RIGHT TO PRIVACY THROUGH CRYPTOGRAPHY & IT ACT 2000 IN PURVIEW OF NATIONAL SECURITY

Deepanshu Sharma & Pritanshu Shrivastava*

INTRODUCTION

The world in this millennium is techno-dependent for almost every aspect of life whether its payment of debts through credit card, entering into contracts by distant parties through online i.e. e-contracts, booking of railway or air tickets online and even social networking through orkut. The technology and communication revolution is at global plethora, as this revolution has crossed political boundaries, demolished economic barriers and proved effective in making up of cultural differences. Internet has spread its roots in even in those far flung areas so that individuals from different corners of the world can communicate freely and cost effectively. This has compelled the Governments in all over the world to review the laws and policies related to the information technology.

But with the technology advancing the traditional safe-locked documents are replaced by encryption/cryptographic techniques. The use of encryption is a practice of communication in which no third party can understand the matter being communicated without being permitted by the communicator themselves. Therefore this practice can be said to be legitimate use of right of private conversation and speech and expression without anyone's intrusion.

One of the most basic liberties of the individuals after right to life is right to freedom of speech and expression that has been granted in the Constitution probably of all democratic countries. The Indian Constitution also in Part III related to Fundamental Rights make speech, expression and communication as inalienable right of an individual. But as no right/liberty is absolute in any democratic country so some reasonable restrictions are being imposed on it. Article 19(1) (a) of the Indian Constitution guarantees to all citizens freedom of speech and expression, but Article 19(2) places restrictions on it for matters related to national security concerns. But this raises the question in minds of citizens that their right of privacy in context of communication is then violated as restriction on the right will entertain State intrusion. Right to privacy

* B.A., LL.B. (Hons.) – III Year, Gujarat National Law University, Gandhinagar

although not expressly mentioned in the list of fundamental rights but has been included as a subset of Art. 21 of Indian Constitution through judicial pronouncements. As Art. 21 can be taken away only by procedure established by law the same is with the right to privacy.

But as we all know with good there's always evil so this method of private conversation is vulnerable for use by the anti-social elements of the society for detriment of a nation to give shape to their illegal activities. Thus, restrictions on the practice must nevertheless be permissible and essential keeping in view the detrimental effects. Just the problem lies in justifying the restriction as one purely for public interest and not for keeping track of individuals' private lives without sufficient cause.

What is Encryption?

As the internet has emerged as one of the most effective and fastest medium of communication today it has also become sensitive to several problems like virus attacks, spoofing, hacking, etc. so it becomes essential for individuals to devise method for securing the matter in communication so that its not intercepted and used by others.

Encryption is a process of sending the information by one party to another party with a code-lock on the envelope and code for opening and locking only known to sender and the recipient thus ensuring total privacy even in an open network of internet eg. chat rooms, email accounts, etc. It involves use of secret codes and ciphers to communicate information online in a manner that person knowing the secret code and cipher can open and understand the information. As internet is being excessively used as business medium encryption helps in curbing electronic fraud and ensuring authenticity. Without encryption what people send via computers is the electronic equivalent of a postcard open to view by many people while the message is in transit. With encryption people could put both messages and money into electronic envelopes to secure the subject matter so that its not accessible to anyone except the intended recipient.[1]

Cryptography is the study of secret codes and ciphers and the innovations that occur in the field. Cryptography although seems essential to ensure privacy for communication but to the government it represents a legitimate security threat[2]. In USA National Security Agency (NSA) has the responsibility to maintain high expertise in cryptographic technology and to up-to-date their knowledge in the advancements made in the field

[1] Jonathan Rosenoer, 'Cryptography & Speech'<http://www.cyberlaw.com/cylaw1095.htm/> Last accessed on 21 December 2008

[2] Nandan Kamath , *Law Relating to Computers, Internet & E-Commerce*(3rd edn. Universal Publications, Delhi 2007) 285-286

not only domestic but also international; thereby protecting vital US government and military operations.[3] Not only in US, but also in India, the Indian Telegraphic Act, 1885 empowered the State to intercept the communication if there is a reasonable ground of security crisis and to safelock the vital State information from traitors. Thus, it seems that it sometimes become necessary to sacrifice a little of privacy for greater good.

