And Intellectual Property, 673, 676 (2013)

[32] Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 Columbia Science And Technology Law Review 416, 449 (2012).

[33] The Financial Express, *'Future of Governance': Aadhaar protected by high-tech encryption, authentication, says UIDAI Chairman*, May 24, 2018, available at https://www.financialexpress.com/aadhar-card/future-of-governance-aadhaar-protected-by-high-tech-encryption-authentication-says-uidai-chairman/1180100/ (Last visited on June 22, 2018).

[34] European Union Agency For Network And Information Security, *Cyber Security and Resilience of smart cars*, 8 (2016)

[35] National Academies Of Sciences, Engineering, And Medicine, *Decrypting the Encryption Debate: A Framework for Decision Makers* 20 (February 15, 2018) available at https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2018/feb/cs02152018_Encryption_Debate.pdf (Last visited on June 22, 2018).

[36] *Id.*, 62.

[37] Andy Greenberg, *Don't Rely on an Unlock Pattern to Secure your Android Phone*, Wired, September 22, 2017, available at https://www.wired.com/story/android-unlock-pattern-or-pin/ (Last visited on June 25, 2018). (This 'key' can be in the form of a four or six digits PIN, unlock pattern, biometrics or even faceprint. The user can configure their phone to use any of the aforementioned 'keys' to unlock their device.)

[38] CHI Conference on Human Factors in Computing Systems, May 7-12, 2016, *The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens*, 4806-4817, available at https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/44675.pdf (7th May, 2016).

the confines of private networks such as Local Area Networks (LAN).[39] This has greatly helped in securing online banking transactions, e-commerce, internet browsing, *etc*. which involves transmission of data from one device to another.

Further, encryption has been used profusely in messaging applications like WhatsApp, Signal, Skype, *etc*. These applications use end-to-end encryption protocols to prevent third parties as well as service providers from having access to the plaintext of messages.[40] End-to-end encryption is similar to the public key cryptography. In this method, when the sender sends a message to the recipient, it is encrypted specifically for the receiver using a 'public-key'.[41] Now, the message can only be read by the recipient using his 'private key', which corresponds to the 'public key' with which the message was encrypted. Over the Top ('OTT') service providers like WhatsApp or Signal do not have access to the private keys of either users, and thus cannot decrypt the message. Such strong encryption provides "a zone of privacy" and anonymity to users "to hold opinions and exercise freedom of expression" without any unlawful interference from state as well as non-state actors.[42] Thus, in recent times, encryption has become a potent means towards ensuring civil rights and liberties.[43] However, extensive use of encryption has also resulted in the problem of "going dark".[44] The problem of "going dark" conveys that law enforcement officials are not able to lawfully access communications because they are shrouded under the veil of strong encryption. Consequently, governments all around the world view encryption as creating "safe spaces" for criminals and terrorists to operate. Therefore, many countries have enacted or sought to enact legal solutions through which law enforcement

[39] National Cyber Security Centre, *Cloud Security Principle 1: Data in transit protection*, September 21, 2016, available at https://www.ncsc.gov.uk/guidance/cloud-security-principle-1-data-transit-protection (Last visited on June 23, 2018).

[40] WhatsApp, *End-to-end encryption*, available at https://faq.whatsapp.com/en/android/28030015/ (Last visited on October 15, 2018).

[41] The Guardian, *Australia's plan to force tech giants to give up encrypted messages may not add up*, available at https://www.theguardian.com/technology/2017/jul/14/forcing-facebook-google-to-give-police-access-to-encrypted-messages-doesnt-add-up (Last visited on June 24, 2018).

[42] United Nations Human Rights Council [UNHRC], *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, 7 U.N. D.O.C. A/HRC/17/27 (May 22, 2015).

[43] Freedom House, *Freedom on the Net 2017*, (November 2017), available at https://freedomhouse.org/report/freedom-net/freedom-net-2017 (Last visited on June 24, 2018).

[44] Brookings Institution on Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? James Comey, Director, Federal Bureau of Investigations, (October 16, 2014). (Former Federal Bureau of Investigation ('FBI') Director James Comey succinctly summarised the problem that law enforcement and intelligence agencies all over the world faced because of increasing use of devices using complex encryption technology. As per Comey:

> "law hasn't kept pace with the technology, and this disconnect has created a significant public safety problem. We call it "Going Dark," and what it means is this: Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so.")

agencies can have access to the encrypted data. This will be dealt with in the following chapter.

III. ACCESSING ENCRYPTED DATA

Today, mobile phones and computers have become such an integral part of our lives that we literally live our lives and experience everyday realities through these virtual mediums. These mediums have changed the way we interact with ourselves and the society. Technological innovations have also profoundly changed the modus operandi of crimes. In hindsight, it has been argued that technology has greatly facilitated crimes because of its accessibility and efficiency.[45] Consequently, accessing electronic evidence like data stored on devices like mobiles and laptops and content data like messages shared using internet messaging services like WhatsApp provides crucial evidentiary leads to law enforcement agencies while investigating a crime.[46]

The relevance of electronic evidence in criminal investigations can be inferred from the requests governments across the world make to technology companies like Facebook and Google for access to user data. For example, Facebook received 22,024 data requests from the government of India in the year 2017 alone.[47] According to Facebook, it produced some user data to the government in 53.5 percent of the cases.[48] Similarly, Google received a total of 8,351 user data disclosure requests from the government of India in the year 2017.[49] As per Google it complied with fifty-six percent of the total requests in some form.[50] Google further states that it only produces user data if the government requests are in compliance with the law of the land and Google's policies.[51] This shows that technology companies are willing to co-operate with the government provided the data requested is within their reach and the request is lawful. This chapter will elucidate the legal procedures adopted or proposed in the United States, Europe, and India to access user data from technology companies.

[45] The Reuters, *Technology in now at root of almost all serious crime: Europol*, March 9, 2017, https://www.reuters.com/article/us-crime-europol-idUSKBN16G1XN (Last visited one October 13, 2018).

[46] United States Senate Judiciary Committee, *Written Testimony of New York County District Attorney Cyrus R. Vance, Jr. Before the United Sates Senate Committee on the Judiciary on "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy"*, July 8, 2015, available at https://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Vance%20Testimony.pdf (Last visited on October 14, 2018).

[47] Facebook Transparency Report, *India,* available at https://transparency.facebook.com/government-data-requests/country/IN (Last visited on October 14, 2018).

[48] *Id.*

[49] Google Transparency Report, *India*, available at https://transparencyreport.google.com/user-data/overview?hl=en&user_requests_report_period=series:requests,accounts;authority:IN;time:&lu=legal_process_breakdown&legal_process_breakdown=expanded:5 (Last visited on October 14, 2018).

[50] *Id.*

[51] Google, *User data requests FAQs*, available at https://support.google.com/transparencyreport/answer/7380434 (Last visited on October 14, 2018).

A. THE UNITED STATES

The rapid developments in communication technology in the early 1990s forced the United States Congress to pass the Communications Assistance for Law Enforcement Act ('CALEA').[52] Under the CALEA, a 'telecommunication carrier' is required to develop and deploy intercept solutions in their networks to ensure that the government is able to lawfully intercept the electronic communication.[53] The reach of CALEA extends only to 'telecommunications carriers' and does not include popular internet-based communication services such as internet messaging or e-mail.[54] Therefore, in the absence of any legal framework and obligations, most internet-based communications like WhatsApp are not required by statute to provide lawful interception capabilities to law enforcement agencies. Therefore, when a court orders these companies to monitor or intercept a suspect's communication by a court order or warrant, the companies are unable to do so because they haven't developed and deployed the required interception capabilities.[55]

Alternatively, law enforcement agencies in the United States can also use the Stored Communications Act ('SCA') enacted in 1986 to gain access to stored wire and communications records.[56] Under the SCA the government may lawfully compel disclosure of the substantive contents of stored electronic communication as well as the metadata[57] from third party electronic communication service providers.[58] A valid subpoena or a court order issued under the SCA is required to compel internet messaging services like WhatsApp to disclose basic subscriber records like name, service start date, last seen date, IP address, email

[52] For more discussion on CALEA within the context of encryption, *See* Justin Hurwitz, *Encryption Congress Mod (Apple + CALEA)*, 30(2) Harvard Journal Of Law And Technology 356, 371 (2017); Steven Morrison, *Breaking iPhones Under CALEA And The All Writs Act: Why The Government Was (Mostly) Right*, 38 Cardozo Law Review, 2039, 2058 (2017); Stephanie K. Pell, *You Can't Always Get What You Want: How Will Law Enforcement Get What It Needs In A Post-CALEA*, Cybersecurity-Centric Encryption Era?, 17(4) North Carolina Journal Of Law And Technology 599, 616 (2016); Eric Manpearl, *Preventing "Going Dark": A Sober Analysis And Reasonable Solution To Preserve Security In The Encryption Debate*, 28 University Of Florida Journal Of Law And Public Policy 65, 70 (2017).

[53] Communications Assistance for Law Enforcement Act, 1994, Pub. L. no. 103-414, §107 (codified at 47 U.S.C. §§1001-1010 (2006)).

