**GOVERNMENT ACCESS TO ENCRYPTED COMMUNICATION**

**BY**

**DEEPTIKA SINGH**

**2ND YEAR, B.A LL. B**

**AMITY LAW SCHOOL, NOIDA**



 **www.probono-india.in**

**ABSTRACT**

The purpose of this research paper is to examine the effectiveness of encryption and to theextent it becomes a minacious. The research aims at explaining in detail the very meaning of encryption, how it affects our way of communication and does it safeguard our privacy.

My research finding indicated that though encryption aims to protect the privacy of users it has its deficiencies and disadvantages. One of the disadvantages in small scale is the flow of erroneous and inaccurate the flow of information and at large scale, rackets of child pornography and planning of crimes, etc. because of which there has always been scrimmage between governments and private service providers, which is one of the main subject matter of this research paper. Countries have form legislation to work and regulate the working of such applications like Australia U.S.A, China, etc. whereas India is still working on the formulation of such legislation. One of the attempts made by the government was the creation of the Draft of National Encryption Policy which did not gather enough support from experts and citizens and was ultimately withdrawn. The research paper greatly deals with all the regulations, law, provisions, acts, bills that have been made regarding the encryption in India. As India at this time do not have any law specifically devoted to encryption which makes it extremely difficult for the government to manipulate foreign companies’ services to form it according to the needs of the country.

**INTRODUCTION**

Privacy is one aspect of life that concern everyone. Every person has its level of privacy which he/she wants to secure from others, even when it comes to communication. This is the reason why nowadays people are moving to the application which provides a secure flow of data and communication like, for example, WhatsApp, Facebook, etc. which is done through a method called “Encryption”, however, applications like these many times proves to be a pain for the government. Encryption is important when it comes to protecting the information and data of private individuals, also Right to Privacy is one of the Fundamental Rights as declared by the Supreme Court, under article 21. However, is it not possible to study the concept of encryption only from one side. Encryption also invites negative effects as because of the high level of encryption security and end-to-end encryption give easy access to the commission of crimes and also get away with it easily as no one can trace the origin of the information or such user engaged in such activities, even companies themselves who are providing such service fails and a result government also face obstruction in tracking the culprit and maintaining law and order. All this scenario sincerely speaks of the need for laws that are specifically concerned with encryption, meaning, level of security, the flow of personal information, encryption provided by foreign and domestic companies. However, even after many attempts the Indian Government fails to make Legislation surrounding this particular field of technology, some of the attempts were draft of encryption policy, personal data protection bill. Even though there is the absence of such laws it doesn’t mean India is fully deprived of Encryption laws, many acts and rules contain some provisions regarding it but it will not be wrong to say that they are not enough to handle such a vast emerging phase of increasing interaction of technology with the rapidly increasing flow of information and communication. This paper deals in every detail with all aspects of encryption, its increasing impact on government, individuals, laws, and attempts to answer the question as to what extent can government access encryption communication.

**WHAT IS ENCRYPTION?**

Encryption is a process to encode a message or text into unreadable random text by use of a key. That key is called the Encryption key. This text or message is to be encrypted is called plaintext. That key contains algorithms to change the plain text into a secret coded looking text, which can be obtained by the help of a decryption key. This secret code is technically called ciphertext. This decryption key is already given to the receiver. Key algorithms are based on the set of mathematical values which can be reversed to change ciphertext again to plaintext. These encrypted messages are sent to the receiver, by the help of a decryption key these messages are decrypted by the receiver and then turned into understandable text. Without the key even if these messages are to be hacked or have any unauthorized access, it would be highly unlikely to understand its meaning.This process of encryption and decryption is called cryptography.[[1]](#footnote-2)There are two type of Encryption: -

1. Symmetric key encryption
2. Asymmetric key encryption

**Symmetric Key Encryption:**In symmetric key encryption only one key is used to encrypt and decrypt the plaintext. It is more efficient than Asymmetric encryption hence it is used when a high amount of data is to be transferred. There are two types of Symmetric encryption:

1. Block cipher: - In this predetermined number of bits are taken from the plaintext and encrypt that block. Block size can be different for different types of encryption example 32bits, 64bits,128 bits.
2. Stream cipher: - It encrypts each bit and then sends it. It encrypts 1 bit at a time.

Block cipher is used most, though it is slower than stream cipher, but it is more efficient and can operate on large size hence it is more used. Blockcipher can act as a stream cipher when the block size is set as 1 bit.[[2]](#footnote-3)

**Asymmetric Key Encryption**: In Asymmetric key encryption there are two keys one in encryption key and the other is decryption key. Once the message is encrypted, it cannot be decrypted by an encryption key. It can only be decrypted by using the decryption key. In other words,once the message is encrypted even the sender cannot read it without a decryption key.The asymmetric encryption key is known as the public key, and the decryption key is known as the private key. Asymmetric encryption is safer than symmetric encryption. But it requires a high level of processing, hence takes more time, and therefore it is not used in encryption.

