Privacy and the Indian Constitution: A Case Study of Encryption

Dr..Nehaluddin Ahmad

MA, LL.B., LL.M.(Lucknow India)LL.M.(Strathclyde,UK.)LL.D. (Meerut India)
Senior Lecturer, Faculty of Business and Law, Multimedia University,
Jalan Ayer Keroh Lama,75450 Melaka, Malaysia
E-mail: ahmadnehal@yahoo.com

Abstract

The growth of telecommunication and electronic commerce has led to a growing commercial market for digital encryption technologies. Business need encryption to protect and to establish secure links with their customer .Law enforcement needs it to stop those under investigation from intercepting police communications. Individuals need it to protect their private communication.

Such technology is, liable to be misused by individuals. The problem, however, is ensuring that the restriction is legitimate and solely for in the interests of national security, the state not being allowed to interfere and keep a track on individuals' activities" and private lives without sufficient cause. Governmental regulation of cryptographic security techniques endangers personal privacy. Encryption ensures the confidentiality of personal records. In a networked environment, such information is increasingly at risk of being misused. The entire issue, at its simplest level, boils down to a form of balancing of interests.

The specific legal and rights-related problems arising from the issue of cryptography and privacy in the Indian context are examined in this paper.

Introduction

Emerging computer and communications technologies have radically altered the ways in which we communicate and exchange information. Along with the speed, efficiency, and cost-saving benefits of the digital revolution come new challenges to the security and privacy of communications and information traversing the global communications infrastructure.

In response to these challenges, the security mechanisms of traditional paper-based communications media envelopes and locked filing cabinets are being replaced by cryptographic security techniques. Through the use of cryptography, communication and information stored and transmitted by computers can be protected against interception to a very high degree.

In this electronic environment, the need for privacy-enhancing technologies is apparent. Communications applications such as electronic mail and electronic fund transfers require secure means of encryption and authentication features that can only be provided if cryptographic know-how is widely available and unencumbered by government regulation. Governmental regulation of cryptographic security techniques endangers personal privacy[1]. Encryption ensures the confidentiality of personal records, such as medical information, personal financial data, and electronic mail.

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 utilisation of the right to freedom of speech and expression and the right to have a private conversation without intrusion[2].

The privacy of communication is explicitly protected by Article 12 of the Universal Declaration of Human Rights, Article 17 of the International Covenant on Civil and Political Rights, and national law[3].
In some developing countries the state-owned telecommunications companies were active participants in helping the security services monitor political activist /human rights advocates. These problems are not limited to developing countries. The French Commission Nationale de Contrôle des Interceptions de Securité estimated that there are some 100,000 illegal taps conducted each year in France[4]. There have been numerous cases in the

[1] Theodore F. Claypoole:- "Privacy Regulations a Concern with Internet" LexisNexis Martindale-Hubbell (R)Legal Articles (June 27, 2004)
[2] Privacy International :-" Responding toTerrorism" PHR 2005; Available online:- http://www.privacyinternational.org/article.shtml?cmd[347]=x-347 - [Visited on 10 Aug.2008]
[3] Universal Declaration of Human Rights Available online:- http://www.un.org/Overview/rights.html [Visited on 10 Aug. 2008]
[4] Jack Nelson, "FBI Warns Companies to Beware of Espionage." The International Herald Tribune.13 January 1998; Paris.

United Kingdom which revealed that the British intelligence services monitor social activists, labor unions and civil liberties organizations. In Germany, wiretapping stature adopted 1998 that allows[5], for the first time since the Nazi era, the ability to bug journalists' offices. The European Parliament issued a report in January 1998 revealing that the U.S. National Security Agency was conducting massive monitoring of European communications[6]. US House passes a surveillance law that allows the government to spy on foreign telephone calls and electronic correspondence without court permission[7].

Many human rights groups currently use encryption (cryptographic techniques) to protect their files and communications from seizure and interception by the governments they monitor for abuses.

Such technology is, however, liable to be misused by individuals, to carry on clandestine 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 legitimate and solely for in the interests of national security, the state not being allowed to interfere and keep a track on individuals' activities" and private lives without sufficient cause[8]. Governmental regulation of cryptographic security techniques endangers personal privacy. Encryption ensures the confidentiality of personal records, such as medical information, personal financial data, and electronic mail. In a networked environment, such information is increasingly at risk of being stolen or misused.

Uses of Encryption

The phenomenal growth of the Internet has brought encryption issues to the forefront. It is generally accepted and agreed that e- commerce on the internet is unlikely to take off until there is widely available secure encryption. This is particularly important for monetary transactions, but rights owners are also looking at encryption as a way of distributing their copyright works for payments over the internet without risking widespread unlicensed copying[9]. On the other hand, governments are fearful that such encryption would put a powerful weapon into the hands of terrorists and other criminals, and would make the job of law enforcement much more difficult. These issues have been widely discussed, in the US, and the US government has given up trying to prevent the export of strong encryption and to gain ready access to encrypted communications by means of a proposed compulsory scheme of escrowing keys[10]. Encryption has also been under discussion by various European governments.