[54] James Comey, Director, Federal Bureau of Investigation, *Joint Statement with Deputy Attorney General Sally Quillian Yates Before the Senate Judiciary Committee on Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy*, July 8, 2015, available at https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy (Last visited on October 14, 2015).

[55] *Supra* note 44.

[56] David Opderbeck, *Encryption Policy and Law Enforcement in the Cloud*, 49(5) Connecticut Law Review 1657, 1668 (2017).

[57] As per Australian National Data Service, metadata is "information about an object or resource that describes characteristics such as content, quality, format, location and contact information." Metadata is generally data about the data. *See* Australian National Data Service, *Metadata*, available at https://www.ands.org.au/working-with-data/metadata (Last visited on October 15, 2018).

[58] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, §2703 (codified at 18 U.S.C. §§2701-2012 (2006)),

address, profile photos, address book, *etc*., but not the contents of communication.[59] However, law enforcement agencies in the United States feel that metadata alone is not enough to build a concrete case against the criminals or get hold of information threatening national security.[60] Therefore, there has been clamour in recent months to provide law enforcement agencies with "extraordinary access" to encrypted devices.[61]

B. EUROPE

The e-privacy jurisprudence received a major fillip in Europe when the European Parliament enacted the General Data Protection Regulation ('GDPR') in 2018.[62] The GDPR recognises that every natural person has a right to protection of personal data.[63] To further the objectives set out in Article 8 of the European Convention of Human Rights ('ECHR') and the GDPR, the European Parliament approved the E-Privacy Regulations ('EPR').[64] The EPR seeks to prohibit interference with the transmission of personal electronic communication data without the consent of the communicating parties.[65] However, the European Commission also recognises the fact that there cannot be an absolute right to personal data, especially with respect to electronic communication services or social networks, as

[59] WhatsApp, *Information for Law Enforcement Authorities*, available at https://faq.whatsapp.com/en/general/26000050 (Last visited on October 14, 2018).

[60] The Washington Post, *As encryption spreads, U.S. grapples with clash between privacy, security* April 10, 2015, available at https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html?noredirect=on&utm_term=.a6a5eea81d37 (Last visited on October 16, 2018).

[61] The New York Times, *Justice Dept. Revives Push to Mandate a Way to Unlock Phones*, March 24, 2018, available at https://www.nytimes.com/2018/03/24/us/politics/unlock-phones-encryption.html (Last visited on July 6, 2018).

[62] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (Last visited on October 17, 2018).

[63] European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, Art. 8, available at https://www.echr.coe.int/Documents/Convention_ENG.pdf (Last visited on October 16, 2018). (It reads:

1. "Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.")

[64] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0010 (Last visited on October 17, 2018).

[65] *See id*., Art. 6.

it can be used to facilitate crimes.[66] In this regard the European Parliament has proposed rules which will create a new framework for the European Union Member States to access cross-border electronic information and metadata, also known as electronic evidence, in order to investigate and prosecute criminals.[67]

The European Commission proposed the new rules in April, 2018. The proposed rules are in the form of a Directive and a Regulation.[68] The Directive requires the foreign service provider offering services in the European Union to either establish its registered offices in the Union or designate at least one legal representative for the receipt, compliance and enforcement of decisions and orders issued by competent authorities.[69] If the service providers fail to comply with the requests, orders or decisions of the competent authority, they may be subjected to sanctions.[70]

Under the proposed Regulation, a Member State of the Union may order a service provider to produce or preserve electronic evidence regardless of the location of the data.[71] This Regulation can be used by the Member States, subject to certain conditions, to gain access to four types of user data: content data, transactional data, subscriber data and access data.[72] Further, the Member States may also issue preservation orders to service providers to prevent them from removing, deleting or altering data in view of subsequent requests for production of the same.[73] As per the Regulations, the service providers can decline to comply with the production or preservation orders on the grounds that they were not issued by the competent authority or contain manifest errors.[74] The service provider can also refuse to comply with the order if such compliance is not possible because of *de facto* impossibility (in case of end-to-end encryption),[75] or such compliance will be in conflict with the laws of a third country that protects "the fundamental rights

[66] Press Release, EUROPEAN COMMISSION, January 10, 2017, available at http://europa.eu/rapid/press-release_IP-17-16_en.htm (Last visited on October 15, 2018).

[67] Press Release, EUROPEAN COMMISSION, April 17, 2018, available at http://europa.eu/rapid/press-release_MEMO-18-3345_en.htm (Last visited on October 14, 2018).

[68] *Id.*

[69] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL laying down harmonised rules on the appointment of legal representatives for the purposes of gathering evidence in criminal proceedings, COM/2018/226 final-208/0107 (COD), Art. 3, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:226:FIN (Last visited on October 14, 2018).

[70] *See id.*, Art. 5.

[71] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final- 2018/0108 (COD), Art. 5, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN (Last visited on October 14, 2018).

[72] *See id.*, Art. 2.

[73] *See id.*, Art. 6.

[74] *See id.*, Art. 10.

[75] *See id.*, Art. 14(4).

of the individual concerned" or the "fundamental interests of the third country related to national security or defence".[76]

C. INDIA

In India, the Information Technology Act, 2000 ('IT Act') and rules framed thereunder prescribes the procedures and guidelines for the government to request user data from technology companies. The government has formulated the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (the '2009 rules'), under §69 of the IT Act under which the government can request technology companies' assistance in accessing encrypted information.[77] As per Rule 3 of the 2009 rules, the competent authority[78] can issue any decryption direction[79] to the decryption key holder, which may include the consumer as well as the service provider, for decryption "of any information generated, transmitted, received or stored in any computer resource."[80]

Further, Rule 8 states that before issuing the directions under Rule 3, the competent authority should consider all the possibilities of acquiring the necessary information by other means.[81] Rule 13 puts the onus on intermediaries like WhatsApp to provide all the facilities and assistance for interception or decryption of information directed under Rule 3.[82] This Rule further states that any decryption direction issued under Rule 3 to an intermediary is limited to the extent that "the information is encrypted by the intermediary or the intermediary has control over the decryption keys".[83] Interestingly, Rule 14 requires every intermediary[84] to designate one officer to receive requests and another officer to process such requests for decryption of information generated, transmitted, received or

[76] *See id.*, Art. 15.

[77] The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 2(g). (It defines 'decryption assistance' as "any assistance to –
(i) allow access, to the extent possible, to encrypted information; or
(ii) facilitate conversion of encrypted information into an intelligible form;" (emphasis added))

[78] *See id.*, Rule 2(d). (It defines 'competent authority' as "
(i) the Secretary in the Ministry of Home Affairs, in case of the Central Government; or
(ii) the Secretary in charge of the Home Department, in case of a State of Government or Union territory, as the case may be;")

[79] *See id.*, Rule 2(h). (It defines 'decryption direction' as "a direction issued under Rule 3 in which a decryption key holder is directed to –
(i) disclose a decryption key; or
(ii) provide decryption assistance is respect of encrypted information")

[80] *See id.*, Rule 3.

[81] *See id.*, Rule 8.

[82] *See id.*, Rule 13.

[83] *See id.*, Rule 13.

[84] The Information Technology Act, 2000, §2(1)(w). (It defines an 'intermediary' with respect to any particular electronic message as "any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message.")

stored.[85] However, the Rule does not specify any legal consequence for non-compliance with the same. Nevertheless, §69 of the IT Act provides for imprisonment upto seven years for any person, including an intermediary, who fails to comply with the decryption direction.[86] In the following chapter this paper argues that the aforementioned Rules must be amended as they lack constitutional and legal validity.

Further, it must be pointed out that the government in the United States and Europe do not seek to weaken or control the use of encryption by technology companies.[87] They only expect the service providers, device manufacturers and application developers to provide access to "critical investigative tools" like user data.[88] India, on the other hand, proposed a policy which would have forced technology companies to weaken their encryption systems for the government to access the encrypted data.

IV. INDIA'S RESPONSE TO THE CHALLENGE OF 'GOING DARK'

Presently, India does not have any specific legislation or policy regulating the use of cryptography by technology companies. Though, the IT Act deals with certain specificities of cryptography under §69, it is more or less silent as to its use and limitations.[89] However, the Act provides for prescribing the mode for encryption and decryption under §84A[90] and §69[91] respectively. In the absence of

[85] The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 14.

[86] The Information Technology Act, 2000, §69.

[87] Rod Rosenstein, Deputy Attorney General of the United States, Remarks on Encryption at the United States Naval Academy (October 10, 2017) available at https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval (Last visited on October 14, 2018); Press Release, European Commission, October 18, 2017, available at http://europa.eu/rapid/press-release_IP-17-3947_en.htm (Last visited on October 14, 2018).

[88] *Id.*

[89] The Information Technology Act, 2000 was enacted "to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as 'electronic commerce'". Though the Act deals with certain basics of cryptography like digital signatures, it is mostly silent on the level and the type of encryption that an individual or an organisation can employ. *See* The Information Technology Act, 2000, Preamble.

[90] The Information Technology Act, 2000, §84A. (It reads: "The Central Government may, for secure use of the electronic medium and for promotion of e-governance and e-commerce, prescribe the modes or methods for encryption.")