Working on encryption: It is a simple processin which the sender decides which encryption is to be used to encrypt. The sender converts the pain text into ciphertext and sends it. The receiver receives the messages and decrypt the message by the decryption key provided, and reads it.[[3]](#footnote-4)

**THE DRAFT OF NATIONAL ENCRYPTION POLICY**

The government of India under section 84A of the information technology act 2000 have the power to issue methods or modes for encryption. Section 84A was inserted by information technology amendment act 2008, and read as under:

Section 84A: Modes or methods for encryption. - The Central Government may, for secure use of the electronic medium and promotion of e-governance and e-commerce, prescribe the modes or methods for encryption.[[4]](#footnote-5)

Accordingly, a draft was made by an expert team, the public allowed to express comments on the drafted policy through email or letter to Shri A. S. A. Krishnan, scientist, one of the members of the expert team. Largely the policy laid down the vision, objective, strategies, and regulations to be followed by every authority and individual.[[5]](#footnote-6)Before diving into the drafted policy it is important to first understand the meaning of the terms which largely concern the policy. Cryptography- it can be explained as a method through which protection of information and communication between parties is ensured through the use of codes. In computer science, cryptography refers to techniques through which information and end-to-end communication is made undecipherable employing algorithms and mathematical concepts, which can only be made decipherable by the use of the symmetric key. It is a powerful tool to ensure confidentiality and integrated communication in transmit as well as storage. Originally it was used to safeguard the confidentiality of information of diplomatic and military communication but with the advancement in computer technology and revolution of the internet with time and increase use online applications as well as the recent innovations of encryption, a new market for cryptographic products in E-commerce & E-Governance has developed rapidly. Communication and E-commerce applications such as E-mails and fund transfer, E-banking, etc. which require secure communication, makes considerable use of encryption for securement of information and authentication of the same. The Information Technology Act, 2000 provides modes and methods for encryption (Section 84A) and decryption (Section 69). This policy takes into account the need to protect information resources, national concerns for security. The policy supports the broad use of cryptography that can facilitate individual as well as businesses' privacy and international economic competitiveness including the government.

This policy is not uniform but includes largely every sector under its cover. The policy does not apply to sensitive departments as well as agencies of the government mainly designated and performing sensitive and strategic duties. This policy applies to all Central and State Government Departments including sensitive Departments and Agencies performing nonstrategic & non-operational duties, all statutory organizations, executive bodies, business and commercial establishments, including public sector undertakings and academic institutions and all citizens including Personnel of Government as well as Business performing non-official and personal functions. The policy aims at providing confidentiality to information on the internet, protection to sensitive or exclusive information of individuals and of businesses, and ensuring coherence of national critical information network systems. The policy gives three main objectives, first, for the act of synchronization with the global digital economy, the use of encryption for security purposes, ensuring the confidentiality of the information/data. Second, to encourage extensive use of digital signature by different institutions including government. And third, to encourage the promotion of information security by all institutions including stakeholders of government, individuals, and citizens engaged in industrial activities. They all have to work according to the guidelines provided under the policy if it was passed by the government which was not as after the draft was released in the general public it received massive criticism which resulted in the withdrawal of the policy.

The policy describes the category of users which is based on the type of management that requires encryption. The users are categories as: “G” Government both Central and State Government and their Departments including sensitive departments and agencies. Then “B” which includes within its ambit all statutory organizations, executive authorities, commercial enterprises, and educational institutions. “C” All citizens.

“G2G”- Government to Government users. “G2B”- government to business, “G2C”- government to citizen, “B2G”- business to government and “C2G”- citizen to government. The policy lays down the use of Encryption technology for communications between the “G” group and “B” or “C” groups with protocols and algorithms, key, Digital Signature which has to be notified by the Government occasionally. Organizations within “B” and “C” groups were granted discretion to use Encryption for storage and communication purposes. Encryption algorithms and key sizes according to the policy has to be prescribed by the Government. The policy also included the condition that the user has to produce Plain text and encrypted text pairs using software or hardware which is used in such context.[[6]](#footnote-7)Such plain text information has to be stored by the user or organization or agency for 90 days from the date of the transaction and has to be made available to the Law Enforcement Agencies. According to the policy, when communication is established with foreign, the responsibility was laid down on a service provider located in India for providing readable plaintext with Encrypted information. Service Providers whether located in or outside India, using Encryption technology was directed to enter into an agreement with the Government for providing such services in India. It will be the Government’s responsibility to form a proper agency for agreeing with the Service provider. And the users of group “G”, “B” or “C” taking services from the Service Providers are also accountable to provide plain text when demanded by the authority in charge.

This policy also lays down that all vendors who are in charge of encryption products have to register their products with the designated authority assigned by the government for running a business in the country. For registration, the vendors were required to submit the working copies of the encryption software/hardware and 4 professional quality documentation, test suites, and execution platform environments. The vendors were required to renew the registration when the encryption products they are using is upgraded. Mass use products like SSL/TLS are exempted from registration. The Government has to notify the list of registered encryption products occasionally without taking responsibility for security claims made by the vendors. Encryption products was permissible to be exported outside the country but only with prior announcement to the designated authority. Users in India are allowed to use only the products registered in India. The government was given the power to take appropriate action as per Law for any violation of this Policy.

When the policy was exposed to the public for the comments, it received a massive backlash and criticism specifically for its being in vague and uncertain language and compels everyone to store their data for up to 90 days. In response the government later added a supplement to the draft policy which specifies that communication platform like WhatsApp, Facebook, Twitter will be exempted from such policy, later on, in next few days it was announced by the Communication and IT minister Ravi Shankar Prasad that the said policy was withdrawn.[[7]](#footnote-8) To this policy many experts and specialists pointed out the even if this policy was implemented it would not be a success because many users don’t know even the meaning of Encryption, moreover in many cases it is not done by the users but the application that it is used.[[8]](#footnote-9)

**Criticism**: The policy was highly criticized mainly because it violated the privacy of people. According to the draft users were required to store their data in plain text for 90 days and were further required to submit such data to the authority assigned by the government on demand. Many users in India are unaware as to the meaning of the plain text because of which they can be easily be held liable for not submitting the same and disobeying the order of the government.[[9]](#footnote-10) All responsibility was held on the users or organization, in the case where the communication is with foreign entity whole responsibility was laid down onto the user located in India. The user or service provider was also required to register the encrypted products and in case of up-gradation, renew them. The provision in the eyes of people was held illogical and uncertain. The policy gives a very easy way not only to the government but also to the cybercriminals a way to corrupt the sensitive information of the people instead of saving it, which was the motto of the policy.