Advantages of Encryption

The various advantages of encryption are[11]:

1. Encryption can protect information stored on the computer from unauthorized access even from people who otherwise have access to your computer system.
2. Encryption can protect information while it is in transit from one computer system to another.
3. Encryption can be used to verify another of a document[12].
4. Encryption can be used to deter and detect accidental or international alteration in data.

Limitations of Encryption

The various disadvantages of encryption are[13]:

1. Encryption cannot prevent an attacker from deleting the data together.
2. The attacker can compromise the encryption programme itself. The attacker might modify the programme to use a key different from one provided or might record all of the encryption keys in a special file for later retrieval.

Encryption and Cryptography: Modes of communication

Before actually proceeding to understand the legal complexities involved in the issues of encryption and cryptography, it is essential to have at least a cursory understanding of what they encompass and involve.

The most reliable means is through cryptography i.e. encryption and decryption techniques. The most popular and useful method of encryption for general messaging is public key cryptography. i.e.

---

[5]The Constitutional Court (Bundesverfassungsgericht) in Karlsruhe(March 3, 2004) declared Major parts of CS - Bonn the new wiretapping statute is unconstitutional. The German American Law Journal, American Edition 11 March 2004

[6] Encryption in the Service of Human Rights,"Human Rights Watch http://www.aaas.org/SPP/DSPP/CSTC/ briefings/crypto/dinah.html [Visited on 8 Aug.. 2008]

[7] BBC NEWS, Saturday, 15 March 2008 US House passes surveillance law http://news.bbc.co.uk/2/hi/americas/7297865.stm [Visited on 8 Aug. 2008]

[8] Mohammed, E (1999), An Examination of Surveillance Technology and Their Implications for Privacy and Related Issues - The Philosophical Legal Perspective, The Journal of Information, Law and Technology, (JILT) 1999 (2) < http://elj.warwick.ac.uk/jilt/99-2/mohammed.html[Visited on 8 Aug 2008]

[9] ibid

[10] Karen Coyle, Digital Signatures: Identity in Cyberspac *AALL Spectrum*, v.2, n.4,December, 1997.p8-10.

11 *Anoop MS (2007). Public key Cryptography - Applications Algorithms and Mathematical Explanations.* India*:* Tata Elxsi. P.67-68

[12] *Ibid*

[13] *N. Ferguson; B. Schneier (2003).* Practical Cryptography. Wiley *,p 7*

encryption and decryption techniques involve the use of two kinds of keys, public keys and private keys, both of which are mathematically linked. One key is used for encryption and other corresponding key is used for decryption. Each user has a pair of keys, of which the private key is kept secret and the public key is open to all[14]. Thus if X wants to send a message to Y, X will encrypt the message with Y's public key and send it to Y. The message can only be decrypted using Y's private key, which is a secret and only known to Y. Thus, only Y would be able to access the message[15].

To put it very simply, the process of encryption is like sending a postal mail to another party with a code-lock on the envelope, the code for which is known only to the sender and the recipient. This, therefore, has the effect of ensuring total privacy even in an open network like the Internet. Encryption involves the use of secret codes and ciphers to communicate information electronically from one person to another, in such a way that only the persons so communicating know to use the codes and cipher[16] .The field of cryptography on the other hand, deals with the study of secret codes and ciphers and the innovations that occur in the field. It is also defined by some as the ". . .art and science of keeping messages secure[17].", Thus, while encryption is the actual process, cryptography involves a study of the same and is of a wider connotation.

The analogy between the practice of encryption and that of posting a message by a secure envelope may not be totally irrelevant[18] .With the emergence of the Internet as the fastest and most effective medium of communication today, it is but essential that messages transmitted are not intercepted and used by others. It is basically for this reason that encryption assumes great importance. Further, with the excessive growth of the Internet as a business medium, such practices would also go a long way in curbing electronic fraud and ensuring authenticity[19]. Thus, the primary purpose of encryption and cryptography remains: ensuring that messages transmitted remain secure from interference by third parties.

These subjects have has their origin centuries ago, in the crudest of forms. In the context of the USA, its importance was seen as a tool of espionage, during the Cold War era. Even during those times, encryption was not a tool ordinarily used by individual citizens. It remained in the exclusive domains of the military and the intelligence services. Since then, cryptography has progressed in leaps and bounds and today is an instrument known, if not used, by a large number of individuals communicating electronically. Its importance emerged with the advent of the Internet and the boundaries for communication that were thrown open[20].

