June 29, 2008

“The issues of personal privacy and internet – A Critical analysis of Indian position and International scenario”

Nehaluddin Ahmad

Available at: https://works.bepress.com/nehaluddin_ahmad/1/
Article Title:
“The issues of personal privacy and internet – A Critical analysis of Indian position and International scenario”

Author:
Dr. Nehaluddin Ahmad
MA, LL.M. (Luck. India) LL.M. (Strathclyde ,UK), LL.D. (India)
Senior Lecturer,
Faculty of Business and Law
Multimedia University,
Jalan Ayer Keroh Lama
75450 Melaka Malaysia
E-mail: ahmadnehal@yahoo.com
Mobile No: +60166054353

Abstract
The development of technology in the communications industry over the last decade has witnessed the emergence of several relatively new legal and ethical issues, for which no concrete answers are to be found yet. Such technology is, however, liable to be misused by both, individuals and state machinery. That balance is now being shifted by two factors working in combination: on the one hand emerging information and communications technologies and their commercial use and governmental applications.

Communication, speech and expression undoubtedly constitute some of the most basic liberties of individuals and, to a large extent, can be considered inalienable. In the Indian context these rights are given statutory recognition in Part III of the Indian Constitution. An important point to note is that the Indian constitution does not include the ‘right to privacy’ as a fundamental right. Its existence, therefore, as a constitutionally guaranteed fundamental right is debatable. Nevertheless, the judiciary has, on more than once occasion, opined that the right is implicit in the right under Article 21, which provides that no person shall be deprived of his life and personal liberty without a procedure established by law.

This paper may try to assess the extent to which these factors are expected to influence privacy protection with personal liberties and the national safety especially in Indian context along with international scenario .For analysis, this paper focuses on information technologies at various levels of developments and commercialisation
Contents:

1. Introduction
2. The Concept of Privacy
2.1 The Right to Privacy
2.1.1 The Right to Privacy and New Technology
2.2 Privacy under Indian Constitution
3. Privacy and its Protection
3.1 Some comparative position
3.2 Unreasonable restraints on basic liberties
3.3 Privacy under the Indian Information Technology Act 2000
4. Encryption and cryptography: mode of communication
4.1 Restriction on cryptography in India: The information Technology Act 2000
4.2 Procedural safeguard
5. Regulation Models
5.1 The OECD Principles
5.2 US positions
5.2.1 Adult
5.2.2 Children
5.2.3 Seal Programmes
5.2.4 Future Action in the US
5.3 Data protection in the UK
6. Threats to Privacy
6.1 National Security and Privacy
6.2 International Standards
7. Conclusion
8. Bibliography
1. INTRODUCTION

“Technology has made us a ‘global’ community in the literal sense of the world. Whether we are ready or not, mankind now has a completely integrated information marketplace capable of moving ideas to any place on this planet in minutes. Information and ideas will go where they are wanted and stay where they are well treated. It will flee from manipulation or onerous regulation of its value or use, and no government can restrain it for long.”

The development of technology in the communications industry over the last decade has witnessed the emergence of several relatively new legal and ethical issues, for which no concrete answers are to be found … yet, No such development however, has had an impact even comparable to that of the Internet. With the development of the Internet into a ‘global marketplace’, the world has seen a sudden emergence of new, speedy means of communication. Not only has the Internet emerged as a lucrative centre for commercial transactions, it has also grown into an area where individuals from different corners of the world get to communicate freely and const-effectively.

Global computer-based communications cut across territorial borders, creating a new realm of human activity and throwing up a multitude of questions regarding the need for and manner of regulating this virtual world. Territorially based law-makers and law-enforcers find this new environment deeply threatening Electronic communications undermine the feasibility and the very legitimacy of laws based on geographic boundaries, defining a distinct cyberspace that needs its own laws and legal institutions. National infrastructure is common place in countries all across the globe. Individual

---

1 Walter B. Wriston, “The Twilight of Sovereignty: How the IT Revolution is Transforming our World”, 80 Iowa L.Rev.431.
2 Here the author looks at the growth of the internet into business area and concludes that for any business to retain its competitive edge entering the global market area, the internet is a logical necessity. also see Electronic commerce and new ways of working penetration and future development by Jack M. Nilles, Los Angeles 1999 see http://www.ecatt.com/country/us/EcattUSfinalreportformUSA.pdf
3 See generally “The net imperative”, The Economist, Vol. 351, No. 8125. Here, the author looks at the growth of the Internet into a business area and concludes that for any business to retain its competitive edge entering the global market area on the Internet is a logical necessity.
nations, each intent upon preserving what they perceive to be within the perimeters of their national interests, seek to regulate certain forms of speech because of content that is considered reprehensible or offensive to their national well-being or civic virtues.