**LEGALITY OF ENCRYPTION**

India does not have a fully formed and enacted act or laws related to encryption as such, though many attempts were made none of them turned out to be successful. The government has always stated the implementation of encrypted laws that many developed countries have some kind of encryption policy or laws to relate the flow of data and information for counties security purposes. So far nothing has been achieved. Multinational companies in India have also presented the dissent regarding the introduction of encryption laws and choose to maintain their privacy with their users. India, like said above, do not have any enacted act or laws which solely focuses on Encryption, however, some regulations and power have been conferred by many acts to the government to makes certain law in this regard.[[10]](#footnote-11) Following are the list of such acts which further will be dealt with detail:

1. The Information and Technology Act, 2000
2. The India Telegraph Act, 1885
3. The Reserve Bank of India Act, 1934
4. The Securities Exchange Board of India Act, 1992
5. The Payments and Settlements Act, 2007

**THE INFORMATION AND TECHNOLOGY ACT, 2000**

IT services are India is largely regulated by the Information Technology Act, 2000, and is one of the principle acts in the matter of encryption so far in India. **Section 84A** of the IT Act, 2000 was inserted by the IT (amendment) act 2008 and grants specific powers to the government to prescribe such modes and methods for e-governance and secure use of the electronic medium as deems to be necessary. However, the meaning of what “modes” and “methods”, has not been defined by the government and there exists a certain level of uncertainty as to what level of bits should be used by the companies and service providers.[[11]](#footnote-12)To this, companies in India generally use 256 bits level encryption. Also, section 35 of IT Act, 2000 provides enactment for certifying authorities to use electronic signatures.[[12]](#footnote-13) Under the Information Technology (Certifying Authority) Rules, 2000, rules have been laid down by the central government for certifying authorities. In addition to this rule 6 of the Information Technology (Certifying Authority) Rules, 2000, lays down “standards” that have to followed by the authorities:

*Rule 6: Standards: The Information Technology (IT) architecture for Certifying Authorities may support open standards and accepted de facto standards; the most important standards that may be considered for different activities associated with the Certifying Authority’s functions are as under-*

*….*

*RSA Public Key Technology- PKCS#1 RSA Encryption Standard (**512, 1024, 2048 bit)[[13]](#footnote-14)*

The only reference to a specific bit-level, when made under the Information Technology Act, 2000, regarding the certifying authority is 512, 1024, at maximum 2048 bits.

**THE INDIA TELEGRAPH ACT, 1885**

the India Telegraph act, 1885 is the main act in India that regulates communication. Section 3(1) defines "telegraph" as: -

*“… any appliance, instrument, material or apparatus used or capable of use for transmission or reception of signs, signals, writing, images, and sounds or intelligence of any nature by wire, visual, or other electro-magnetic emissions, Radio waves or Hertzian waves, galvanic, electric or magnetic means.”*[[14]](#footnote-15)

Section 4(1) provides to the Central Government the power for the establishment, maintaining, and working for telegraphs in India. This shows that, according to the act, the Government of India has special control over electronic communications which also includes providing telecommunication and internet services in the country. However, **National Telecom Policy, 1999**, states the policy of liberalization according to which the Government of India has allowed private service providers and such companies to provide these telecommunication and internet services, over which the central government had the monopoly, by entering into licensing agreements with the government.[[15]](#footnote-16)Many times government enters into agreements with companies providing services and collecting electronic information for the sake of security. Such acts of government can often take the form of a "licensing regime" where only those companies are allowed to give services in the country who have entered into the agreement with the government and are allowed to operate in the market such. And because of this companies and consumers always look for ways to avoid it, they do not want the government to have discretionary power over them. There is a very high possibility that governments then will only favour those services that allow them unhindered access to data and make communications unsecured. Law enforcement agencies need technical assistance while handling encrypted data which can only be provided by the company. Many countries, for instance, Israel use the licensing regime to gain control over the encrypted communications. The stated objective by Israel's government is to take over 10 encryption technologies. However, mechanism of licensing is lenient in force but instead helps in keeping relations between government and concerned companies. This relation helps keep the authorities of government very well aware of technical developments that take place in the field of cryptography and critical circumstances, enables the exchange of information. India can also adopt some similar methods to allow corporative work with corporations and maybe even exchange of information with private parties. An alternative to a licensing arrangement is a voluntary registration mechanism in which where encryption providers voluntarily register with the government instead of government choosing who can operate in the market. The companies can also provide information such as the level of encryption they are using in their software. As this registration process is fully voluntary, there is no penalty for not registering.[[16]](#footnote-17) In India the licensing agreement which is entered between government and the private party depends on the type of technology and service provided by the private party (internet service provider) and the government policy existing at that time. It is named under the Internet Service Providers License Agreement (ISP License),[[17]](#footnote-18) this agreement is specifically entered with the Department of Telecommunication (DoT). This agreement gives access to the ISP to provide internet services. Under clause 37 of the license agreement it is specifically stated that the licensee is not eligible to deploy bulk encryption equipment.[[18]](#footnote-19)However, this does not mean that the licensee is free from ensuring the protection of private communication.