In India at present, there is no law regulating encryption. According to the Department of Electronics of the Government of India, the cryptography situation in India largely remains in

[14] , Stephen Levy, "Crypto Rebels", at < http://www.eff.org/pub/Privacy/crypto_rebels.article >.[Visited on 10 Aug.2008]

[15] By reversing the process, digital signature can be produced

[16] "Encryption basically involves running a readable message known as "pláintext" through a computer programme that translates the message according to an equation or algorithm into unreadable 'ciphertext". See, *Daniel Bernstein v. United States Dept. of State,* 922 F. Supp. 1426 (N.t). Cal. 1996).

[17] Jonathan Rosenoer, "Cryptography & Speech", at < http://www.cyberlaw.com/cylwl095.html . [Visited on 10 Aug. 2008]

[18] Id. " Without cryptography, 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 cryptography, people can put both messages and money into electronic 'envelopes,' secure in the knowledge that what they send is not accessible to anyone except the intended recipient."

[19] This is by means of digital signatures

[20] The development of cryptography is attributed largely to the work of individuals in the 70s and 80s. An important contribution came from a person called Whitfield Diffie in 1971. Till then, all forms of cryptography were known only to the United States' National Security Agency (NSA). Individuals very rarely even knew what it was about. In this period, appeared a famous book by David Kahn, known as The Code breakers (1967), where the author spoke about the techniques of creating encrypted messages. Diffie was a computer expert from Massachusetts. In the 1970s with the development of the Arpanet, the predecessor to the Internet, he decided to carry out some experiments in cryptography there.
To Diffie, the greatest problem with existent means of cryptography that existed was that secure information was being transmitted through insecure channels. This meant that coded though a message may be, it could still be intercepted by third parties. In 1975, he developed a revolutionary means of cryptography, called the public-key cryptography. This system envisaged the use of keys, called the public key and a private key. A public key was a key held by an individual but accessible to all individuals. Thus, if a person wanted to send information to another, he would encrypt the message using that person's public key, with his permission and send the message to him. The message, however, could be decrypted only by the specific recipient using his private key. This is only a simplistic explanation. See, Stephen Levy, "Crypto Rebels", at < http://www.eff.org/pub/Privacy/crypto_rebels.article >.[Visited on 8 Aug.2008]

the development stage[21].Although the government has not made any effort to define encryption in the Indian IT Act2000, but technically it clearly says that it is not allowed[22].The Department of Telecommunication ("DoT") controls all aspects regarding Telecommunications[23], including encryption. As of today, permission is required from the DoT to send encrypted messages. DoT has, while giving licenses to ISPs, permitted individuals or organizations to deploy indigenous or imported encryption equipment for providing secrecy in transmission up to a level of encryption to be specified[24]. However, if encryption equipment of levels higher than those specified is to be deployed, individuals /groups / organizations should obtain Government clearance and shall deposit one set of keys with the authority, which the government will specify.

While cryptography may be looked at as essential to ensure privacy for communication, to the government it represents a legitimate security threat'[25].Any state agency in India, is given the power to intercept communication if a security crisis were to occur, so as to ensure that vital information regarding the nation is kept away from those involved in activities prejudicial to the state's security[26]. Cryptography, if used to code messages containing such vital information, would be undecipherable to the government. As a result, the only solution seems to lie in maintaining a state monopoly over the entire process of encryption.
Indian Information Technology Act 2000 would require all Internet Service Providers to monitor all traffic passing through their servers, making traffic, including the plain text of encrypted traffic, available to "properly constituted authorities" for "valid reasons of security." Properly constituted authorities include the Central Bureau of Investigation (CBI), the Intelligence Bureau (IB) and the Research and Analysis Wing (RAW).

The resultant problem is about ensuring a balance between the two. On the one hand, it cannot be denied that as a tool to ensure privacy in communication, especially digital communication, cryptography is essential. On the other hand, to completely negate national security concerns could prove disastrous if the concern is legitimate. Thus, it may be essential to sacrifice some amount of personal liberty for the greater good of the entire nation.

Privacy and the Indian Constitution

The last few decades have seen the growth of the belief that the Indian Constitution contains rights other than those expressly mentioned in its content. These rights could be called unenumerated rights. The rationale behind this formulation is simply that the enumerated right would be meaningless without providing for certain other rights by implication. An example may serve to show the point**:** while freedom of the Press has nowhere been expressly provided for in the Constitution it continues to have a very definite presence by virtue of the fact that it constitutes an indispensable part of Article 19(1)(a) which guarantees the right to freedom of speech and expression in India.[27] It is in this context that the question of a right to privacy arises. The scope of such an unenumerated right would be broad since there are a number of Constitutional provisions where the right to privacy would play a significant role. Thus, there would be scope for such a right in Article 21[28], in Article 19(1(a)[29] as well as in Article 19(1)(d)[30]. Since the exact position of the right to privacy with respect to enumerated rights appears to be somewhat vague. It is evident that case law and judicial pronouncements play a significant role in determining the status of the right.