Communication, speech and expression undoubtedly constitute some of the most basic liberties of individuals and, to a large extent, can be considered inalienable. In the Indian context these rights are given statutory recognition in Part III of the Indian Constitution.\(^4\) As a necessary corollary to the freedom to communicate and speak, is the fact that this must be allowed with as little state interference as possible, i.e. in the absence of state intrusion and interference into the content of the communication. This immediately raises the controversial issue of the ‘right to privacy’. An important point to note is that the Indian constitution does not include the ‘right to privacy’ as a fundamental right. Its existence, therefore, as a constitutionally guaranteed fundamental right is debatable. Nevertheless, the judiciary has, on more than once occasion, opined that the right is implicit in the right under Article 21, which provides that no person shall be deprived of his life and personal liberty without a procedure established by law. The right to privacy, it can be said, is considered a logical corollary to the liberty to speak and express oneself.

Essentially, there exist two streams of argument: one choosing to analyse the ways in which existing national laws should or will affect the rights and responsibilities of Net users, and the second positing that no country’s laws should apply to cyberspace. The former group ignores the essentially international nature of the Net and overlooks the fact that regulation of the Net probably will happen at least in part at the international level.\(^5\) The latter group unrealistically claims that cyberspace should be viewed by countries around the world as a new, separate jurisdiction with both the right and the ability to govern itself. These activists overlook the fact that virtually no country in the world is

---

4 Article 19(1)(a) of the Constitution, guarantees to all citizens the fundamental “right to freedom of speech and expression.” While communication is not explicitly mentioned, one may reasonably conclude that communication must be either by means of speech or expression and can be said to be implicit in this right.

likely to agree to this approach, as it would require them to cede a degree of sovereignty to a nebulous group of self-appointed self-regulators.\footnote{FTC (May 2000): Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress.}

No liberty, however inalienable, can exist without restrictions. It is but necessary that circumstances will arise when liberties may be reasonably restricted if not suspended. The right to freedom of speech and expression, under the Indian Constitution too, can be regulated for certain specific purposes contained therein\footnote{In Indian Constitution, Article 19(2) are provided the conditions when the right can be curtailed.}. One of the conditions, when such a restriction may be imposed, is national security. Though this may appear legitimate, the question essentially remains as to what constitutes national security and who it is to be determined by.

It is submitted that regulation of the Net is inevitable. Consequently, advocates of cyber-independence are committing a serious strategic error by concentrating a great deal of their collective energy on their ill-fated campaign. They would be much better advised to take an active role in the nascent regulatory process in order to ensure the enactment of the most effective and least restrictive regulatory scheme. These Net-users are not only the most knowledgeable members of their given societies about the Net, but also the ones who will feel the effects of regulation most acutely. Therefore, it is in their interests to put aside their, often contemptuous, attitudes toward legislators and join in guiding the regulatory process. This should be done by advising governments on the positive value of the Net for democratic processes and should also involve co-operating in the continued development of appropriate laws and of such technologies as content filters and labeling systems in order to minimize the restrictions placed on Net speech, information and communication.

As mentioned earlier, many opponents of governmental regulation of the Net insist that any attempt to enforce laws on the Net through technological means is destined to fail. They claim that the Net is simply too flexible, decentralized and multifaceted to be harnessed by filters or the like. This position fits well with the popular image of the Net
as a place without limits, a massive, multi-headed beast that will find a way around any barrier placed in its path. But that image might not be completely accurate. While the effectiveness of filtering technology remains unproven, significant progress appears to have been made in the development of effective filtering systems in the last few years.

Two potentially important tools have been developed, one is a widely accepted standard for labeling Net documents based on their content and the other, a hardware device that ostensibly would allow local regional or national officials to control what content is available to users in their domain.