*Clause 37 and 37.5 of the license agreements: -*

*37. Confidentiality of information: 37.1 The Licensee shall not employ bulk encryption equipment in its network. Licensor or officers specially designated for the purpose may evaluate any encryption equipment connected to the Licensee’s network. However, the Licensee shall have the responsibility to ensure the protection of privacy of communication and to ensure that unauthorized interception of MESSAGE does not take place.*

*37.5 The use of encryption by the subscriber shall be governed by the Government Policy/rules made under the Information Technology Act, 2000.*

**RESERVE BANK OF INDIA ACT 1934**

Reserve bank of India is India’s Central bank which was constituted under the Reserve Bank of India Act, 1934 and according to payments and settlements act, 2007, the reserve bank of India also serves as a regulator of electronic banking. The reserve bank of India laid down in its ‘report on internet banking’ dated 22 June 2001 some level of encryption for purposes of transaction, also Clause **7.5.4** of the report specifies that internet banking services provided by the banks have 128 bit strong encryption which is widely accepted worldwide as a security standard for financial transaction. Also, clause **8.4.7.3** specifies that all transaction will be authenticated using ID and password and also the 128-bit has to be used as the minimum level security.[[19]](#footnote-20)

**THE SECURITIES AND EXCHANGE BOARD OF INDIA, 1992**

The Securities and Exchange Board of India also directs, for security trading over a phone or a wireless application, the use of 64-bit/128-bit encryption, like the Reserve Bank Of India Act, for grade level network security and use of secured socket layer (SSL) security ideally with 128-bit encryption, for securities trading over a mobile phone or a wireless application platform.

So, overall it appears that there is no specific or uniform level of encryption laid down in any acts or statues so far. Every act specifies its level of encryption that has to follow by the respective authority whether it is for internet Banking purposes or for providing internet services as laid down under the report of internet banking by the reserve bank and by the information and technology act. However, the highest level of encryption approved is 2048 bit under IT act. The uncertainty persists and will be in the future unless a uniform policy or act comes.

**BLACKBERRY CASE, 2007–2012**

The first incident that questioned blackberry services in India and its devices occurred when the Indian government directed Research in Motion’s (RIM) BlackBerry to give law enforcement access to its encrypted data for national security purposes. RIM, like other applications working in India was not subject to the encryption controls specified under the license agreements applicable to telecom companies. On December 31, 2007, the Department of Telecommunication asked the company to stop its services in the country as they cannot monitor the content operated through blackberry devices. The Indian government made it clear to the company that their services will be cut off if they fail to comply with the government to give them lawful excess to encrypted communication. Then came into the picture the 2008 terror attacks in Mumbai and discloser of the facts the individuals involved in these attacks communicated through the blackberry devices with their handlers located in Pakistan.[[20]](#footnote-21) These attacks intensified the demand of the government. In response RIM suggested solutions, one of which was to reduce its encryption level from 256 bit but the government demanded RIM to relocate its server and give access to its encryption keys.

To which, in 2010, RIM agreed to locate in servers in India and to grant plaintext of communications sent through blackberry messenger.[[21]](#footnote-22) This whole incident shows the government is very much in power to lower the security levels of communication services by sustained pressure. This also contributed to the downfall of the blackberry market in India considerably in the following years.

**DRAFT PERSONAL DATA PROTECTION BILL 2019**

In the year 2018 the personal data protection bill was introduced which was passed by the cabinet minister in 2019, it yet be passed by the parliament. The Bill recognized the right to privacy as a fundamental right as held by the supreme court of India in case Puttaswamy v. Union of India[[22]](#footnote-23) 2017. And states the need to respond to the misuse of personal data by private companies located in and outside India. The Bill deals with the processing of personal data by the government, companies located in India, and foreign companies having access to personal data of the individuals in India. Personal data is data that is related to the characteristics and attributes of identity, which can be used to identify an individual. [[23]](#footnote-24)The Bill recognizes certain personal data as sensitive personal data. Such sensitive data includes financial data, biometric data, caste, religious or political beliefs, or any other category of data as specified by the Government, in consultation with the Authority.[[24]](#footnote-25)

The draft Personal Data Protection Bill, 2019, mandates that sensitive personal data that is stored in mirror servers located in the country and all critical personal data should be processed and stored in India. The bill state provisions for the setup of data protection authority, which if passed, will have the power to protect the interests of individuals, safeguard their personal information, prevent the misuse of the same. The central government will have the power to exempt any authority from the preview of the bill on certain grounds.

In recent years India Government has become very concerned about the protection of its individuals and their information. However, it has failed to form any uniform law which can govern the foreign applications in the country and restricts their sources in India or define a specific encryption security level to be followed by such services. Applications like WhatsApp, Facebook, twitter do not come under the cover of the IT act and is not governed by the same, such services results to be problematic with the orders of the government. [[25]](#footnote-26)

**WHATSAPP AND PUBLIC ORDER**

Over the last few years many cases have been reported of mob lynching agitated by WhatsApp “forwards”. The forwarded messages themselves are not true information but edited videos and images and wrong messages and information targeting one community against other, against political leaders with wrong information these all are part of coordinated misinformation campaigns to which normally individuals easily fall, one of the most significant cases over the year, which frequently repeat itself is the circulation of wrong messages, usually in rural areas, about child abductors and as a result, villagers become very furious and agitated towards any outsiders and in many cases murders, mob lynching and violence has been reported.

To ensure public order and to find the source of such circulation of wrong information the government demanded WhatsApp should allow tracing of such messages and help to find the identity of the original sender. However, WhatsApp has not accepted such demand but has introduced other measures such as the label on forwarded messages and restriction on sending 5 persons at a time. From 2016 to 2020 there has been a constant tussle between the government and this messaging application, which have been explained in detail under the following heads.