The Politics of Right to Privacy

Privacy is defined in Black's Dictionary as the right of a person and the persons' property to be free from unwarranted public scrutiny and exposure. Privacy as a right has changed by leaps and bounds in recent times. The theory that an action may lie for the invasion of the right of privacy or as it has been said, the right to be let alone was propounded in 1890 by two American lawyers- Samuel D. Warren and Louis D. Brandeis.[4] Privacy has become the most fundamental and integral part of life of every individual and is utmost necessary for the well being of person in this democratic society. So, this means that the democratic countries believe that there exist public and private lives of an individual but the distinction has become blurred. Recent inventions and business methods like e-commerce call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right to be let alone.[5] Thus, we can say that privacy includes right over one's personal information as well as ability to determine how that information must be used. But as the activities sometime done in private sphere has a detrimental effect on public interest, right to privacy has become a subject of controversy. Encryption of personal information although assure privacy and gives a psychological sense of security to the person who is transmitting personal information on internet but at same encryption barges into security concerns as to political, social and economic health of the nation.

The International Convention on Civil and Political Rights,1966 in its Art. 17 (1) no one must be subjected to arbitrary unlawful interference with the family, home or correspondence, or to the unlawful attack on his honor and reputation; and (2) everyone has a right to protection against such interference of attacks.[6]

---

[3] *Daniel Bernstein v. United States Dept. of State*, 922 F.Supp. 1426 (N.t). Cal. 1996).

[4] Vernon X Miller,*Selected Essays on Torts*(Vantage Press, USA 1978) 122.

[5] Dr. Nehaluddin Ahmad, 'Privacy and the Indian Constitution: A Case Study of Encryption' <http://www.ibima.org/pub/journals/CIBIMA/volume7/> Last accessed on 23 December 2009

[6] International Convention on Civil and Political Rights,1966 (adopted 16 December 1966, entered into force 23 March 1976) art. 17 (1)

European Convention on Human Rights: Article 8

(1) everyone has a right to respect for his private and family life, his home and his correspondence; and

(2) there must be no interference by a public authority with the exercise of this right, except such as is in accordance with the law and is necessary in democratic society in the interest of the nation 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.[7]

Universal declaration of Human Rights, 1948: Article 12- no one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attack upon his honor and reputation. Everyone has the right to protection of the law against such interference or attack[8]

Besides the above international principles adopted by different countries the *Organisation for Economic Co-operation and Development* has done a commendable job in formulating guidelines to examine the extent of right to privacy, these guidelines popularly called as *Guidelines Governing The Protection Of Privacy & Transborder Flows Of Personal Data*, the summed up guidelines are as follows:

Firstly, collection of personal data should be done with the consent of the person and lawfully. Secondly, data collected should be related to the subject under investigation. Thirdly, the objective of collecting personal data should be specified.

Fourthly, data should not be further used without sanction of the law.

Fifthly, security safeguards must be there to prevent leakage of data to unauthorised persons and

Lastly, An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him

[7] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) Article 8

[8] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR) art 12

1. within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

A data controller should be accountable for complying with measures which give effect to the principles stated above.[9]

But instead of such provisions mentioned above, there are many instances of violation of right to confidentiality, like in San Jose, in the US, it is claimed police officers have sold information on individuals obtained from the mammoth Criminal Justice Information System for $25 per report [Mercury News 1993].The situation is little better outside the US

Indian Constitution: Green Flag to Right to Privacy

With the growth of public snivel for justice, the Indian Judiciary has rose to the occasion to give a relief to people knocking its door for justice. Henceforth, there has been emerging trend of judicial activism due to which the Hon'ble judges through judicial pronouncements have included series of unexpressed rights in the catalogue of expressed fundamental rights. These unexpressed rights have same weightage and same force of enforcement as the expressed ones as according to the Judges' opinion the former are so entwined with the latter that the expressed rights that is guaranteed by the Indian Constitution would be hollow and vague without the unexpressed ones, eg. in cases like *Olga Tellis* v. *Bombay Municipal Corp.*[10] the Supreme Court held that Article 21 of the Constitution includes right to shelter which is not expressly provided in the Constitution and in *Unnikrishnan* v. *State of Andhra Pradesh*[11] the Supreme Court held that Art. 21 also includes right to education too.

As the right to education and shelter being the unexpressed rights are now included under the roof of Article 21, the status of right to privacy in the same way can be ascertained by the significant judicial pronouncements & case-laws/precedents. Indian

[9] Directorate of Science & Technology OECD, 'OECD Guidelines on Protection of Privacy & Transborder Flow of Personal Data' <http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html/> Last accessed on 2 January 2010