The first important case dealing with the right to privacy is undoubtedly that of Kharak Singh v.

[21] Information Technology Group Dept. of Electronics Govt. of India <http://www.allindia.com/gov/doe/cryplaw.htm#index>.[Visited on 8 Aug.2008]
[22] Pawan Duggal(cyber law expert)by Urvashi Kaul ,Asian Age(Int.Daily) ,N.Delhi August 11 ,2005
[23] Under Section 4 of Indian Telegraph Act, 1885
[24] Gulshan Rai, R.K.Dubash, and A.K.Chakravarti, "Cryptography Technology and Policy Directions in the Context of NII," Version 1, Cyber law Series 3, December 1997,
[25] One of NSA's primary responsibilities in this arena is to provide the means of protecting vital US government and military communications and information systems of a classified nature. NSA maintains a high degree of expertise in cryptographic technology and keeps abreast of advancements, domestically and abroad, in order to better protect vital government communications." This was a statement issued by USA's National Security Agency, regarding the need to maintain a government monopoly over cryptography.
[26] For instance, in India, under the Telegraph Act, 1885, the state is allowed to intercept information under certain specific conditions.

[27] This has been confirmed in cases such as *Bennelt Coleman v. Union of India,* AIR 1973 SC 106 and *Virendra v. State of Punjab*, AIR 1958 SC 986
[28] Indian constitution Article 21 states that "No person shall be deprived of his life or personal liberty except according to procedure established by law."
[29]Indian constitution Article 19(1)(a) states that "All citizens shall have the right to freedom of speech and expression".
[30] Article 19(1(d) states that " All citizens shall have the right to move freely through the territory of India".

State of Uttar Pradesh[31]. In holding that Regulation 236(b) of the Uttar Pradesh Police Regulations was invalid, k the Court clearly indicated that there did exist a right to privacy within the scope of Article 21. In delivering it's judgment, the Court was influenced by two American decisions in particular. The first of these was the case of Munn v. Illinois[32], which laid down the blanket proposition that the right to life consists of much more than the right to continue a mere animal existence. This decision has been the fount for including various unenumerated rights within the scope of article 21. The second decision was more directly on the point. This was the case of Wolfe v. Colorado[33] where Frankfurter, J., delivered a judgment which set the trend as far as the right to privacy was concerned. The Court also took into account an earlier English judgment, Semayne's case[34], which guaranteed the inviolability of a person's home and held that a person had a right to privacy**.**

It must also be mentioned that neither of these judgments denied the fact that violations of privacy may be possible under the sanction of the law. This fact assumes importance in the later case of Gobind v. State of M.P[35], where the Court reaffirmed that there did exist a right to privacy under the Indian phrase "procedure established by law" as mentioned under Article 21. The Indian Supreme Court did not take into account the fact that the procedure established by law in India might be unjust or unreasonable, a probability which was examined and covered by the United States Supreme Court by referring to the "Due Process of Law" clause. However, post-Menka Gandhi v. Union of India[36], it has been held that there is not substantial difference between the phrases "procedure established by law" as under the Indian Constitution and the phrase "due process of law" as under the United States Constitution.. Thus, in today's context it would not be enough to say that a violation of privacy would be justified by law; it must further be shown that he law under which the violation has taken place is just, fair and reasonable.

A landmark development in this regard would be the case of P.U.C.L. v. Union of India[37], where the issue of "telephone tapping" of several well known personalities connected with the field of politics was examined. The facts of this case have been examined in some detail since they have a direct bearing upon the issue of Internet privacy versus national security.

Section 5(2) of the Indian Telegraph Act was challenged since it allowed the concerned authorities to intercept such mail as they felt might be necessary in the interests of national sovereignty, integrity, security, relations with foreign offence. The judgment delivered by Kuldip Singh, J., took a broad overview of the development of the right to privacy as a constitutional right in India and held that telephone tapping was definitely a move against privacy and, therefore, ought not to be permitted except in the gravest of grave circumstances such as a public emergency.

The case is important on two counts: Firstly, terms such as national security and integrity are very broad and may be interpreted to suit the purposes of the executive. Keeping this in mind, the Court held that the term "public emergency" refers to a very definite category of happenings and as such should not be misconstrued so as to cater to private or personal agendas. The Court also mentioned that the term could be discerned in terms of the Telegraph Act and to that extent it referred to a very definite set of events. The Court also made it clear that it should not be extended to include more ambiguous areas such as economic emergencies. The term "public safety", according to the Court referred to a specific time when the state or condition of freedom of danger or risk to the public prevailed. Therefore, the right to privacy could not and should not be invaded until a public emergency had taken place or public safety was threatened.