WhatsApp enabled its end to end encryption in April 2016 for its all users. That encryption is of 256 bits. The encryption was to protect the data from cyber thieves. But this creates a problem for the government, since the data sent from user to receiver in forms of text, video, images or document can only be accessed by the receiver, because not even the WhatsApp does not keep any decryption key for its user’s privacy concern. This creates a problem if governments require data. This is a similar case to apple vs FBI, Apple prevented sharing its user data to the government or the FBI. 450 million Indians are using WhatsApp which is almost 90% of smartphone users in India, those are provided with this secured and prevented government to have information about these users.[[26]](#footnote-27) These uses are provided with the best privacy makes the government more concerned with the national security of India. A license is required from the Department of Telecommunication to provide such secured services to telecom service providers and internet providers, like Airtel and Vodafone. But these licenses come with many restrictions like license fee, the privacy of user/customer information, and requires lawful interception, security of the network, and monitoring. Applications are not telecom service providers nor internet service providers like WhatsApp, Viber and skype, etc, these are terms as “Over The Top” (OTT) service. It has been taken from its common usage from telecommunications. These Over The Top services does not have any specific laws and without any specific regulation they are governed by IT Act provisions and by other legislation applicable to their services. But due to no regulations and rules being present at this time, WhatsApp end to end encryption policy is legal, which is also a big dilemma for the government. OTT services like WhatsApp is in an area with no legal precedent or rules to whether to allow it or deny its use of 256-bit end to end encryption for messaging, it's only making its service available to users and not limited by any agreement license regarding the encryption policy.

 This issue of Over The Top is being and also faced in other countries and these countries have already dealt with this problem. These problems are taken care of differently in different countries. Like in France, Skype is made to register as a telecom operator, which means that Skype cannot take advantage of being one of the OTT services. In china Voice Over IP (VOIP) calls are made. This VOIP has a different regulatory system under the head of “voice-base call", also these voice-based calls will be subjected to the same security requirements as telecom providers. Similarly, in Germany VOIP is also given the same requirements as other telecom services which was due to the neutral approach of its telecommunications. This tells that even other countries do not have any rules and regulations.

WhatsApp, being an intermediary, is expected to comply with directions to intercept, monitor and decrypt information issued under Section 69 of the Information Technology Act, 2000. According to the “The Economics Times” report, In 2019 Indian government asked WhatsApp to add a digital fingerprint for all the data which was sent by the App. These digital fingerprints will allow to keep track of the messages without causing any harm to the privacy of the user by WhatsApp. This will allow the government to find information of the message, who read it, how many times it was forwarded, who forwarded it and to whom it was sent or forwarded, or where it originated.[[27]](#footnote-28) The demand made by the Indian Government was influenced by one of the acts of the Australian government to apply some methods which allow them to spy on applications like WhatsApp.

Singapore also passed an anti-fake news law (Protection from Online Falsehoods and Manipulation bill) that gives access to the government to keep track of all messaging apps and even of private chat groups. However, if the same demand is considered by Indian government may not end as satisfactory as it did in Singapore and can even lead to a crisis as such route of access hackers and government of other countries as well and will give easy access to cyber-criminals and hostile forces raising serious security issues.[[28]](#footnote-29) In February 2020, India’s Ministry of Electronics and Information Technology was expected to reveal the new rules. Which will give access to the government to identify the identity of the user behind the post. The rules would at large impact services like WhatsApp. The draft provisions laid down that the companies have to give the concerned information to the law enforcement agencies within 72 hours of receiving such a request and were also required to keep their record for at least 180 days. The tech firms would also have to keep their records for at least 180 days.[[29]](#footnote-30)

The rules would apply to any service having more than 5 million users, but it is unclear if the government will be apple to find users outside India. Many experts hold the view that it will be against the right to privacy and freedom of speech.

**A BRIEF SUMMARY OF ENCRYPTION LAWS IN OTHER COUNTRIES**

1. Brazil:In Brazil there is no permission to encrypt the data however its constitution says that there is absolute privacy of the data which is in the form of messages, telecommunication. Permission to access the data can only be given by the court order.[[30]](#footnote-31)
2. Canada:There is no specific law for providers to give access to the encrypted data. But law enforcement officials have access to the data under the orders from the court.[[31]](#footnote-32)
3. Sweden: Laws have been made regarding forced decryption but they lack force and have not been adopted. Every search has to go through a proportionality test. One of the recent cases held that searches on a device can be limited because of the test moreover there has been proposals that would allow the Swedish Government to investigate in suspect’s computers through a programme called Trojan Horse Malware.[[32]](#footnote-33)
4. Japan:In Japan, Carriers are obligated to provide cooperation when required by the Criminal procedure code. However, there is no penalty for being unable to help or required to develop a decryption system.[[33]](#footnote-34)
5. Turkey: In Turkey a certain authorization is required in order to encrypt communication services which is Information and Communication Technologies Authority. And required to intercept when requested by law enforcement.[[34]](#footnote-35)
6. Taiwan: Taiwan law gives power to its intelligent agency to intercept communications for foreign governments or organizations for national security purposes. Though no law gives direct power to the government to have access to encrypted communication, it is the companies that have to acquire such hardware and software that can give access and cooperate with interception and help the government in assisting the encrypted communication.[[35]](#footnote-36)
7. South Africa: According to South African law, all Telecommunication service providers are required to store their all communication related data, messages etc. for at least three to five year and make sure that the systems can be intercepted. And this data can be intercepted by law enforcement and security agencies only through a prior permission or warrant by the court to have access to the decrypted data. Agencies are required to first obtain a warrant from the competent court for access to communication but there is no such requirement of warrant in case of emergency.[[36]](#footnote-37)

**CONCLUSION**

Encryption is used by many applications and service providers to protect the data and information of the users. Encryption is a process through which messages sent by one party converts into undecipherable random text which can be made decipherable by encryption key when received by the receiver. Encryption today is used by internet providers, Facebook messenger, WhatsApp, service providers, and private companies. Encryption in India is mainly controlled by the Information and Technology Act, 2000, in 2008 amendment was made in IT act which added section 84A which gives enormous power to the government to prescribe modes and methods for encryption, but no progress has been made by the government so far in that. No law in India is solely dedicated to encryption, the growing upgrade in technology and growing reliance on online applications speaks of the urgent need to made encryption laws for various reasons and one of which is national security. There have been many cases where the crime was initiated or planned or agitated through or by such online applications but end-to-end encryption present in such application makes it extremely difficult for the government to locate the whole racket or the original sender. Such a case was of Blackberry case in which it was found that the members of terror attacks in Mumbai communicated through blackberry devices.