[91] The Information Technology Act, 2000, §69. (It reads:

"(1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is expedient to do so, in the interest of the sovereignty or integrity of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, general guidelines governing the use of encryption technology to secure electronic transactions and communications, various sector specific guidelines have been issued by an array of government bodies.

The Department of Telecom ('DoT') enters into licence agreements with Internet Service Providers ('ISPs'). The terms of this agreement prescribe that the ISPs are permitted to use symmetric key algorithms up to 40 bit key length.[92] Encryption of higher standard can only be employed with prior approval from the DoT. Similarly, the Securities and Exchange Board of India ('SEBI') prescribes that a 64/128 bit encryption standard may be used to secure online trading.[93] The Reserve Bank of India ('RBI') also mandated the use of 128 bit SSL[94] encryption to secure sensitive data like passwords.[95] Further, the Information Technology (Certifying Authorities) Rules, 2000, have prescribed security guidelines for the management and implementation of information technology security of the certifying authorities.[96] Many of the above mentioned encryption mandates are insufficient to protect the sensitive data. Thus, there is a greater need to harmonise the encryption standards across the technological spectrum.

In 2015, a high-level expert committee appointed by the government recommended a National Encryption Policy to regulate the domestic use of

monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

(2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

(3) The subscriber or intermediary or any person in-charge of the computer resource shall called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to-

(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

(b) intercept, monitor, or decrypt the information, as the case may be; or

(c) provide information stored in computer resource

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.").

[92] Ministry of Communications and IT, *Licence Agreement for Provision of Internet Services*, Condition 2.2(vii), (January 2010).

[93] Press Release, Securities And Exchange Board Of India, January 2000, available at https://www.sebi.gov.in/sebi_data/commondocs/99290report_p.pdf (Last visited on June 23, 2018). (This prescription is only advisable and not mandatory. Moreover, this prescription is subject to the policy prescribed by the DoT, which it hasn't till now.)

[94] SSL, which stands for 'Secure Sockets Layer, is a protocol developed for authentication of server and client at the start of the internet session, and encryption/decryption of data exchanged between the two parties during the session. Using an SSL protocol for online communication between a web server and a browser ensures that no third party is able to access the data in transit. *See* Krishna Kant et al., *Architectural Impact of Secure Socket Layer on Internet Servers*, International Conference on Computer Design 2000, 2 available at http://kkant.net/papers/ssl_paper.pdf (Last visited on December 19, 2018).

[95] Reserve Bank Of India, *Report on Internet Banking*, Chapter 6, 50 (June 22, 2001).

[96] The Centre For Internet And Society, *How India Regulates Encryption*, October 30, 2015, https://cis-india.org/internet-governance/blog/how-india-regulates-encryption (Last visited on June 23, 2018).

cryptography.[97] The then Telecom Minister Mr. Ravi Shankar Prasad made it clear that the encryption policy would be applicable only to "those who encrypt", *i.e.* the technology companies.[98] However, its recommendations, which in fact were applicable to both citizens as well as the service providers, would have had ripple effects across different economic sectors in India, particularly the information technology sector.[99] In the following part the draft National Encryption Policy has been critically analysed.

A. DRAFT NATIONAL ENCRYPTION POLICY, 2015

In 2015, the Department of Electronics and Information Technology (DeitY) invited public comments on a draft National Encryption Policy ('NEP') which was to be the basis of Rules framed under §84A of the Information Technology, Act, 2000. The policy was framed keeping in view the "need to protect privacy and increase the security of the Internet."[100] The NEP, which was formulated in response to rapid technological developments in information and communications technology in India and abroad, was laudable in its intent and objectives.[101] However, the draft was fraught with many problems especially that of compliance obligations placed on government institutions, technology companies and users, which eventually led to its withdrawal soon after it was released.[102]

[97] PIB, *Encryption Policy of Government*, September 22, 2015, http://pib.nic.in/newsite/PrintRelease.aspx?relid=127106 (Last visited on December 19, 2018).

[98] The Indian Express, *Criticism forces government to roll back its draft encryption policy*, September 23, 2015, https://indianexpress.com/article/india/india-others/government-withdraws-draft-national-encryption-policy-after-furore/ (Last visited on July 7, 2018).

[99] Ryan Budish, Herbert Burkrt, & Urs Gasser, *Encryption Policy and Its International Impacts: A Framework for Understanding Extraterritorial Ripple Effects*, A Hoover Institution Essay, Aegis Series Paper No. 1804, 11 (2018).

[100] Draft National Encryption Policy, 2015, available at https://netzpolitik.org/wp-upload/draft-Encryption-Policyv1.pdf (Last visited on June 24, 2018). (The Preamble of the draft NEP read:

> "The recognition of the need to protect privacy and increase the security of the internet and associated information systems have resulted in the development of policies that favour the spread of encryption worldwide. The Information Technology Act 2000 provides for prescribing modes or methods for encryption (§84A) and for decryption (§69). Taking into account the need to protect information assets, international trends and concerns of national security, the cryptographic policy for domestic use supports the broad use of cryptography in ways that facilitates individual/business privacy, international economic competitiveness in all sectors including Government.")

[101] *Id.* (The Objectives of the draft NEP were:

"i. To synchronise the emerging global digital economy/network society and use of the Encryption ensuring the security/confidentiality of data and to protect privacy in information and communication infrastructure without unduly affecting public safety and National Security.

ii. To encourage wider usage of Digital Signature by all entities including Government for trusted communication, transaction and authentication.

iii. To encourage the adoption of information security best practices by all entities and Stakeholders in the Government, public & private sector and citizens that are consistent with industry practice.")

[102] The Indian Express, *Draft National Encryption Policy withdrawn: Narendra Modi government's flip flop style*, October 7, 2016, https://indianexpress.com/article/explained/

The NEP stated that the use of encryption technology for communications between business to citizen ('B2C'/'C2B'), citizen to citizen ('C2C'), government to business ('G2B'/'B2G'), and government to citizens ('G2C'/'C2G') shall be based on encryption algorithms and key sizes prescribedby the government through notification from time to time.[103] This, in its essence, amounted to the government forcing businesses and citizens to use only a particular type of encryption system. According to Global Partners Digital, a global think tank aimed at fostering digital democracy, India and Senegal are the only two countries in the world which in some way or the other prescribe maximum standards for encryption products.[104] Further, such type of regulations is not feasible in the present IT landscape because people and businesses will find ingenious ways to subvert them.

Many countries perceivethe use of encryption as an essential means to protect the personal data of citizens. In Finland, the Act on the Protection of Privacy in Electronic Communications, 2004, provides that subscribers and users may "protect their messages and identification data in any way they wish, using any technical means available for the purpose."[105] In Brazil, the Constitution itself declares secrecy of correspondence and online communications as inviolable except for court-ordered interceptions.[106] Similarly, the German Basic Law under Article 10 provides that the privacy of correspondence, mail, and telecommunications is inviolable.[107] The above examples show that many countries have recognised a general right of individuals to use encryption to secure their personal and communicational freedom. Thus, when the NEP restricts the use of encryption, it inevitably chips away at the freedom of Indian citizens to secure their online communications in the mode and manner they wish to deploy.

Further, the draft NEP required all citizens and companies using encryption for communication to store the plaintexts of the encrypted information for ninety days from the date of transaction, and provide verifiable plaintext to law enforcement as required.[108] It also required all vendors of the encryption product to register their products with the government and "submit working copies of the encryption software/hardware to the Government."[109] The government later issued a clarification stating that mass use encryption products and social media applications like WhatsApp, Facebook, Twitter, *etc.* were exempted from the purview of

encryption-draft-withdrawn-modi-governments-flip-flop-style/ (Last visited on June 24, 2018).

[103] Draft National Encryption Policy, 2015.

[104] Global Partners Digital, *World map of encryption laws and policies*, available at https://www.gp-digital.org/world-map-of-encryption/ (Last visited on October 14, 2018).

[105] Act on the Protection of Privacy in Electronic Communications, 516/2004, §6 (Finland).

[106] Constituição Federal [C.F.], 1988 Art. 5(XII).

[107] Grundgesetz Für Die Bundesrepublik Deutschland [Grundgesetz] [GG] [Basic Law], May 23, 1949, Bundesgesetzblatt [BGBl.] [Federal Law Gazette] I at 1.

[108] Bedavyasa Mohanty, '*Going Dark' in India: The legal and security dimensions of encryption,* December 13, 2016, available at https://www.orfonline.org/research/going-dark-in-india-the-legal-and-security-dimensions-of-encryption/ (Last visited on June 23, 2018).

[109] Draft National Encryption Policy, 2015.

the NEP.[110] However, other internet messaging services like Gmail and other applications were not excluded from the NEP. According to cyber security experts, the said requirement would have led to the violation of the fundamental right to privacy, as it would have forced users to monitor their messages.[111]

The NEP also required service providers located within or outside India and using encryption technology for providing any type of service in India, to enter into an agreement with the government. The NEP further stated that the service providers must submit their working copies of the encryption software to the government.[112] Many experts believe that such provisions would have ushered in a licence raj.[113] If these provisions would have taken effect, companies like Apple, Microsoft, Flipkart, Amazon, *etc*., would have had to register with the government as they use encryption technologies at various levels of their operation and services. Further, they would have had to comply with the standards set by the government, as opposed to the globally accepted encryption standards. This would have eroded considerable trust in the Indian cyber security market. Further, it would have provoked these companies to either reconsider their engagements with the Indian market, or to exit it, which could have affected India's projection of herself as a robust global digital economy.