Activists at both ends of the spectrum disregard an integral aspect of the global composition of the Net. Those who advocate unfettered Net communication and those who espouse some form of national Net regulation are similarly constrained in the pursuit of their objectives by the very structure of the information infrastructure. It is the global aspect of the information infrastructure that shapes the debate on freedom of speech and limits absolutists and regulators at the same time.\(^8\)

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 become necessary in the interests of national security.\(^9\) 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.\(^10\)

That balance is now being shifted by two factors working in combination: on the one hand emerging information and communications technologies and their commercial and

---


governmental application and on other governmental actions in response to rising crime and terrorism.

New anti-terrorism laws, particularly those that expand the surveillance authority of the state, now threaten freedom and privacy on every continent. Against this backdrop, the new measures could potentially impact privacy and civil liberties significantly. Will freedom, privacy, and other values be compromised by these changes? This paper may try to assess the extent to which these factors are expected to influence privacy protection with personal liberties and the national security especially in Indian context along with international scenario. For analysis, this paper focuses on information technologies at various levels of developments and commercialisation.

2. THE CONCEPT OF PRIVACY

“Privacy is the interest that individuals have in sustaining a ‘personal space’, free from interference by other people and organization” 11

In the 1890s, U.S. Supreme Court Justice Louis Brandeis articulated a concept of privacy that urged that it was the individual's "right to be left alone." Brandeis argued that privacy was the most cherished of freedoms in a democracy, and he was concerned that it should be reflected in the Constitution. 12

So perhaps a more useful definition (from American Professor of Law, Alan Westin) is that privacy is the "claim of individuals to determine for themselves, when, how and to what extent information about themselves is communicated to others". This claim of informational privacy assumes that all information about an individual is fundamentally his or her property to communicate or withhold as desired. 13

Of all the human rights in the international catalogue, privacy is perhaps the most difficult to define and circumscribe. 14 Privacy has roots deep in history. The Bible has

11 Rogers Clark “introduction of Dataveillance and Information Privacy, and Definitions of Terms“
numerous references to privacy. Islam recognizes the right of every citizen of its state that there should be no undue interference or encroachment on the privacy of his life. There was also substantive protection of privacy in early Hebrew culture, Classical Greece and ancient China. These protections mostly focused on the right to solitude.

The essence of the privacy is the understanding that individual can legitimately claim that information about themselves should not be automatically available to other individuals and organizations, and that even where such information is possessed by other party, the individual must be able to exercise a substantial degree of control over that information or data and its use. Flowing from this, it is quite natural that individuals feel the need for a mechanism by which interest is protected. Obviously, there are opposing interests too but protection is a process of finding appropriate balance between privacy and these multiple competing interest.

The pervasive nature of online information management system makes it extremely difficult for end user to identify abuse of their personal privacy. Most of the technologies used to monitor or profile individual, and the interactions they make possible, are invisible to the internet user. Data collection, data aggregation and data mining carried out by third party organizations, and their use for making purpose are therefore greatly facilitated and underlying use of the internet justifies people’s concern about the possibility of intrusion into their personal information.

2.1 THE RIGHT TO PRIVACY

It appears to be a matter of consensus in most liberal democracies that there do exist private and public spheres in every citizen’s life and that these two spheres are distinct

16 Human Rights In Islam; published by The Institute of Islamic Information and Education http://www.usc.edu/dept/MSA/humanrelations/humanrights/
17 Published by Science and Technology Options Assessment (STOA). Ref : project no. IV/STOA/RSCH/LP/politicon.1
19 supra note 9
and have to be treated as such as pornography or the use of narcotics, it is generally agreed that the liberal democratic state has no power to interfere with the private aspects of its citizens’ lives. However, as has been stated before, a dilemma arises if activities undertaken in the so-called private sphere have an impact upon the so-called public sphere. It is in this context that the issue of a right to privacy arises. Therefore, in a modern state, when means of communication and communication networks have undergone a radical change, the threat to the right of privacy appears to be a real and threatening concern.

There is a common misconception that the right to privacy is merely a weapon to ensure confidentiality in human affairs. This, however, does not present the complete picture. Confidentiality is, no doubt, one element in the panorama of rights covered by the right to privacy, but it is just that, one element. It must not be forgotten that the right to confidentiality only arises after information regarding human transactions or affairs have reached third parties. The stage prior to this is with regard to the collection of data regarding individuals and it is here that the problems start. It has to be recognized that the right to privacy extends over the entire gamut of collection, retention, use and disclosure of information. It stems out of the basic human desire for a secure identity of one’s own and, to that extent, cannot be denied.