A step was taken by the government in 2015 and formed a draft of encryption policy in which every person, government offices, service providers, organizations companies was required to store their data for 90 days and hand it to the authorized agency of government when demanded in plaintext form. After the draft was formed it was published for people to see and comment and as a result it received a massive backlash from experts and people saying that such a draft is vague and uncertain. Most of the people in India are uneducated and do not have proper knowledge as to how the technology works and by introducing such regulations can make them vulnerable to penalization. As a result, the policy was withdrawn by the IT minister. Acts in India also do not specify the level of encryption to be used. The Information and Technology Act, 2000 do prescribe encryption security level as 512, 1042 and 2048 under Information Technology (Certifying Authorities) Rules, 2000, standard 6, but these encryption levels are only for certifying authorities for using electronic signatures. Also, in the 2018 Draft of Personal Data Protection Bill was introduced, it not has been passed by the parliament to become and act. The draft was aimed at securing the privacy of citizens following the judgment of the supreme court which declared the Right to Privacy as fundamental right under article 21. The draft focus on the localization of personal information contained in companies and private operators. The draft also gives punishments for leaking personal information of users. However, there is a danger that localization of users’ information may be vulnerable for state intrusion and may even contribute to cybercrime, if criminals gain access to. Though encryption is very essential to maintain privacy but there are equal chances that such a platform can be used for crimes or may even facilitate one, and because of the absence of specific laws it is very difficult for the government to cope with the situation in real-time.

**REFERENCES**

‘What is encryption’ (Cloud flare) <<https://www.cloudflare.com/learning/ssl/what-is-encryption>> accessed 2 May 2020

Jeff Tyson, ‘How encryption works’ (Computer how stuff works) <<https://computer.howstuffworks.com/encryption.htm>> accessed 2 May 2020

Information Technology Act 2000, s(84A)

‘Draft of National Encryption Policy’ <<https://netzpolitik.org/wp-upload/draft-Encryption-Policyv1.pdf>> accessed 4 May 2020

‘Encryption Policy’ <<https://iapp.org/media/pdf/resource_center/India-Encryption-Policy>> accessed 5 May 2020

‘Government exempts WhatsApp, social media from Encryption Policy’ ( 22 September 2015) < indiatoday.in/india/story/goverment-exempts-whatsapp-social-media-from-encryption-policy-264161-2015-09-22 > accessed 4 may 2020

1. ‘Government to withdraw draft encryption policy’ <<https://www.thehindu.com/news/national/govt-to-withdraw-draft-encryption-policy/article7677348.ece>> accessed 6 May 2020
2. Yuthika Bhargava, ‘why encryption was withdrawn’ ( The Hindu, 11 September 2017) <<https://sflc.in/faq-legal-position-encryption-india>> accessed on 6 May 2020
3. ‘How many bits are enough ? the legality of encryption’ <<https://iltb.net/how-many-bits-are-enough-the-legality-of-encryption-d3d7b9bbc537>> accessed on 7 May 2020
4. Information Technology Act 2000, s (84A)
5. Information Technology Act 2000, s (35)
6. ‘INFORMATION TECHNOLOGY (CERTIFYING AUTHORITIES) RULES, 2000 <<https://meity.gov.in/writereaddata/files/Information%20Technology%20%28Certifying%20Authority%29.pdf>> accessed 7 May 2020

‘Indian Telegraph Act 1885’ <<https://dot.gov.in/act-rules-content/2442>> accessed 8 May 2020

‘New Telecom Policy, 1999’<<https://dot.gov.in/new-telecom-policy-1999>> accessed on 8 May 2020

1. Bedavyasa Mohanty, ‘Encryption Policy 2.0: Securing India's Digital Economy’ (ORF specialreport,May2017)<<https://www.orfonline.org/wpcontent/uploads/2017/05/ORF_SpecialReport_35.pdf>> accessed 9 May 2020
2. ‘LICENSE AGREEMENT FOR UNIFIED LICENSE’ <[https://dot.gov.in/sites/default/files/Unified%20Licence>](https://dot.gov.in/sites/default/files/Unified%20Licence%20%3E) accessed on 9 may 2020
3. License Agreement, Clause (37.1) (37.5)
4. ‘ReportonInternetBanking’<<https://www.rbi.org.in/SCRIPTs/PublicationReportDetails.aspx?UrlPage=&ID=243>> accessed 11 May 2020
5. ‘Why terrorists love the BlackBerry’ (August 24, 2010)

<<https://news.rediff.com/slide-show/2010/aug/24/slide-show-1-why-terrorists-love-the-blackberry.htm>> accessed 11 May 2020