Presently, many countries in the world require providers or users of encryption products or services to be licensed or registered in some manner. In South Africa, the Electronic Communications and Transaction Act, 2002, provides that cryptography providers must register with the Minister of Communications in order to provide cryptography services.[114] Under the Russian Federal Law, provision of information encryption services is subject to licensing.[115] In China, the Commercial Use Password Management Regulations of 1999 states that use and distribution of encryption products produced abroad is prohibited, except when such products are approved by the State Encryption Management Commission. In most cases, it is difficult to force technology companies, who are generally incorporated in the United States, to follow such stringent requirements. In such

[110] The Indian Express, *Encryption Policy: WhatsApp, web services out of draft encryption policy after outcry*, September 22, 2015, available at https://indianexpress.com/article/technology/tech-news-technology/draft-national-encryption-policy-you-might-need-to-store-whatsapp-messages-for-90-days/ (Last visited on June 23, 2018).

[111] Firstpost, *Any Encryption Policy Requires Holistic, Inter-Connected Approach: Cyber Crime Expert*, September 28, 2015, available at https://www.firstpost.com/tech/news-analysis/any-encryption-policy-requires-holistic-inter-connected-approach-cyber-crime-expert-3671939.html (Last visited on October 14, 2018).

[112] Draft National Encryption Policy, 2015.

[113] The Indian Express, *No WhatsApp in national encryption policy draft, but still it is a tough one to digest*, October 7, 2016, available at https://indianexpress.com/article/explained/whatsapp-might-be-out-but-the-encryption-policy-is-still-ambiguous/ (Last visited on October 14, 2018).

[114] Electronic Communication and Transactions Act, 2002, §29.

[115] Federal Law No. 128-FZ on Licensing Specific Types of Activities, Art. 17.

situations, countries like Brazil[116] and China[117] have resorted to blocking and censoring the encryption services.

The NEP also prescribed maximum key sizes up to 256 bits in encrypted products and devices.[118] Academicians, who view this debate from a communitarian perspective, argue that people should not be allowed to use strong encryption as it impossible for the government to carry out searches of criminals threatening the society as a whole.[119] However, this argument overlooks the fact that strong cryptography is a deterrent to cyber-crimes, especially those relating to the hacking of personal data, bank frauds, *etc.*[120] Further, the NEP's proposal of limiting the key size to a maximum of 256 bits was short-sighted, because strong cryptography is required in the future, considering the increase in computational power.[121] The passage of time has made it clear that the draft NEP was only a knee-jerk reaction to the 'going-dark' debate happening worldwide, particularly in the United States. This is also evident from the fact that the Indian government has not come up with any other proposal to synergise encryption and national security since then.[122]

The underlying purpose of the draft NEP was to access encrypted data from both vendors of encrypted products as well as citizens. It was impracticable for the users of encrypted products to store information for more than ninety days, or encryption vendors to agree to the terms and conditions of the government with regards to the use of encryption keys, *etc.*[123] It could be argued that gaging citizens from deleting their personal messages amounts to restraining their freedom to exercise free speech. Another major problem with the draft NEP was that it was not applicable to "sensitive departments/agencies of the government designated for performing sensitive and strategic roles."[124] The NEP should have

[116] Jill Slay, *Why is Brazil trying to block WhatsApp*, The Conversation, May 5, 2016, available at https://theconversation.com/why-is-brazil-trying-to-block-whatsapp-58855 (Last visited on October 14, 2018).

[117] The New York Times, *China Blocks WhatsApp, Broadening Online Censorship*, September 25, 2017, available at https://www.nytimes.com/2017/09/25/business/china-whatsapp-blocked.html (Last visited on October 14, 2018).

[118] Draft National Encryption Policy, 2015.

[119] Amitai Etziono, *End to End Encryption, the Wrong End*, 67 South Carolina Law Review 561, 583 (2018).

[120] F. Lynn McNulty, *Encryption's Importance to Economic and Infrastructure Security*, 9 Duke Journal Of Comparative And International Law 427, 429 (1999).

[121] Factor Daily, *The encryption policy will be back soon, here's what you need to know*, January 2, 2017, available at https://factordaily.com/india-encryption-policy/ (Last visited on June 24, 2018).

[122] NDTV, *Terrorists Take to WhatsApp Calls, Centre Considers Blocking Them*, June 12, 2018, available at https://www.ndtv.com/india-news/as-terrorists-take-to-whatsapp-calls-centre-considers-blocking-them-1865912 (Last visited on June 24, 2018).

[123] Bedavyasa Mohanty, *'Going Dark' in India: The legal and security dimensions of encryption*, December 13, 2016, available at https://www.orfonline.org/research/going-dark-in-india-the-legal-and-security-dimensions-of-encryption/#_ednref13 (Last visited on June 23, 2018).

[124] The Indian Express, *In fact: Needed, clear, robust encryption policy- without a backdoor*, October 1, 2015, available at https://indianexpress.com/article/explained/in-fact-needed-clear-robust-encryption-policy-without-a-backdoor/ (Last visited on June 23, 2015).

focused more on the securing and enhancing the critical government networks rather than excluding them.[125]

B. OVERRIDING THE LAWS OF MATHEMATICS

Recently, the Madras High Court *suo motu* took up a public interest litigation[126] concerning a matter where a boy committed suicide under the influence of an online game.[127] Most of the participants receive a link to participate in this game by way of WhatsApp, which uses end-to-end encryption. Such encryption ensures complete anonymity of users, leaving the law enforcement agencies with little evidence to prosecute crime and prevent terrorism.[128] The High Court expressed a concern that such applications could also pose a threat to the national security, as the source of the messages and the sender of invitation to participate in the online game in the instant case, remains untraceable.[129]

In the instant case, the Madras High Court directed the Central Government "to take appropriate steps … to bring all the "Over The Top" services as well as service providers into a legal framework obliging them to comply with the laws of India and to provide the required information to the law enforcing agencies."[130] The laws of mathematics dictate that the OTT service providers who use end-to-end encryption cannot be legally forced to part with data, as they do not have the same in the first place. However, the government can force the service providers to provide access to the encrypted information in two ways: first, by creating a 'backdoor', *i.e.* mandating the OTT service providers to encrypt the

[125] Rajya Sabha Debates, *Security breaches of UIDAI database*, Session Number 242, March, 10, 2017, *comments by Shri Ravi Shankar Prasad*, available at http://164.100.47.5/official_debate_hindi/Floor/242/F10.03.2017.pdf (Last visited on July 3, 2018). (Different government networks have different encryption standards. For example, government schemes like Aadhaar which records and stores biometric details of over 1 billion Indians on its servers are vulnerable to hacking. To prevent this, identity data stored in the Unique Identification Authority of India's (UIDAI) Central Identities Data Repository (CIDR) is encrypted using 2048 bit encryption and is digitally signed. Further, a resident's Personal Identity Information (PII) is encrypted for both enrolment and authentication transactions using 2048-bit public key.)

[126] Madras High Court v. Union Ministry of Communications, Govt. of India, 2017 SCC OnLine Mad 25298.

[127] The BBC, W*hy is 'Blue Whale' hysteria gripping India?*, September 19, 2017, available at https://www.bbc.com/news/world-asia-india-40960593 (Last visited on June 24, 2018). (Blue Whale is an online game which enjoins its participants to perform certain daring tasks, whose difficulty increases day by day, the ultimate task being death.)

[128] Thomas Fox-Brewster, *Forget About Backdoors, This Is the Data WhatsApp Actually Hands To Cops*, Forbes, January 22, 2017, available at https://www.forbes.com/sites/thomasbrewster/2017/01/22/whatsapp-facebook-backdoor-government-data-request/#34c562671030 (Last visited on June 24, 2018). (While OTT services like WhatsApp do not store messages, either in plaintext or encrypted form on their servers, they store user metadata like mobile numbers, location, IP addresses, device type, mobile network, mobile numbers of contacted people on WhatsApp, data on web pages visited through the app, time of chats and duration of chats.)

[129] *Id.*

[130] Madras High Court v. Union Ministry of Communications, Govt. of India, 2017 SCC OnLine Mad 25298.

message at the point of encryption not only for the recipient's key but also for the service provider's key. This will make sure that it can decrypt the message, as and when the law enforcement agencies ask for it. Second, the OTT service providers can be mandated to copy and store the unencrypted messages before they are sent by the sender.[131] However, such regulations have a deleterious impact on the privacy and businesses of individuals, companies, and even the security of the nation.