In this context, it may be said that privacy involves the right to control one’s personal information and the ability to determine if and how that information should be obtained and used.

The above principle has sometimes been referred to as the right to “informational self-determination” and has been recognized as a distinct right of citizens by a German

---

22 Privacy International, Privacy and Human Rights 1999  
http://www.privacyinternational.org/survey/Overview.html  
23 Clyde Wayne Crews Jr., (June 26, 2003) Protecting Privacy in the Database Nation  
http://www.cato.org/dailys/06-26-03.html  
24 For a broader definition see generally, A.H. Robertson, 1973, Privacy and Human Rights, 1st edn., Manchester University Press, Manchester
Constitutional Court. However, this right is not as well recognized in other constitutions the world over. This has led to the legal position on the right to privacy becoming extremely nebulous and the specter of arbitrariness seems to have crept in with regard to judicial pronouncements on the right to privacy.

This principle becomes all the more relevant with the onset of the Internet and e-commerce in India. The volume and varying nature of transactions carried out on the net are such that the right to privacy must exist at least to a limited extent. At the same time, the very same factors – volume and nature of transactions also raise the issue of security concerns as to the political, social and economic health of the nation. Encryption of the details of our personal transactions could certainly assure us of a greater degree of privacy but may also encroach upon the domain of national security concerns and the two ends may be said to be in conflict. Internet privacy could also be viewed as economically important since it gives consumers the assurance that their personal particulars will not be released to unauthorized persons. This, in turn, would give consumers the confidence to participate more fully in e-commerce transactions. Moreover, the right to privacy is intimately connected with the freedom of expression and disregarding the right may lead to gross violations of the freedom of expression via the Internet.

India is a signatory to the International Convention on Civil and Political Rights, 1966, which, by Article 17, provides for a right to privacy. In view of the fact that an established principle of law postulates that if there are two possible interpretations of a municipal law, the one favouring International Law is to be taken, should not Indian Constitutional law permit the right to privacy?

26 A case directly on the point is Rajagopal v. State of Tamil Nadu, 1995 (6) SCC 632, where a murderer’s proposal to write his autobiography was challenged on the ground that it would infringe upon the right to privacy of several persons named in the book.
27 Article 17 of the ICCPR provides that (1) No one shall be subject to arbitrary or unlawful interference with his privacy, family, human or correspondence, nor to lawful attacks on his honour and reputation.
28 A judicial precedent may also be found in Khanna, J’s., judgment in the ADM Jabalpur case, (1973) 4 SCC 225.
Before examining constitutional positions in India as well as the world over, it may be necessary to examine the guidelines along which the extent of the right to privacy may be determined. The guidelines, which may be generally taken as accepted, have been framed by a European organization, named the Organisation for Economic Co-operation and Development, in 1980. The principles are as follows:

- Firstly, collection of personal data should be done with the consent of the person and lawfully.
- Secondly, the data collected should be pertinent to the subject under investigation. Therefore, for example, a man’s medical problems ought not to be investigated while data on his tax returns is being collected.
- Thirdly, the purpose as to collection ought to be clearly specified.
- Fourthly, such data should not be further used except without express consent of the subject and under the sanction of the law.
- Fifthly, there ought to be adequate security safeguards so as to prevent leakage of data into the hands of unauthorized persons or the destruction of classified material.
- Sixthly, there ought to be a high degree of accountability detailing the persons who are in charge of the process of collection and this is linked with the next point, which deals with the individual’s participation in the process of data collection. The individual should have the right to confirm whether there is any data on him and whether such data is pertinent or relevant to the purpose for which it is collected. He should also have the right to access any data dealing with him at any time as may be convenient to him and such data should be made completely available to him in a reasonable manner and if the data collected is not entirely accurate he should have the opportunity to point out the fallacies that may exist.29

These then may be said to be the broad principles governing the existence of the slightly ambiguous right to confidentiality. Although the principles in themselves appear to be

29 supra., n. 23
reasonably straightforward and precise, it is only when they are viewed in the light of conflicting national security concerns that they appear to be more problematic.

An example may be relevant at this juncture. If the principles framed by the OECD were to be followed in totality, entities such as official intelligence agencies would practically be rendered inoperative, as would bodies possessing policing functions. Under a strict construction of the terms of OECD, every potential suspect would have to be informed before his actions were scrutinized, thus putting him on the alert.\(^\text{30}\) The very purpose of having such bodies would be negated.