[10] AIR 1986 SC 180

[11] (1993) 1 SCC 706

Constitution has not yet granted but only reasoned this right. The forerunning case in regard to right of privacy being a fundamental one is *Kharak Singh* v. *State of Uttar Pradesh*[12]. The question was whether Right to Privacy might be implied from existing Fundamental Rights in the Constitution of India, 1950, Articles 19(1)(d), 19(1)(a) and 21. Majority opinion was that our Constitution does not in express terms confer any such right on the citizens. Minority opinion (SUBBA RAO J.) was in favour of inferring right to privacy from right to personal liberty under the Constitution of India, 1950, Article 21. This right again came for examination before the Supreme Court of India in *Govind* v *State of Madhya Pradesh*[13], and this time Supreme Court took a more elaborate view and accepted a limited right to privacy as an emanation from Articles 19 (1)(a), 19 (1)(d) and 21. It was also said that the right is not absolute. So, reasonable restrictions may be imposed on this right. These restrictions must be the same as are provided under the Constitution of India, 1950, Article 19(2). It was also held that the right could be done away with in compliance to 'procedure established by law' as mentioned in Article 21.

A historic judgment in the arena is probably the case of *People's Union for Civil Liberty (P.U.C.L.)* v. *Union of India*[14] popularly known as *"Phone-Tapping case"* where the Hon'ble Supreme Court has held telephone tapping as a grave invasion of an individual's right to privacy which is a part of the right of life and liberty enshrined under Article 21 of the Indian Constitution. This case has comportment on the issue of this paper as in this case also there was argument whether right to privacy is paramount to national security or not? In this case popular political personalities complained of unauthorized phone-tapping. Thus, a writ petition was filed by P.U.C.L. highlighting the incidents of telephone-tapping in recent years & also in wake of the report on tapping of politicians phones by the Central Bureau of Investigation (CBI).

The other issue which arose with the misuse of State's discretion in exercise of the powers vested in it under Section 5(2) of Indian Telegraph Act, 1885. Hence, the petitioners also challenged the constitutional validity of the Section 5(2) of the Indian Telegraph Act since it allowed the State authorities to intercept messages as they felt might be necessary in the interests of national sovereignty, integrity, security, friendly relations with the foreign States, public order or to prevent incitement to commit an offence. The Supreme Court therefore taking a futurist view of the problem stated "...in absence of just and fair procedure for regulating the exercise of power by the State authorities under Section 5(2) of the Indian Telegraph Act,1885 it may not be possible to safeguard the rights of citizens guaranteed under Arts. 19(1)(a) & 21. The court hope

[12] AIR 1963 SC 1295

[13] (1975) SCC (Cri) 468

[14] AIR 1997 SC 568

that the guidelines framed by it to regulate the discretion vested in the State under Section 5(2) of Indian Telegraph Act for purpose of phone-tapping & interception of message will be strictly followed by the State authorities so as to safeguard public interest from arbitrary & unlawful exercise of power by the Government."

The case is important from the count that as the terms mentioned in the Section 5(2) of Indian Telegraph Act such as public safety including national security & public emergency are so broad that they could be interpreted in either way by the Executive, therefore the Supreme Court to narrow down the ambit of the terms said "public emergency & public safety are sine qua non under provisions of Section 5(2)of Indian Telegraph Act. Public emergency would mean the prevalence of sudden condition or state-of-affairs affecting people at large calling for immediate action. The term public-emergency/-safety should not include more ambiguous areas such as economic emergencies, etc." Thus when either of these two conditions are not in existence the Central or State Government or the authorised officers cannot resort to telephone tapping or interception of messages even though there is satisfaction that it is expedient in interest of national security or integrity of the country.

The Court has also laid down the following procedural safeguards for the exercise of power under Section 5(2) of the Indian Telegraph Act-

1. An order for telephone tapping can be issued only by Home Secretary of Central or State Government.
2. The copy of order must be sent to a Review Committee within one week of the passing of the order.
3. the order shall unless renewed, cease to have effect at the end of two months from the date of issue.
4. Only such information ought to be collected & retained as is pertinent to the issue at hand.
5. Records of the intercepted message should be made for accountability.
6. If on investigation the Review Committee concludes that there has been a contravention of the provisions of section 5(2) of the Act, shall set aside the order.
7. Review Committee may also direct destruction of the intercepted information.

The aforementioned judgments delivered by the Divisional Bench comprising of Justice Kuldip Singh and Justice Ahmad took a broad overview in protection and development of right to privacy as a constitutional right in India, but permitted wire-tapping in rarest of the rare circumstances as right to speech and expression under Article 19(1)

(a) of the Constitution can be reasonably restricted on the grounds mentioned in Article 19 (2) and so on the same grounds telephonic or telegraphic conversation can be too restricted.

As it is evident from analysing the constitutional position of right to privacy in India the right must be subservient to the national interest, national security and public safety at all times.

But the Court also agrees that with advent of highly sophisticated communication technology the right to hold telephone conversation in the privacy at one's home or office without interference is increasingly susceptible to abuse.