Introducing a 'backdoor' is akin to introducing a vulnerability into the security which could be exploited both by the state as well as the non-state actors.[132] In the world of cyberspace, creating a 'backdoor' will empower the government to breach and intercept any data which the government wants.[133] However, once a 'backdoor' is created it leaves the system vulnerable, and can be used by hackers, terrorists, and even hostile governments.[134] Consider the example of the National Security Agency ('NSA'), a national level intelligence agency of the United States. The NSA and its counterparts in the United Kingdom, collaborated with technology companies and internet service providers to insert backdoors into commercial encryption software.[135] However, in 2017 it was reported that the sophisticated tools used by the NSA to defeat encryption fell into the hands of hackers.[136] The hackers used the same tools to attack/hack computer networks in the United States and Europe.[137] These incidents further confirm that the binary of 'privacy versus security' is false, because the former more often than not ensures the latter. This is particularly true in case of India.

[131] The Guardian, *Smartphones, PCs and TVs: the everyday devices targeted by the CIA*, March 7, 2017, available at https://www.theguardian.com/technology/2017/mar/07/cia-targeting-devices-smartphones-pc-tv-wikileaks (Last visited on June 25, 2018). (Recently, it has been revealed that the United States' Central Intelligence Agency (CIA) has the capability to bypass the encryption of OTT service providers like WhatsApp. In here, the CIA does not defeat the encryption but waits till the recipient decrypts the message herself.)

[132] Orin Kerr & Bruce Schneier, *Encryption Workarounds*, 106 The Georgetown Law Journal 989, 1011 (2018).

[133] Thomas Fox-Brewster, *Apple Fights 'Dangerous' FBI Order For Backdoor Into San Bernardino Shooter iPhone,* Forbes, February 17, 2016, available at https://www.forbes.com/sites/thomas-brewster/2016/02/17/tim-cook-takes-on-fbi-over-encryption-bypass/#236d85904bc7 (Last visited on June 25, 2018).

[134] The New York Times, *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, September 5, 2013, available at https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=2 (Last visited on June 25, 2018).

[135] The Guardian, *Revealed: how US and UK spy agencies defeat internet privacy and security*, September 6, 2013, available at https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (Last visited on October 14, 2018).

[136] The New York Times, *Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core*, November 12, 2017, available at https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html (Last visited on October 14, 2018).

[137] The New York Times, *Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool*, May 12, 2017, available at https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html (Last visited on October 14, 2018).

Incidents of Cyber Attacks in India (2013-2016)[138]

Year	**Total number of cyber-security incidents**	**Website hacking incidents**	**Number of government websites hacked**
2013	41319	28481	189
2014	44679	32323	155
2015	49455	27205	164
2016	50362	32224 (approx.)	199

The above figures indicate that sensitive personal and government data is increasingly vulnerable to cyber-attacks from foreign state as well as non-state actors. Taking into consideration the pitiable situation of India's cyber security infrastructure, it is impossible for the government to secure any 'backdoors' which it has access to.[139] Further, the knowledge of such a 'backdoor' could erode the trust between the users and the service provider.[140] The users will eventually shift to service providers which they know will secure their privacy.[141] Thus, any sort of regulation that undermines the security provided by encryption should be eschewed as it is sure to backfire. It must be noted that in the past the Government of India has said that it will not force technology companies to create backdoors, as doing so may jeopardise the privacy of citizens.[142] However, this view may change considering the fact that many countries like Australia[143] and the United Kingdom[144] are getting serious about forcing technology companies to create backdoors.

[138] Rajya Sabha Debates, *Cyber attacks and hackings*, Session Number 234, March 11, 2016, *comments by Shri Ravi Shankar Prasad*, available at http://rsdebate.nic.in/bitstream/123456789/645980/2/PQ_234_20032015_U2613_p211_p212.pdf#search=hack (Last visited on October 15, 2018).

[139] Aman Thakker, *It's Time for India to Update Its Cybersecurity Policy*, The Diplomat, October 10, 2017, available at https://thediplomat.com/2017/10/its-time-for-india-to-update-its-cybersecurity-policy/ (Last visited on June 26, 2018).

[140] Ian Brown, Handbook Of The Economies Of The Internet, 248 (Johannes Bauer & Michael Latzer, 2016).

[141] Jessi Hempel, *Encrypted-Messaging App Telegram Now Has 100 Million Users*, Wired, February 23, 2016, available at https://www.wired.com/2016/02/encrypted-messaging-app-telegram-hits-100-million-people/ (Last visited on June 25, 2018).

[142] Rajya Sabha Debates, *Cyber attacks and hackings*, Session Number 239, May 6, 2016, *comments by Shri Ravi Shankar Prasad*, available at http://rsdebate.nic.in/bitstream/123456789/660255/2/PQ_239_06052016_U1520_p203_p204.pdf#search=encryption (Last visited on October 15, 2018).

[143] ABC News, *New tech surveillance laws more a 'side gate' than 'back door' into Australian phones*, August 14, 2018, available at https://www.abc.net.au/news/2018-08-14/tech-surveillance-laws-less-of-a-back-door-and-more-a-side-gate/10114534 (Last visited on October 15, 2018).

[144] The Hill, *UK minister calls for encryption backdoors after London attack*, March 27, 2017, available at https://thehill.com/policy/cybersecurity/325880-uk-home-minister-calls-for-encryption-backdoors (Last visited on October 15, 2018).

V. RATIONALISING CRYPTOGRAPHY AND PRIVACY

Legal scholars have observed that there is a certain trade-off between the use of bulk surveillance[145] by the government and the privacy of citizens.[146] Though the legality of bulk surveillance hasn't been discussed at length in India, it has been an issue of legal debates in countries like the United States and the United Kingdom.[147] This article does not seek to examine the legality of bulk surveillance, but the means through which the government gets the power to do so, *i.e.* by regulating encryption. Presently, encryption has become the most potent tool at the disposal of an individual to protect his or her private data. Thus, any government policy which seeks to regulate the use of encryption must also take into consideration its potential impact on the privacy of the citizens.

A. REASONABLE EXPECTATION OF PRIVACY

A nine-judge bench of the Supreme Court in *K.S. Puttaswamy* v. *Union of India* ('*Puttaswamy*') unanimously held that the right to privacy "is protected as an intrinsic part of the right to life and personal liberty" under Article 21 of the Constitution.[148] This judgment touched upon various aspects of privacy, the one pertinent to this discussion being "information privacy".[149] For most part of the judgment, the judges discussed privacy in the context of data protection against state and non-state actors.[150] However, in the age of information, it is encryption which ensures informational privacy of an individual. Encryption makes sure that an individual has substantive control over his or her data. It creates a domain of sanctity for an individual to operate freely and securely; a sphere where the individual can be sure that he or she will not pried upon.

[145] Axel Arnbak & Sharon Goldberg, *Loopholes for Circumventing the Constitution: Unrestricted Bulk Surveillance on Americans by Collecting Network Traffic Abroad*, 21 Mich. Telcomm. & Tech, L. Rev. 317, 325 (2015).

[146] Richard Alexander & Roberta Spurgeon, *Privacy, Banking Records and the Supreme Court: A Before and After Look at Miller*, 10 South West University Law Review, 13, 13 (1978).

[147] John Yoo, *The Legality of the National Security Agency's Bulk Data Surveillance Programs*, 37 Harvard Journal Of Law And Public Policy 901-1171 (2014); Laura Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 Harvard Journal Of Law And Public Policy 757-900 (2014).

[148] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, ¶652.

[149] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, ¶584.

[150] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, ¶328. (Chandrachud, J. emphasised upon the need for a law on data protection in following words:

> "Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but also from non-state actors as well. We commend to the Union Government the need to examine and put into place a robust regime for data protection. The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the state.")

Every individual using a certain encryption device has a reasonable expectation of privacy. This reasonable expectation entails that neither the government nor the service provider can access the user's information without his or her express consent. The Supreme Court of the United States in *Katz* v. *United States* ('Katz') introduced the idea of "reasonable expectation of privacy."[151] This view was affirmed by Chandrachud J. in Puttaswamy*,* where he observed that "[t]he sphere of privacy stretches at one end to those intimate matters to which a reasonable expectation of privacy may attach."[152] Further, the right to privacy entails a positive obligation on the part of the state, enjoining it to take all necessary steps to protect the privacy of the citizens.[153] The above discussion gives rise to two preliminary inferences: first, that citizens reasonably expect that the encryption standards they are using on their electronic devices are able to protect their privacy; and second, that the government has to make sure that the encryption policy it adopts will help in protecting the privacy of the individuals. However, the extent to which a person reasonably expects his or her electronic data to remain private is a contentious issue.

Recently, the Supreme Court of Canada ('SCC') in *R.* v. *Marakah* ('Marakah') sought to address the question –do Canadian citizens ever reasonably expect the text messages they send to remain private, even after the messages have been delivered to the receiver?[154] In this case, A, the accused, sent text messages to B, his accomplice, regarding illegal transactions in firearms. While conducting a lawful search of their homes, the police seized the mobile phones of both A and B. On searching the mobile phones, the police found the incriminating text messages and sought to use the same against A. A argued that the incriminating messages from both the devices should not be used as evidence against him as they were obtained in violation §8 of the Canadian Charter of Rights and Freedoms (the 'Charter').[155] Answering the aforementioned question in the affirmative, the SCC held that the search of phones by the police was unreasonable and illegal under §8 of the Charter, asan electronic text message attracts a reasonable expectation of privacy.[156]

[151] Katz v. United States 389 US 347 (1967). (This case pertains to the protection granted by the Fourth Amendment to the United States Constitution against unreasonable searches and seizures. Here, the Court ruled that unreasonable search and seizures, without warrant, is protected by the Fourth Amendment. Harlan, J. in his concurring opinion observed that a conversation is protected from unreasonable search and seizure if it meets a twofold requirement: "first, that a person has exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognise as 'reasonable'".)