The P.U.C.L. case is also relevant inasmuch as it sets down the guidelines for a general invasion of

[31] AIR 1963 SC 1295,. In this case, the appellant, who had served time in jail was being continually harassed by police visits under Regulation 236(b) of the U.P. Police Regulations which permitted for "domiciliary visits at night".

[32] 94 US 113 which has been used in justifying a number of cases on matters such as the right to shelter in *Olga Tellis v. Bombay Corpn*., AIR 1986 SC 180, and the right to education in *Unnikrishnan v. State of A.P*., (1993) 1 SCC 706.

[33] 338 US 25. Justice Frankfurter's judgment clearly says "The security of one's privacy against arbitrary intrusion by the police is a basic of free society.", thus indicating his position on the right to privacy.

[34] (1604) 5 Co Rep 91.

[35] (1975) SCC (Cri) 468. The facts in this case were also relating to surveillance according to Regulations 855 and 856 of the Madhya Pradesh Police Regulations. However the court held that although the right to privacy existed, it had not been violated since the procedure was as required by law.

[36] AIR 1978 SC 597.

[37] (1997) 1 SCC 318.

privacy as well as for specified invasions of privacy. While in the case of a specific invasion, only a particular person or group of persons would be targeted, in the case of a general invasion every citizen would risk a loss of his right to privacy. It is primarily in the case of a general invasion that the P.U.C.L guidelines, as to first establishing the fact that there exists a state of "public emergency", becomes relevant. On the other hand, in the case of a specific invasion, it may not be necessary to establish the existence of a "public emergency" in order to justify a violation of privacy. It would be sufficient to say that a specific breach of peace may occur necessitating the violation of the right to privacy. However, even in such a case, the procedure laid down in P.U.C.L. would have to be complied with.

It is evident, from a detailed examination of the Constitutional position and the history of the right to privacy in India that the right must be made subservient to the national interest and national security at all times. It is also important to note that the formulation of safeguards by Justice Kuldip Singh in the P.U.C.L case is remarkably similar to the safeguards devised by the OECD. There is however, one important exception. The OECD guidelines make it clear that the person who is the subject of the investigation should be consulted before any kind of action is taken[38]. This position has been rejected in P.U.C.L. since it may result in rendering the idea of surveillance or information gathering useless. It may be mentioned that in certain cases, the matter could be referred to the judiciary for prior review.

Do citizens have a right to encrypt data pertaining to their transactions on the Internet so as to prevent it from falling into the wrong hands? If the right to encryption is allowed it may indeed result in complete privacy for the individual on the Internet[39] but it would simultaneously mean that national authorities would not be able to examine the record of one's dealings on the Internet.

The point of the entire issue on constitutionality until now has been that we do have the right to privacy but that right is necessarily subservient to the national interest. Going by the strict terms of the P.U.C.L. case, it clear that what constitutes national interest is, as yet, not very clear. For example, if an Internet equivalent of the securities scam were to take place, the government may still be unable to invade one's privacy simply by virtue of the fact that an intended by the P.U.C.L. case.

The Constitutional position is that Article 19(2) imposes the restrictions upon the freedom of speech conferred by Article 19(1)(a) but since the right to privacy has been held to be largely under Article 21, it is subject only to "procedure established by law". This term may actually encompass more possibilities than have been intended by Article 19(2) but if one were to extend provisions such as those of the Telegraph Act to the Internet scenario it is clear that the effect would be to have restrictions similar to those imposed by Article 19(1(a). That this extension is possible may be shown by the Japanese position where consumer protection is governed by the Law Concerning Door-to-Door Sales (Direct Sales Law) enacted in 1976. This law continues to govern sales made over the net. The moral of the story is that existing laws can occasionally cover the cyber age, if properly used.

Privacy under the Indian Information Technology Act, 2000

At the time of legislating on cyber laws, India's Parliament seems to have largely neglected the issue of privacy of personally identifiable information. There in only a single provision dealing with this and that provision is very limited in its scope.

Section 72 of the Act, establishing an Information Technology Offence of "Breach of Confidentiality and Privacy" reads as under:

"72. Breath of confidentiality and privacy.—Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made there under, has secured access 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."

It will be noted that this provision deals only with information collected by a person who secures the information in pursuance of powers that he or she exercises under the Act. It punishes with imprisonment or fine or both the disclosure of such information to third parties without the consent of

[38] OECD Assaults Individual Privacy in the Name of World Government (Brief Article) Insight on the News, May 21, 2001, by Paul Craig Roberts http://www.findarticles.com/cf_dls/m1571/19_17/75021648/p1/article.jhtml[Visited on 8 Aug.2008]

[39] Brin, David(.1998) The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom? (Reading, MA: Addison-Wesley, 1998).

the person who the information relates to. This provision would, therefore, be extremely narrow in its application, being relevant only to offences by authorities such as Adjudicating Officers, the members of the CRAT or Certifying Authorities under the Act.