1. ‘RIM gives in, BlackBerry server to be located in India’ ( Aug 30, 2010)
<<https://economictimes.indiatimes.com/tech/hardware/rim-gives-in-blackberry-server-to-be-located-in-india/articleshow/6462225.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst>> accessed on 12 May 2020
2. Justice K. S. Puttaswamy (Retd.) vs Union Of India And Others [2017] WP (C) 494/2012.
3. ‘THE PERSONALDATA PROTECTION BILL, 2018’ <[https://meity.gov.in/writereaddata/files/Personal\_Data\_Protection\_Bill,2018.pdf](https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018.pdf)>accessed on 12 May 2020
4. THE PERSONAL DATA PROTECTION BILL 2018 , s(3)(29)
5. ‘Encryption can secure the right to privacy’ , (the Hindu business line, 3 May 2019) <<https://www.thehindubusinessline.com/opinion/encryption-can-secure-the-right-to-privacy/article27027075>> accessed on 12 May 2020
6. ‘WHATSAPP'S END-TO-END ENCRYPTION IS LEGAL IN INDIA, BUT NOT FOR LONG’ (12 April, 2016) < https://www.firstpost.com/tech/news-analysis/whatsapps-end-to-end-encryption-is-legal-in-india-but-not-for-long-3679985.html> accessed 13 May 2020
7. ‘WhatsApp maintains its stand on govt's request for message traceability in India’ ( 19 June 2019) <<https://www.indiatoday.in/technology/news/story/whatsapp-maintains-its-stand-on-govt-s-request-for-message-traceability-in-india-1551098-2019-06-18>>accessed 13 May 2020
8. ‘India's request to WhatsApp for message traceability could impact individual privacy’ (19 June 2019) <https://www.businesstoday.in/technology/news/india-request-whatsapp-message-traceability-end-to-end-encryption-privacy/story/357311.html>accessed 13 May 2020
9. <https://ia.acs.org.au/article/2020/india-wants-to-see-your-whatsapp-messages.html>accessed 13 May 2020

‘the International Encryption debate’ ( 12 June 2019) <<https://www.lexology.com/library/detail.aspx?g=41bce78b-f790-4901-ba88-7b9f6ffdd488>> accessed 18 May 2020

‘Lawful access & and encryption in Canada’ <[https://commentary.canlii.org/w/canlii/2019CanLIIDocs2613#!fragment/zoupio-](https://commentary.canlii.org/w/canlii/2019CanLIIDocs2613#!fragment/zoupio-_Toc21976985/BQCwhgziBcwMYgK4DsDWszIQewE4BUBTADwBdoAvbRABwEtsBaAfX2zgCYBGATgHYAbDwAcAVgCUAGmTZShCAEVEhXAE9oAcg2SIhMLgRKV6rTr0GQAZTykAQuoBKAUQAyTgGoBBAHIBhJ5KkYABG0KTs4uJAA)>accessed on 18 May 2020

# ‘Online Privacy Law: Japan’ <<https://www.loc.gov/law/help/online-privacy-law/2012/japan.php>> accessed 18 May 2020

# ‘Turkey’s Data Protection Law: Long-Awaited Legislation Finally Takes Effect’ ( 7 March 2017) <<https://www.nortonrosefulbright.com/en/knowledge/publications>>accessed on 18 May 2020

### ‘World map of encryption laws and policies’ <<https://www.gp-digital.org/world-map-of-encryption/>> accessed 18 May 2020

#  ‘Government Access to Encrypted Communications: Taiwan’ <<https://www.loc.gov/law/help/encrypted-communications/taiwan.php>> accessed 18 May 2020

# ‘Sweden's new digital surveillance law’ <<https://www.thelocal.se/20200304/what-you-need-to-know-about-swedens-new-digital-surveillance-law>> accessed 18 May 2020

# ‘encryption’ (search security) <<https://searchsecurity.techtarget.com/definition/encryption>> accessed 18 May 2020

**ABOUT AUTHOR**

Deeptika Singh is a student of 2nd year in Amity Law School, Noida. She is part of the Legal Aid Committee of her college and has taken part in many camps as speaker and reporter and has done moot courts. She finds her interest more in criminal law and constitutional law.

1. ‘What is encryption’ (Cloud flare) <https://www.cloudflare.com/learning/ssl/what-is-encryption> accessed 2 May 2020 [↑](#footnote-ref-2)
2. #  ‘encryption’ (search security) <https://searchsecurity.techtarget.com/definition/encryption > accessed 18 May 2020

 [↑](#footnote-ref-3)
3. Jeff Tyson, ‘How encryption works’ (Computer how stuff works) <https://computer.howstuffworks.com/encryption.htm> accessed 2 May 2020 [↑](#footnote-ref-4)
4. Information Technology Act 2000, s(84A) [↑](#footnote-ref-5)
5. ‘Draft of National Encryption Policy’ <https://netzpolitik.org/wp-upload/draft-Encryption-Policyv1.pdf>accessed 4 May 2020 [↑](#footnote-ref-6)
6. ‘Encryption Policy’ <https://iapp.org/media/pdf/resource\_center/India-Encryption-Policy> accessed 5 May 2020 [↑](#footnote-ref-7)
7. ‘Government exempts WhatsApp, social media from Encryption Policy’ (22 September 2015) <indiatoday.in/india/story/goverment-exempts-whatsapp-social-media-from-encryption-policy-264161-2015-09-22> accessed 4 may 2020 [↑](#footnote-ref-8)
8. ‘Government to withdraw draft encryption policy’ <https://www.thehindu.com/news/national/govt-to-withdraw-draft-encryption-policy/article7677348.ece> accessed 6 May 2020 [↑](#footnote-ref-9)
9. Yuthika Bhargava, ‘why encryption was withdrawn’ (The Hindu, 11 September 2017) <https://sflc.in/faq-legal-position-encryption-india> accessed on 6 May 2020 [↑](#footnote-ref-10)
10. ‘How many bits are enough? the legality of encryption’ <https://iltb.net/how-many-bits-are-enough-the-legality-of-encryption-d3d7b9bbc537> accessed on 7 May 2020 [↑](#footnote-ref-11)
11. Information Technology Act 2000, s (84A) [↑](#footnote-ref-12)
12. Information Technology Act 2000, s (35) [↑](#footnote-ref-13)
13. ‘INFORMATION TECHNOLOGY (CERTIFYING AUTHORITIES) RULES, 2000 <https://meity.gov.in/writereaddata/files/Information%20Technology%20%28Certifying%20Authority%29.pdf>accessed 7 May 2020 [↑](#footnote-ref-14)
14. ‘Indian Telegraph Act 1885’ <https://dot.gov.in/act-rules-content/2442> accessed 8 May 2020 [↑](#footnote-ref-15)
15. ‘New Telecom Policy, 1999’<https://dot.gov.in/new-telecom-policy-1999> accessed on 8 May 2020 [↑](#footnote-ref-16)
16. Bedavyasa Mohanty, ‘Encryption Policy 2.0: Securing India's Digital Economy’ (ORF special report, May 2017) <https://www.orfonline.org/wp-content/uploads/2017/05/ORF\_SpecialReport\_35.pdf> accessed 9 May 2020 [↑](#footnote-ref-17)
17. ‘LICENSE AGREEMENT FOR UNIFIED LICENSE’ <https://dot.gov.in/sites/default/files/Unified%20Licence> accessed on 9 may 2020 [↑](#footnote-ref-18)
18. License Agreement, Clause (37.1) (37.5) [↑](#footnote-ref-19)
19. ‘Report on Internet Banking’ <https://www.rbi.org.in/SCRIPTs/PublicationReportDetails.aspx?UrlPage=&ID=243> accessed 11 May 2020 [↑](#footnote-ref-20)
20. ‘Why terrorists love the BlackBerry’ (August 24, 2010)