[152] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, ¶307.

[153] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, ¶326.

[154] R v. Marakah, [2017] 2 S.C.R. 608.

[155] Charter of Rights and Freedoms, §8, Part 1 of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982. (It states that "[e]veryone has the right to be secure against unreasonable search and seizure.")

[156] R. v. Edwards, [1996] 1 S.C.R. 128. (In this case, the accused was suspected of dealing with drugs and storing the same at his girlfriend's residence. The police constantly kept a watch on the accused and his girlfriend. One time, they arrested the accused for driving despite his license being suspended. While he was kept in custody, the police pursued the investigation into his drug

The SCC delineated the issues with regard to expectation of privacy of the accused vis-à-vis the text messages as follows: first, what was the subject matter of the alleged search?; second, did the claimant have a direct interest in the subject matter?; third, did the claimant have a subjective expectation of privacy in the subject matter?; and fourth, was the claimant's subjective expectation of privacy objectively reasonable?[157] The SCC observed that the subject matter of the search was the electronic conversation between A and B in which the accused, A, had a direct interest as he was the author of and participant in that electronic conversation.[158] The SCC further observed that A had a subjective expectation of privacy as he expected B to keep the contents of the messages private.[159] As regards to the fourth issue, the Court put forth some unique propositions by referring to the following three factors: (i) place where the search occurs; (ii) private nature of subject matter; and (iii) control over the subject matter. I will briefly deal with the first and the third factor, as the same provide a unique perspective to look at privacy in the context of electronic communications. The second issue has not been dealt with here because I believe that the contents of an electronic message are intrinsically private, whether they are personal/biographical or otherwise.[160]

1. The Place of Search

Criminal jurisprudence in India as well as the world over has understood 'place' in the context of territorial privacy interests.[161] The SCC provided a novel interpretation to the idea of 'place'. It observed that though electronic communications do not occupy physical space, they take place through an interconnection of devices through the internet.[162] This interconnection creates a 'digital space' for an individual which is as real as the real world. We, the Court observed, use the 'digital space' to "seclude ourselves and convey our private messages, just as we might use a room in a home or an office to talk behind closed doors."[163] Therefore, the Court implies that when two individuals are communicating electronically, they are occupying a certain portion of the 'digital space' which they

dealings. In such pursuance, they sought cooperation from the accused's girlfriend to search her residence. During search, the police found large quantities of drugs belonging to the accused. The SCC, citing United States v. Gomez, 16 F. 3d 254 (United States Court of Appeals, Eight Circuit), observed that the accused had no expectation of privacy in his girlfriend's residence as (i) the accused was not present at the time of search, (ii) he had no control over the residence as he was "just a visitor", and (iii) he was not the owner of the property.)

[157] *Id.*

[158] R v. Marakah, [2017] 2 S.C.R. 608, ¶21.

[159] *See id.*, ¶23.

[160] *See id.*, ¶32. (McLachlin, C.J. writing for the majority observed that if the unlawful search reveals private information, it attracts reasonable expectation of privacy. He further reasoned that this factor, *i.e.* private nature of information, concerns itself not with the "actual contents of the message the police have seized, but with the potential of a given electronic conversation to reveal personal or biographical information.")

[161] The Code of Criminal Procedure, 1973, §95.

[162] R v. Marakah, [2017] 2 S.C.R. 608.

[163] *See id.*, ¶28.

want to secure from others. These spaces, as per the SCC, can be the place of search.[164]

2. Control Over Messages

The SCC, in *R.* v. *Edwards* ('Edwards'), had considered 'control' as one of the relevant factors in determining whether a subjective expectation of privacy is objectively reasonable.[165] The SCC, in Marakah, built upon this idea in the context of electronic communications. In this case, McLachlin, C.J., writing for the majority, observed that "where 'technological reality' deprives an individual of exclusive control over his or her personal information, he or she may yet reasonably expect that information to remain safe from state scrutiny."[166] The Chief Justice further observed that in case of electronic messages, control may not be exercised over a physical object, but it may be exercised by way of the choice of medium and the designated recipient.[167] This reasoning may be applicable to instant messaging services like WhatsApp where once the user sends the message, it technically goes out of her control. However, she still has control over the message as she is using her agency to choose the medium, WhatsApp in the instant case, and the recipient. The user expects the medium to deliver the message only to the designated recipient and no one else.

Further, Moldaver, J. in his dissenting opinion expressed that reasonable expectation of privacy will also arise where a person exercises 'constructive control' over the subject matter.[168] He further observed as follows:

> "[C]onstructive control may exist by virtue of a claimant's professional or commercial relationship with another person or entity that has direct control over the subject matter in question. … The most obvious examples where this arises included a claimant's relationship with a lawyer, doctor, psychiatrist or another

[164] *See id.*, ¶28.

[165] In R. v. Edwards, [1996] 1 S.C.R. 128, the SCC held that the following factors needs to be considered to determine in totality whether a person had a reasonable expectation of privacy: (i) presence at the time of search; (ii) possession or control of the property or place searched; (iii) ownership of the property or place; (iv) historical use of the item; (v) ability to regulate access; (vi) existence of subjective expectation of privacy; and (vii) the objective reasonableness of the expectation.

[166] R v. Marakah, [2017] 2 S.C.R. 608, ¶41.

[167] *See id.*, ¶44.

[168] *See id.*, ¶136. (Here, Moldaver, J. held that the accused had reasonable expectation of privacy when the electronic message was being transmitted to the accomplice. However, the accused had no reasonable expectation of privacy once the message was delivered to B. In such situation, only B,

> "had exclusive control over the text message conversations on his phone. B was free to disclose them to anyone he wished, at any time and for any purpose. To conclude that M had a reasonable expectation of personal privacy in those conversations on W's phone despite his total lack of control over them severs the interconnected relationship between privacy and control.")

> professional who owes a duty of confidentiality or trust to the claimant."[169]

When a person uses instant messaging services like WhatsApp, she enters into a commercial or fiduciary relationship with the company once she agrees to the terms and conditions of the usage of services. She trusts WhatsApp with her personal messages with a belief that the company will not share the same with any other state or non-state entity. Thus, when the government tries to access her encrypted messages through the company without lawful authorisation, it breaches her reasonable expectation of privacy.

B. THIRD PARTY JURISPRUDENCE

At this juncture, it is pertinent to delve into the jurisprudence developed in the United States and India regarding unlawful searches and seizures. As per the draft NEP, third parties, *i.e.* the service providers, were to be the gateway through which the Indian government was to access user data and information. In *United States* v. *Miller* ('Miller')*,* the Supreme Court of the United States posited the 'third party' doctrine to deal with situations where an individual entrusts his personal data to a third party of his own will.[170] In this case, the Court created an exception to Katz when it held that "a person has no legitimate expectation of privacy in information he voluntary turns over to third parties."[171] Essentially, the 'third-party' doctrine means that if a person voluntarily or knowingly passes on his data to a third party, even if for limited purposes only, the government can obtain such information from the third party without violating the fundamental rights of the citizens.

However, the Supreme Court of India in *District Registrar and Collector* v. *Canara Bank* ('Canara Bank') rejected the 'third-party' doctrine.[172] The Court here held that the right to privacy of an individual extends to his or her information held by a third party.[173] The Court further held that there must

[169] *See id.*, ¶137.

[170] United States v. Miller 425 U.S. 435 (1976).

[171] The ratio of Miller was later reiterated by the Supreme Court of the United States in Smith v. Maryland, 442 U.S. 735 (1979).

[172] District Registrar and Collector v. Canara Bank, (2005) 1 SCC 496. (In this case §73 of the Indian Stamp Act, 1899 as incorporated by Andhra Pradesh, was challenged for being *ultra vires* the Constitution. The impugned provision allowed the Collector, or any person authorised by him to inspect "any registers, books, records, papers, documents or proceedings" which may lead to the discovery of any fraud or dereliction of duty. Ultimately the court held that the impugned provision is *ultra vires* the Constitution as it violates the "right to privacy both of the house and of the person.")

[173] In Miller and Smith*,* the Supreme Court of the United States narrowed down the scope of right to privacy to property rather than to person. In here the Court deviated from its previous decisions in Warden v. Hayden, 387 U.S. 294 (1967), and Roe v. Wade, 410 U.S. 113 (1973) wherein it was held that right to privacy deals with "persons and not places." The Supreme Court of India in Gobind v. State of M.P., (1975) 2 SCC 148, also adopted a similar approach. In here, Matthew, J. observed

be "some probable or reasonable cause or material" for the government to extract such information from the third party.[174] Recently, the Supreme Court of the United States in *Carpenter* v. *United States*[175] ('Carpenter') also held that the 'third-party' doctrine evolved in *Miller* cannot be applied[176] to cellular data because it conveys a "detailed and comprehensive record of the person's movements." The Court also observed that the government must obtain a warrant supported by a "probable cause" before acquiring an individual's records from a third party.[177] The position of law propounded in Canara Bank and Carpenter is similar to the SCC's decision in Marakah.