It is apparent that the larger issue of online privacy has remained ('completely outside the scope of the legislation. There seems to be no particular authority concerned with understanding the importance of the issue and bringing in regulations to curb unscrupulous use of personal information. It is not even as if a self-regulatory model for online business is in place and legislation is not required.
It is important that legislators understand that the protection of personally identifiable information is vital if one seeks to foster a secure and trustworthy electronic environment the avowed purpose of the IT Act. This is one void in law and policy that just cannot be ignored.

Restrictions on Cryptography in India and Information Technology Act, 2000
The use of cryptography and encryption in India is a relatively new phenomenon. The use of technology in itself, for the purposes of communication, has begun only over the last 15-20 years in India. The use of the Internet is a phenomenon of the mid-90s.

According to a report[40], in India, there are very few companies involved in the development of tools for cryptography. Further, cryptography remains, by and large, within the domain of the defence sector. It was only as late as 1995 that India introduced a list of items that required licensing before export. The list only included encryption software for telemetry systems in specific and did not relate to encryption software in general[41]. Under a recent agreement between India and US, the former has agreed to facilitate the import of items listed on the US Munitions List. This, as we have seen earlier, might require specific licensing both for export and imports.

The Information Technology Act, 2000 introduces some form of control over the use of encryption for communication in India. 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.

Of importance to the present discussion however, is section 69 of the Act[42]. This section provides the Controller of Certifying Authorities with the power to intercept any transmission if certain criteria are satisfied. One such criterion provided for is the security of the state and concerns about the sovereignty and integrity of the nation. In such a case, the subscriber is under an obligation to decrypt the information for the authority. The viability of this provision however, remains questionable. The section provides that the controller can call upon any subscriber to decrypt a message in the event of certain circumstances arising. 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.
One cannot deny that there will be exceptional circumstances when transmissions need to be

[40] "Cryptography and Liberty 1999: An International Survey of Encryption Policy". At http://www/gilc.org/crypto/crypto-survery-99.html[Visited on 9 Aug.2008]
[41] Ibid

[42] Section 69 reads as under. "69. Directions of Controller to a subscriber to extend facilities to decrypt information.-(1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

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. The wording, it may be pointed out, is similar to that of the Telegraph Act, 1885, that came up for discussion in the P.U.C.L. case discussed earlier. If one follows the ruling in that case, it may be said that inadequate procedural safeguards would render the section inapplicable.

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.*

Encryption and Procedural safeguards

As in the case of any issue affecting constitutional rights, the validity, or alternatively, the invalidity, of restrictions on the practice of cryptography and encryption remains mere speculation. True, the right to privacy is recognized as inherent in the right to life with dignity in Article 21 and the right to freedom of speech and expression in Article 19. Neither of these can and should be allowed to stand as an impediment in curbing activities prejudicial to national security and interests. Not surprisingly, both these rights contain express conditions when they may be deprived.

At the same time, the balance cannot be allowed to tilt completely to one side, so as to negate the basic liberties, even when not absolutely essential. The only way out is a compromise between the two extremes. While the restrictions on cryptography and encryption may be abused for several illegitimate purposes,[43] so also the freedom is liable to be misused for antinational activities. The solution lies neither in absolute freedom nor unwarranted state control.

A possible solution to the problem may lie in the very technology that encryption uses. The problem has to be looked at, at a two-fold level. At one level, is the issue of encryption and cryptography as a mode of free speech and other is the more important issue of cryptography as an integral part of the right to privacy[44]. While the former can be subject to reasonable restrictions, the second can be restricted only by a procedure established by law.

With regard to the issue of free speech, it would be only reasonable to adopt the standard applied by the courts in permitting restrictions on other modes of expression. Cryptographic studies should therefore be dealt with as any ordinary publication and restraints on the same should be allowed only in so far as Article 19(2) permits them. With regard to 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.

It may not be unreasonable to build procedural safeguards into the existent IT Act, 2000. Such safeguards would have to include procedures for declaring when an issue involving national security concerns have arisen and on what grounds the same is to be determined. In such a scenario, the government or the concerned authority should be allowed to intercept encrypted information and be permitted to decrypt the same. Such a proclamation is not to be invoked at the absolute discretion of the authority; it will have to be made by the concerned legislature. Further, by making such a proclamation public, a provision could also be built in providing that for the period of the emergency or security concern, encryption should be avoided. In spite of this, if encryption is carried on, the government should have the authority to intercept the same. This would have the dual effect of avoiding unnecessary breaches of privacy and also reduce the task of the government, in intercepting and maintaining records, substantially.