<https://news.rediff.com/slide-show/2010/aug/24/slide-show-1-why-terrorists-love-the-blackberry.htm>accessed 11 May 2020 [↑](#footnote-ref-21)
21. ‘RIM gives in, BlackBerry server to be located in India’ ( Aug 30, 2010)
<https://economictimes.indiatimes.com/tech/hardware/rim-gives-in-blackberry-server-to-be-located-in-india/articleshow/6462225.cms?utm\_source=contentofinterest&utm\_medium=text&utm\_campaign=cppst> accessed on 12 May 2020 [↑](#footnote-ref-22)
22. Justice K. S. Puttaswamy (Retd.) vs Union Of India And Others [2017] WP (C) 494/2012. [↑](#footnote-ref-23)
23. ‘THE PERSONAL DATA PROTECTION BILL, 2018’ <https://meity.gov.in/writereaddata/files/Personal\_Data\_Protection\_Bill,2018.pdf> accessed on 12 May 2020 [↑](#footnote-ref-24)
24. THE PERSONAL DATA PROTECTION BILL 2018 , s(3)(29) [↑](#footnote-ref-25)
25. ‘Encryption can secure the right to privacy’ , (the Hindu business line, 3 May 2019) <https://www.thehindubusinessline.com/opinion/encryption-can-secure-the-right-to-privacy/article27027075>accessed on  12 May 2020 [↑](#footnote-ref-26)
26. ‘WHATSAPP'S END-TO-END ENCRYPTION IS LEGAL IN INDIA, BUT NOT FOR LONG’ (12 April, 2016) <https://www.firstpost.com/tech/news-analysis/whatsapps-end-to-end-encryption-is-legal-in-india-but-not-for-long-3679985.html> accessed 13 May 2020 [↑](#footnote-ref-27)
27. ‘WhatsApp maintains its stand on govt's request for message traceability in India’ (19 June 2019) <https://www.indiatoday.in/technology/news/story/whatsapp-maintains-its-stand-on-govt-s-request-for-message-traceability-in-india-1551098-2019-06-18> accessed 13 May 2020 [↑](#footnote-ref-28)
28. ‘India's request to WhatsApp for message traceability could impact individual privacy’ (19 June 2019) <https://www.businesstoday.in/technology/news/india-request-whatsapp-message-traceability-end-to-end-encryption-privacy/story/357311.html> accessed 13 May 2020 [↑](#footnote-ref-29)
29. 'India wants to see your WhatsApp messages' <https://ia.acs.org.au/article/2020/india-wants-to-see-your-whatsapp-messages.html> accessed 13 May 2020 [↑](#footnote-ref-30)
30. ‘the International Encryption debate’ (12 June 2019) <https://www.lexology.com/library/detail.aspx?g=41bce78b-f790-4901-ba88-7b9f6ffdd488> accessed 18 May 2020 [↑](#footnote-ref-31)
31. ‘Lawful access & and encryption in Canada’ <https://commentary.canlii.org/w/canlii/2019CanLIIDocs2613#!fragment/zoupio-> accessed on 18 May 2020 [↑](#footnote-ref-32)
32. # ‘Online Privacy Law: Japan’ <https://www.loc.gov/law/help/online-privacy-law/2012/japan.php> accessed 18 May 2020

 [↑](#footnote-ref-33)
33. #  ‘Turkey’s Data Protection Law: Long-Awaited Legislation Finally Takes Effect’ (7 March 2017) <https://www.nortonrosefulbright.com/en/knowledge/publications> accessed on 18 May 2020

 [↑](#footnote-ref-34)
34. ### ‘World map of encryption laws and policies’ <https://www.gp-digital.org/world-map-of-encryption/>accessed 18 May 2020

 [↑](#footnote-ref-35)
35. #  ‘Government Access to Encrypted Communications: Taiwan’ <https://www.loc.gov/law/help/encrypted-communications/taiwan.php> accessed 18 May 2020

 [↑](#footnote-ref-36)
36. #  ‘Sweden's new digital surveillance law’ <https://www.thelocal.se/20200304/what-you-need-to-know-about-swedens-new-digital-surveillance-law> accessed 18 May 2020

 [↑](#footnote-ref-37)