Henceforth from the discussion above, we can agree on the point that we are primarily concerned with the use of non-recoverable encryption by persons engaged in illegal activity as right to encryption is also subset of right to privacy and if encryption is allowed it may result in complete privacy and thus, a problem for national authorities to examine record of one's activities which may prove a hanging sword onto public safety.

Also, Section 72 of IT Act 2000 provides punishment for breach of confidentiality and privacy by accessing to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

The Information Technology Act 2000 & Restrictions on Cryptography

As the there is a technology lag in India, the concept of encryption/cryptography is not much known. That is also evident from the fact that India got its IT Act 2000 because the United Nations General Assembly on 30 January 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. This is referred to as the UNCITRAL Model Law on E-Commerce. Following the UN Resolution India passed the Information Technology Act 2000 in May 2000 and notified it for effectiveness on October 17, 2000.[15]

The Act takes into consideration the system of 'key-pair encryption' for the recording and authentication of digital signatures. The Act provides specifically, that the public key is to be deposited with a Certifying Authority.

[15] < http://en.wikipedia.org/wiki/Information_Technology_Act > Last accessed on 12 January 2010

Section 69 empowers the Central Government/State Government/ its authorized agency to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource if it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence or for investigation of any offence. Thus, in the absence of any co-operation from the subscriber, even the controller cannot directly intercept and decrypt a message, since he is only a repository of the public keys and not of the private keys necessary for the process of decryption. Non-cooperation with the authority is made punishable under the section. Thus, it is only through the process of coercion that the controller can actually decrypt and decipher encrypted messages. Since the controller cannot directly decrypt messages, the right to privacy is still protected to a large extent.

It will be seen that complete discretion is vested with the controller to determine whether a condition has arisen where a transmission may be intercepted in the interests of national security. The right to an encrypted transmission may be viewed as integral to the right to privacy flowing from Article 21 of the Constitution. In such a case, the right can only be curbed by a "...procedure established by law." It is now well settled that such a procedure must be right, just, fair and reasonable to be valid. The question, which necessarily arises, is whether the procedure under section 69 is sufficient to thwart the right to privacy.

Further, considering the fact that the section also provides for punishment in the event of non-compliance, it is imperative that stronger safeguards be built into the system. Thus, the question as to what constitutes a security threat or when the friendly relations are being threatened should not be left to the sole discretion of the controller, but must emanate from the legislature. In the alternative, the controller should frame specific regulations under Section 89, laying down specific criteria as to when the security of the nation is being threatened and the like. In the absence of such measures, the provision in section 69 can be said to be an infringement of the right to privacy in Article 21 and, consequently, unconstitutional and void *ab initio*.

CONCLUSION

The practice of encryption and its study (cryptography) provides individuals with means of communication that no third party can understand unless specifically permitted by the communicators themselves. It would therefore seem that this practice is a legitimate utilization of the right to freedom of speech and expression and the right to have a private conversation without intrusion.

Nevertheless, this could carry on surreptitious operations to the detriment of national security. Some restrictions on the practice therefore are not only permissible but necessary in the interests of national security. The problem, however, is ensuring that the restriction is justifiable and exclusively for the benefit of the nation, the state not being allowed to interfere and keep a track on individuals' activities and private lives without sufficient cause.

One cannot deny that there will arise exceptional circumstances when transmissions need to be intercepted to prevent anti-national activities. But, such circumstances cannot be abused to further political vendetta. On a plain reading of Section 69, it may be concluded that the procedure is not adequate as it leaves complete discretion in the hands of the controller.

Privacy has become the most vital part of life of every individual in this democratic society. A possible solution may lie in the very technology that encryption uses. The problem has to be looked at, at a two-fold level. At one level cryptography should be dealt as any ordinary publication and restraints on the same should be allowed only in so far as Article 19(2) permits them. On the other level the issue of privacy and the deprivation of the same by a procedure established by law, the answer lies in a strong and comprehensive set of safeguards to ensure that state interference is permitted only when absolutely essential.

Even if an interception is to take place, the same will have to be done with certain specific guidelines. Detailed records and copies of the intercepted messages should be kept and destroyed once the proclamation is no longer in force. The cryptographic keys obtained should be similarly deleted from government resources to ensure that authorities can no longer use them to intercept messages, in the absence of any emergency. Another alternative might be the process of prior judicial permission, before the actual passing of the order. However, this approach has several practical problems and may not be appropriate, when action needs to be taken immediately.

While it is true that no procedure is completely infallible, avoid any breach of their privacy. Maybe the aforesaid guidelines may become threshold point of balance of use of encryption, privacy and saving national interests.