In addition to a general invasion of privacy possible through the process set forth above, it may also be necessary, as mentioned earlier, to intercept the messages of specific individuals even when an actual emergency is not proclaimed. In such a scenario, it would be both unreasonable and impractical to require a proclamation by the legislature. However, here too, the circumstances necessitating the invasion will have to be clearly set forth by the relevant authority and the

[43] Nick Ellsmore , (April 5 2000) Cryptology: Law Enforcement and National Security vs. Privacy, Security & The Future of Commerce http://secinf.net/cryptography/Cryptology_Law_Enforcement_and_National_Security_vs_Privacy_Security__The_Future_of_Commerce.html[Visited on 8 Aug.2008]

[44] David M. Bessho National Security, Cryptography, and Personal Security http://www.gsu.edu/~lawppw/lawand.papers/dbessho.html[Visited on 8 Aug.2008]

procedural guidelines as to maintenance and destruction of intercepted messages will have to be adhere to. While this does give the authority concerned the power to single out an individual, it nevertheless will still be subject to review by an advisory board, as laid down in the P.U.C.L case and later, if necessary, by the judiciary. Arbitrary action would be reduced. 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.

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.

Conclusion

It is quite obvious, from law and practice, that there is a discernible difference in the perceptions towards privacy that people of different nations have. For example, Europeans seem to value view their privacy much more seriously than Americans do.

In the USA, people routinely give out everything from their driver's license numbers to their Social Security numbers to access to virtually all of their credit card transactions, and with very little justification. Europeans are much more concerned about privacy and have established a higher barrier so that companies cannot routinely trade databases and cannot get involved in the wholesale invasion of personal privacy[45].

It is not surprising that there is a much greater body of law in Europe and it varies from country to country as to the nature of personal privacy. In this context, it is fair to say that no generally applicable norms specifying standards to determine privacy infringement will be found - globally acceptable[46]. This is a reality that must be faced.

Again, as in the case of so many other cyber law issues, the principal villain behind the difficulties in emerging with a solution to this issue seems to be the absence of uniformity and the corresponding need to build up this 'commonality' through some form of international dialogue. Meanwhile, it ought to be the role of each state to ensure the protection of privacy and set relevant standards in a manner appropriate to the peculiar needs of its citizens.

While it is true that no procedure is completely foolproof and without loopholes, the procedure outline above gives individuals the choice to avoid the usage of encryption for a specific period and, thereby, avoid any breach of their privacy. While the executive should work out the exact nature of the guidelines and procedures, the aforesaid scheme may provide a starting point. Nevertheless, it has to be remembered that for a true democratic set up where liberties of individuals are supreme to function, mere legislation in the absence of a political will, would be futile.[47]

Bibliography:

Books

1. J Vaidya, M Zhu, CW Clifton – Advance in information security , Privacy Preserving Data Mining ,Springer 2005
2. Arthur Raphael Miller The Assault on Privacy: Computers, Data Banks, and Dossiers Published (1971)University of Michigan Press digitized Nov.2006
3. Simon Garfinkel Publisher Database Nation : The Death of Privacy in the 21st Century: O'Reilly & Associates; 1 edition (January 2001)
4. Reg Whitaker, Reginald Whitaker, The End of Privacy : How Total Surveilance Is Becoming Reality (Paperback) Publisher: New Press; (February 2000)
5. David Lyon (Editor) Surveillance as Social Sorting: Privacy, Risk and Automated DiscriminationPublisher: Routledge; 1st edition (December 2002)
6. Indian Constitution by VM Shukla (2000)
7. I Lloyd, Information Technology Law, Butterworths, 1993
8. Solove, Daniel J. and Marc Rotenberg "Information Privacy Law Cases and Materials" Aspen Publishing Co, 2002,
9. Bamford, J. *Body of Secrets : Anatomy of the Ultra-Secret National Security Agency from the Cold War Through the Dawn of a New Century.* New York: Doubleday, 2001.
10. Barr, T.H. *Invitation to Cryptology.* Upper Saddle River (NJ): Prentice Hall, 2002
11. Bauer, F.L. *Decrypted Secrets: Methods and Maxims of Cryptology,* 2nd ed. New York: Springer Verlag, 2002.
12. Denning, D.E. *Cryptography and Data Security.* Reading (MA): Addison-Wesley, 1982.
13. Ferguson, N. & Schneier, B. *Practical Cryptography.* New York: John Wiley & Sons, 2003.

[45] Legal Issues of Broadcasting on the Internet, Broadcasted over the Internet", at: http://www.tourolaw.edu [Visited on 8 Aug.2008]

[46] Malayan L.J. 205 (2002).,Abdul Haseeb Ansari,, Terrorism, National Integrity and Human Rights: A Critical Appraisal

[47] Professor Eben Moglen ,(2002) Computers, Privacy & the Constitution, Columbia Law School.