I accept that the law enforcement agencies need access to encrypted data in order to conduct criminal investigations, as it provides crucial evidentiary links. However, such data must be acquired only after following the due process of law. It is important to point out that the present laws with regard to compelling decryption lack the procedural safeguards espoused in Canara Bank and Carpenter. As discussed in the earlier chapter, the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (the 'Rules') deal with the method and manner in which the government can

that the state must have a "reasonable basis" for intruding the right to privacy of the citizens. In Canara Bank the Court accepted rationale laid down in *Gobind.*

[174] District Registrar and Collector v. Canara Bank, (2005) 1 SCC 496, ¶53. (In here the Court observed:

> "the right to privacy deals with 'persons and not places', and the documents or copies of documents of the customer which are with the Bank, must continue to remain confidential vis-à-vis the person, even if they are no longer at the customer's house and have been voluntarily sent to a Bank. … Once that is so, then unless there is some probable or reasonable cause or reasonable basis or material before the Collector for reaching an opinion that the documents in the possession of the Bank tend, to secure any duty or to prove or to lead to the discovery of any fraud or omission in relation to any duty, the search or taking notes or extract therefore, cannot be valid.").

[175] In Carpenter v. United States, No. 16-402, 585 U.S. _ (2018), the FBI used the cell site location information ('CSLI') of the mobile phone of the suspect to prove that he was at the scene when the crime took place. The defendants argued that the FBI illegally procured the information from the wireless carriers because it constituted a "search" under the Fourth Amendment. The defendants further argued that the suspect had a "reasonable expectation of privacy" when he passed on his personal information to the wireless carriers. The Court agreed with the defendant's arguments. It observed that "the acquisition of [defendant's] CSLI was a search… [and] the Government must generally obtain a warrant supported by probable cause before acquiring such records."

[176] In this case the Court did not explicitly overrule Miller and Smith. It observed that the third-party doctrine was evolved to apply to telephone numbers and bank records which only convey certain specific aspects of personal information of the user. However, recent technological innovations like cell phones convey to the third party "not just dialled digits, but a detailed and comprehensive record of the person's movements." The Supreme Court of the United States adopted a similar view in United States v. Jones, 565 U.S. 400 (2012).

[177] Carpenter v. United States, No. 16-402, 585 U.S. _ (2018). (The Court observed that "when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user. Moreover, the retrospective quality of the data here gives the police access to a category of information otherwise unknowable." If a government gets hold of a person's CSLI, it basically gets access to detailed chronicle about that persons' life. Thus, before compelling a third party to hand over customer data, the Government ought to have obtained a warrant by showing "probable cause".)

force a decryption key holder to disclose a decryption key or "provide decryption assistance in respect of encrypted information."[178] Rule 5 confers upon the competent authority the power to give "any decryption direction to the decryption key holder for decryption of any information involving a computer resource".[179] As per the Rules, the competent authority does not need any "reasonable or probable cause or material" to compel the decryption. Further, the competent authority does not require a judicial warrant[180] before acquiring decrypted information from a decryption key holder.[181] Thus, any new encryption policy must necessarily incorporate the constitutional safeguards endorsed in Canara Bank and Carpenter.

From a careful analysis of above judgments, we can infer that privacy cannot be obtained in the abstract, it has to be achieved using certain concrete means. A house is said to be the castle of every person because the walls create confidence in the minds of the occupant that she can speak or act within the confines of the walls without attracting the prying eyes of others. However, privacy at its abstract best is a state of mind. The walls do not constitute privacy in itself. However, their existence creates an environment where the dweller can enjoy her life the way she wants with a guarantee of security, privacy and comfort. In a very similar way, encryption creates an environment where people can communicate with each other through digital mediums knowing that their conversations are secure. Encryption takes fear out of people's minds when they communicate digitally. It gives ordinary citizens the extraordinary power of secure communication even in the most autocratic countries. Therefore, an encryption policy must aim at securing the sacrosanct constitutional rights of the citizens and remedying the power imbalance between the citizen and the state.

VI. SUGGESTIONS FOR A NEW ENCRYPTION POLICY

In the age of information technology, most of the C2C, B2C, B2G and G2C transactions take place in binary bits. The Indian government must take adequate steps to promote the use of strong cryptography, thereby ensuring national security without endangering public safety and economic interests.[182] Encryption also ensures protection of individual privacy, safeguards human rights, and guarantees freedom of speech and expression. Though the 2015 draft NEP sought to

[178] The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption) Rules, 2009, Rule 2(j).

[179] *See id.*, Rule 5. (It reads: "Issue of decryption direction by competent authority – The competent authority may under Rule 3 give any decryption direction to the decryption key holder for decryption of any information involving a computer resource or part thereof.")

[180] The Code of Criminal Procedure, §93.

[181] The Information Technology Act, 2000, §69(2).

[182] The Washington Post, *Why the fear over ubiquitous data encryption is overblown*, July 28, 2015, https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html?utm_term=.73411faf6acb (Last visited on June 26, 2018).

bridge the gap between national security concerns and the privacy of citizens, in essence it sought to substantially weaken and complicate the prevalent encryption standards. A new encryption policy must focus on two important issues: first, securing India's digital infrastructure; and second, using constitutionally and legally sound ways to access encrypted data.

In order to harmonise the encryption standards, the new encryption policy must make it mandatory for all the C2C, B2G, B2C, G2C, and G2G communications to adopt a minimum encryption standard of at least 128 bits.[183] A greater focus must be to protect G2G information which is vital to the interests and security of the nation. For example, in the Unites States a statutory body called the National Institute of Standards and Technology (NIST) recommends cryptographic standards for government agencies from time to time.[184] These standards are invariably followed by private players in the industry.[185] There is a need to create such a statutory body in India, which will make sure that the cryptographic standards adopted by public and private entities are conforming to the needs of the times.[186] The encryption policy must also focus on promoting home-grown cryptographic technology, while also fostering innovation in cyber security. In such pursuance, the government could look at emerging technologies like blockchain to secure cyber data.[187]

[183] Bedvyasa Mohanty, *'Going Dark' in India: The legal and security dimensions of encryption*, December 13, 2016, https://www.orfonline.org/research/going-dark-in-india-the-legal-and-security-dimensions-of-encryption/ (Last visited on June 27, 2018).

[184] National Institute of Standards and Technology, *NIST Cryptographic Standards and Guidelines Development Process*, 3 (2016).

[185] Memorandum from the Executive Office of the President of the United States to the Heads of Executive Departments and Agencies, (October 30, 2015), available at https://www.hsdl.org/?view&did=788143 (Last visited on June 28, 2018).

[186] It must be pointed out that the Joint Cipher Bureau of the Government of India has the jurisdiction over issues of public key and private key management, production of customised cryptographic products, *etc*. However, the Bureau serves mostly as an arm of the Indian Army as it provides it with tactical cryptographic equipment and the management thereof. *See* Sukanya Bhaumik, *Cryptography and Law* in On Cyber Crime And Cyber Law 538, 551 (G. S. Bajpai, 2011).

[187] A blockchain is a 'distributed database' based on the concept of 'distributed ledger', where each member is responsible for verifying the data being added. A block is basically a piece of data created by one user and verified by any of the other users. Each and every transaction made by a user, which is stored in the form of a block, is verified by the others forming a chain of sequences. Hence, it is known as 'blockchain'. Blockchain uses 'hash algorithm' to secure information as well as create a digital signature. This takes away the need to use keys for verification. Instead, the data distributed through nodes is independently verified, and if someone tries to change information on a particular block, the nodal network analyses the whole mass of chains, compares them to the previous transactions and excludes any data which doesn't match with the sequence. Thus, blockchain offers a totally different approach to storing information and making transactions, where transactions between unknown actors will be highly secured without any outside interference. *See* Omri Barzilay, *3 Ways Blockchain is Revolutionizing Cybersecurity,* Forbes, Aug 21, 2017, https://www.forbes.com/sites/omribarzilay/2017/08/21/3-ways-blockchain-is-revolutionizing-cybersecurity/#438aeb622334 (Last visited on June 28, 2018); Meghna Bal, *Leveraging technology for trust: A blockchain-based Aadhaar?*, September 13, 2017, https://www.orfonline.org/expert-speak/leveraging-technology-for-trust-a-blockchain-based-aadhar/ (Last visited on June 28, 2018).

A new encryption policy must focus on fostering co-operation between the law enforcement agencies and the private sector. Instead of focusing on weakening the encryption standards, the law enforcement agencies must effectively use the surveillance powers that they already have. Many OTT service providers store certain metadata.[188] Metadata analysis could offset the loss of encrypted content and increase the proficiency of criminal investigations. However, as pointed out in the previous chapter, the present legal structures do not provide for the necessary constitutional and legal safeguards. Therefore, the decryption rules must be amended to reflect these concerns. Further, most of the criminal investigations get delayed because the law enforcement agencies are not able to effectively analyse the available metadata.[189] Therefore, the urgent priority must be to train digital forensic and cyber-crime specialists, and to harmonise their work with law enforcement agencies.