14. Mao, W. *Modern Cryptography: Theory & Practice*. Upper Saddle River (NJ): Prentice Hall Professional Technical Reference, 2004.
15. *N. Ferguson; B. Schneier (2003).* Practical Cryptography. Wiley. ISBN 0-471-22357-3.
16. *J. Katz; Y. Lindell (2007).* Introduction to Modern Cryptography. CRC Press. *ISBN 1-58488-551-3.*
17. A. J. Menezes*; P. C. van Oorschot;* S. A. Vanstone *(1997). Handbook of Applied Cryptography. ISBN 0-8493-8523-7.*
18. *Anoop MS (2007). Public key Cryptography - Applications Algorithms and Mathematical Explanations.* India*:* Tata Elxsi.

Journals /Articles

1. Singleton, Solveig. "Privacy as Censorship: A Skeptical View of Proposals to Regulate Privacy in the Private Sector." Cato Policy Analysis No. 295. (January 22, 1998). (skim)
2. Roger Clarke, CRYPTO-CONFUSION ,*Privacy Law & Policy Reporter* 3, 2 (May 1996), pp. 24-27, 30-33
3. Baker, Andrew. "The Historical Development of the G-7: An Incoherent and Disjointed Response to Global Interdependence?" G7RU Working Paper No. 2. Jordanstown: School of Public Policy, Economics and Law, University of Ulster, 1996.
4. Bayne, Nicholas. "The G8's Role in the Fight Against Terrorism." Remarks to the G8 Research Group, Toronto, 8 November 2001 http://www.g7.utoronto.ca/g7/speakers/baynenov2001.html.
5. Mark E Plotkin**;** Bert Wells**;** Kurt A Wimmer**,** E-commerce law & business , Aspen, 2003 New York, NY p 114-115
6. ITU Workshop on Ubiquitous Network Societies Document:UNSO5/ April 2005 Available online: http://www.itu.int/osg/spulni/ubiciuitous/Papers/Privacy%2obackground%20paper.pdf
7. Privacy International :-" Responding to Terrorism" PHR 2005; Available online: http://www.privacyinternational.org/article.shtml?cmd[3471=x-347-
8. Thomson and Knight LLP :-"Privacy when the World is On-Line" (18 June 2004) LexisNexis Martindale-Hubbell (R) Legal Articles [Visited 28 December . 2007]
9. Beth Givens ,Privacy Today: A Review of Current Issues, updated April 2008 http://www.privacyrights.org/ar/Privacy-IssuesList.htm
10. Randall Frost Who is securing your identity on line, June 28 ,2008, brand channel.com http://www.brandchannel.com/features_effect.asp?pf_id=177#more
11. David H. Holtzman , The Privacy Issue, Business Week,___Special Report April 8, 2008 http://www.businessweek.com/technology/content/apr2008/tc2008047_101047.htm
12. Key Technology . Privacy/Security Policy http://www.keyww.com/privacy.cfm
13. John D. Woodward, Jr. ,Biometrics: Facing Up to Terrorism ,2001 http://www.rand.org/publications/IP/IP218/IP218.pdf
14. By John Geralds US e-surveillance worries privacy groups, vnunet.com, in Silicon Valley [26-09-2001] http://www.vnunet.com/News/1125669
15. Does the Constitution Contain a Right to Privacy?by Harry Browne May 9, 2003 http://www.harrybrowne.org/articles/PrivacyRight.htm
16. Judith Miller, ReportCalls for Plan of Sharing Data to Prevent Terror ,New York Times, October 7,2002 http://emoglen.law.columbia.edu/CPC/archive/terror//07HOME.html
17. Unger, Robert, Robertson, Lawrie G. SRA Journal. "Reducing risky e-mail: there is no such thing as e-mail privacy. Winter 1998 v29 i3-4 p3(1)
18. Hurriyah El Islamy :-" Information Privacy in Malaysia: A Legal Perspective" (2005) 1MLJA 25
19. Theodore F. Claypoole:- "Privacy Regulations a Concern with Internet" LexisNexis MartindaleHubbell (R) Legal Articles (June 27, 2004)
20. Sweet & Maxwell 2002, Abu Bakar Munir & Mohammad Yasin, Privacy and Data Protection: A Comparative Analysis with Special Reference to the Malaysian Proposed Law
21. Malayan L.J. 205 (2002).,Abdul Haseeb Ansari, Terrorism, National Integrity and Human Rights: A Critical Appraisal 3
22. Rosnazura Idrus, "Leaving MyKad at Guardhouse under Review," New Straits Times (Malaysia), July 9, 2003.
23. ThirdAge Media. "Fight for Your Privacy."(1999) http://www.thirdage.com/news/archive/990317-01.html?rs March 17,1999.
24. Froomkin, A. Michael, "The Death of Privacy?" Stanford Law Review, Vol 52, (2000)1461-1543 http://personal.law.miami.edu/~froomkin/articles/privacy-deathof.pdf