The government could also consider formulating a law legitimising government-sponsored hacking.[190] Instead of mandating service providers to create back doors in their crypto systems, the government could ethically hack or exploit the vulnerabilities of such systems in order to extract relevant data. Countries like France, Germany, Poland and the United Kingdom have enacted specific legislations allowing the law enforcement agencies to use hacking techniques.[191] For example in the United Kingdom, the Investigatory Powers Act, 2016 permits law enforcement agencies to interfere with the electronic devices.[192] However, this power is not unbridled. To engage in hacking, the law enforcement agencies must seek a warrant from the appropriate law enforcement chief and get it approved by a Judicial Commissioner.[193] Thus, due process must be followed by the government before it intrudes upon the privacy of an individual.

In recent years, the number of OTT service providers has increased substantially. However, many of them operate anonymously and without any registration, making it difficult for the investigating agencies to collect data from

[188] For example, WhatsApp stores user information like mobile phone number, location information, usage and log information, device information like hardware model, operating system information, signal strength, mobile network, *etc*. WhatsApp's privacy policy states that it collects, preserves, and shares this information with the law enforcement agencies whenever the latter asks. *See* WhatsApp Legal Info, *WhatsApp Privacy Policy*, April 24, 2018, https://www.whatsapp.com/legal?eea=1#how-we-process-your-information (Last visited on June 29, 2018).

[189] A. Agarwal, M. Gupta & S. Gupta, *Systematic digital forensic investigation model*, 5(1) International Journal Of Computer Science And Security 118, 122 (2011).

[190] Instead of weakening the encryption standards, the government could try to find the vulnerabilities in them with legal backing. *See* Steven Bellovin et al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the internet*, 12(1) Northwestern Journal Of Technology And Intellectual Property 1, 5 (2014).

[191] European Parliament, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*, 10 (2017).

[192] Investigatory Powers Act, 2016, Part V, Chapter 2 (U.K.).

[193] Investigatory Powers Act, 2016, §229.

them.[194] Thus, it must be made mandatory for all the OTT service providers/social networking sites to register with the Government of India, or at least designate a legal representative in the country. However, this does not mean that they will have a data sharing agreement with the government, as was proposed in the draft NEP. This will make sure that the OTT service providers/social networking sites are effectively complying with the lawful directives issued by the law enforcement agencies and courts, without compromising their service standards in any way.[195] Further, the government could also impose sanctions on those service providers who refuse to register or designate a legal representative in the country.[196] Though this step may seem to be authoritative on the face of it, one must not lose sight of the fact that the OTT service providers are business companies with the sole motive to earn profit.

The government should adopt a targeted approach towards encryption rather than a general approach, *i.e.* instead of compelling the intermediaries to decrypt the data, an approach of compelling decryption by the individual

[194] Madras High Court v. Union Ministry of Communications, Govt. of India., 2017 SCC OnLine Mad 25298, observed:

> "[t]he investigators are often at a dead end because they have neither the access to the communication inside the OTT services/social networking sites nor could they collect the crucial user information required for investigation from the anonymous service providers. For instance, no one knows who is operating "Telegram". It does not have a nodal officer who can be called upon to comply with the directives that may be issued by the law enforcement agencies. Even if they are available in India, they tend to take the stand that the OTT service/social networking service is provided by another company incorporated in USA or any other foreign country and that therefore they are not in a position to furnish the information sought for. They also claim that they do not have the obligation to comply with the directions issued by the Indian Authorities.")

[195] Many OTT service providers like WhatsApp and Telegram have reluctantly agreed to register with foreign governments. Similarly, they must be forced to register or at least designate a legal representative in the country so that they may be called upon to comply with the directives of the court. *See* The Financial Times, *Telegram founder agrees to register app with Russian censors*, June 29, 2017, https://www.ft.com/content/8bfc8e20-5c15-11e7-9bc8-8055f264aa8b (Last visited on July 2, 2018).

[196] The government could effectively ban recalcitrant service providers by blocking the Internet Protocol (IP) addresses associated with them. For example, Russia blocked nineteen million IP addresses associated with the messaging application Telegram. Most of these IP addresses were hosted by Google. Therefore, the Indian government can effectively ask hosts like Google and Apple to ban the unregistered applications from their servers. *See* The Guardian, *Russia blocks millions of IP addresses in battle against Telegram app*, April 17, 2018, https://www.theguardian.com/world/2018/apr/17/russia-blocks-millions-of-ip-addresses-in-battle-against-telegram-app (Last visited on June 28, 2018); Aaron Mak, *What's Happened Since Russia banned Telegram*, SLATE, April 25, 2018, https://slate.com/technology/2018/04/russian-internet-in-chaos-because-of-telegram-app-ban.html (Last visited on July 28, 2018); Apple and Google have been complying with government requests to block content. However, this also depends upon the business of these companies in the particular country and the influence the government has over these companies. *See* The New York Times, *Apple Removes Apps From China Store That Help Internet Users Evade Censorship*, July 29, 2017, https://www.nytimes.com/2017/07/29/technology/china-apple-censorhip.html?_r=0 (Last visited on June 28, 2018).

consumers of these products could be taken.[197] Further, every request for decryption, both from the intermediary as well as from the consumers, must be warranted by a judicial magistrate because it entails a higher degree of intrusion than a standard search and seizure.[198] The government must recognise the fact that encryption is a market strategy adopted by the companies to attract consumers in this privacy conscious world. However, the market forces themselves will restrict the use of encryption, especially end-to-end encryption, because majority of the OTT service providers/social networking sites rely on access to user data for revenues and product functionality.[199]

VII. CONCLUSION

This paper attempted to understand cryptography, its applications, national security threats, and perceptions. Modern forms of encryption has pervaded nearly all levels of everyday technological use. It has greatly helped in securing instant internet messaging, online banking transactions, e-commerce, internet browsing, *etc*. However, cryptography, like any other technology, has its fair share of drawbacks. Inadvertently, it has also created 'safe spaces' for criminals to operate in. In the course of the paper, it has also been shown that the binary of 'privacy versus security' is false, because decryption of necessary and accessible data can be lawfully achieved to further criminal and national security investigations without debilitating the privacy of citizens. To this end, the presently applicable decryption rules must be amended to reflect the recent developments in privacy jurisprudence in India, United States and Canada.

[197] The House Judiciary Committee & House Energy and Commerce Committee of the United States in its year-end report observed that "compelling decryption by the individual consumers … [o] n a case by case basis, with proper court process, requiring an individual to provide a passcode or thumbprint to unlock a device could assist law enforcement in obtaining critical evidence without undermining the security or privacy of the broader population." *See* House Judiciary Committee & House Energy And Commerce Committee, *Encryption Working Group Year-End Report*, 12 (December 20, 2016); however, forcing individuals to decrypt data which could be self-incriminating will be violative of Art. 20(3) of the Constitution of India. Though the Indian courts haven't dealt with this situation at large, the courts in the United States have dealt with it at length with somewhat contradictory stances. In United States v. Fricosu, 841 F. Supp. 2d 1232 (D. Colo. 2012), the Tenth Circuit Court held that the Fifth Amendment privilege was not applicable to compelled decryption if the existence of the encrypted contents was a "foregone conclusion". However, the Eleventh Circuit Court in United States v. Doe, 670 F.3d 1335 (11th Cir. 2012), rejected the 'foregone conclusion' doctrine. It observed that compelled decryption, though not incriminatory, forms a part of a "chain of evidence that is designed to lead to incriminatory evidence" which is "sufficient to invoke the Fifth Amendment privilege." *See* Riley Atwood*, The Encryption Problem: Why the Courts and Technology are Creating a Mess for Law Enforcement*, 34 Louis U. Pub. L. Rev. 420 (2014).

[198] Jill M. Ryan*, Freedom to Speak Unintelligibly: he First Amendment Implications of Government-Controlled Encryption*, 4(3) William & Mary Bill Of Rights Journal 1165, 1171 (1996).

[199] Gasser, U., et al, *Don't Panic: Making Progress on the "Going Dark" Debate*, Berkman Center Research Publication 3, 2016.

Any new encryption policy which the government intends to formulate must aim at securing India's digital infrastructure. This paper argued that the use of strong encryption must be promoted with an aim to secure the sacrosanct constitutional rights of the citizens and to remedy the power imbalance between the citizen and the state. The government could also take a leaf from the proposed European e-evidence rules by making it mandatory for the service providers to designate a legal representative in the country, so as to ensure effective compliance with the court directives. The Indian government could also look at other methods of accessing available data like legal hacking.

Technologies like cryptography potentially affect our behaviour and the way we live our lives. However, there is little understanding between the general masses as to how it works. Similarly, the Government also seems clueless as to how it should be regulated. The larger objective of this paper has been to address all the general and technical concerns associated with cryptography and to provide solutions to better regulate it. No technology can be perfected unless it is tempered and tailored to reflect the legal theory developed to secure the life and liberty of people.