A possible compromise may be achieved by reading the terms of the OECD so as to interpret them harmoniously with such provisions of the constitutions of the various nations as may be relevant. It is here, then, that it becomes important for us to examine certain provisions of the Indian constitution that may have an impact, direct or otherwise, upon the conflict between the need or privacy as opposed to security concerns which are vital for the continuation of the nation state.

2.1.1 THE RIGHT TO PRIVACY AND NEW TECHNOLOGY:

Modern technological developments and, in particular, the so-called “convergence” of computer and telecommunications technologies have created an environment in which here is inexpensive and ready access to an ever growing pool of personal information. Further, the interoper-ability of modern systems have made it possible for even the smallest of businesses to collect and analyse detailed information about identifiable individuals almost anywhere in the world.\(^\text{31}\)


The Internet is, itself, a rich source of information about online consumers. Web sites collect much personal information both explicitly, through registration pages, survey forms, order forms, and online contests, and by using software in ways that are not obvious to online consumers. Through cookies and tracking software, Web site owners are also able to follow consumers’ online activities and gather information about their personal interests and preferences.

The volume and varying nature of transactions carried out on the net are such that the right to privacy must exist. At the same time, the very same factors – volume and nature of transactions – also raise the issue of security concerns as to the political, social and economic health of the nation. Internet privacy could also be viewed as economically important since it gives consumers the assurance that their personal particulars will not be released to unauthorized persons. This, in turn, would give consumers the confidence to participate more fully in e-commerce transactions. Moreover, the right to privacy is intimately connected with the freedom of expression and disregarding the right may lead to gross violations of the freedom of expression via the Internet.

2.2. PRIVACY UNDER THE INDIAN CONSTITUTION

The last few decades have seen the growth of the belief that the Constitution contains rights other than those expressly mentioned in its content. These rights could be called unenumerated rights. Further, there exists a test for determining whether an unenumerated right actually exists or not. To establish the presence of such a right it must be shown that the right in question is an integral part of the enumerated right upon which its existence depends. If the unenumerated right is a definite and integral part of the enumerated right, then it has as much force as the enumerated right itself and is subject to

---

32 Most people who use the Internet probably do not realize that banner ads that they are seeing on Web pages are also sending information about them back to Internet marketing companies.
33 supra note 26
36 Harry Browne, May 9, 2003, Does the Constitution Contain a Right to Privacy? http://www.harrybrowne.org/articles/PrivacyRight.htm
the same conditions and restrictions as the enumerated right itself. 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.\textsuperscript{37} 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\textsuperscript{38}, in Article 19(1)(a)\textsuperscript{39} as well as in Article 19(1)(d)\textsuperscript{40}. 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. State of Uttar Pradesh\textsuperscript{41}. In holding that Regulation 236(b) of the Uttar Pradesh Police Regulations was invalid, the Court clearly indicated that there did exist a right to privacy within the scope of Article 21. In delivering its judgment, the Court was influenced by two American decisions in particular. The first of these was the case of Munn v. Illinois\textsuperscript{42}, 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

\textsuperscript{37} 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

\textsuperscript{38} Indian constitution Article 21 states that “No person shall be deprived of his life or personal liberty except according to procedure established by law.”

\textsuperscript{39} Indian constitution Article 19(1)(a) states that “All citizens shall have the right to freedom of speech and expression”.

\textsuperscript{40} Article 19(1)(d) states that “All citizens shall have the right to move freely through the territory of India”.

\textsuperscript{41} 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”.

\textsuperscript{42} 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 Corp., AIR 1986 SC 180, and the right to education in Unnikrishnan v. State of A.P., (1993) 1 SCC 706.
second decision was more directly on the point. This was the case of Wolfe v. Colorado\textsuperscript{43} 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\textsuperscript{44}, which guaranteed the inviolability of a person’s home and held that a person had a right to privacy.

It may be relevant to mention here that the U.S Supreme Court decision in Wolfe’s case was made simpler by the existence of the Fourth Amendment\textsuperscript{45} to the Constitution which guarantees that the houses or other private properties of citizens would not be searched and that no searches or seizures shall be made without a warrant. Therefore, within the framework of the U.S Constitution, there does appear to be some space for a right to privacy and the connection to be made is not as tenuous as it is in India. In India, citizens do not enjoy a right to correspondences specifically as is enjoyed under the Japanese Constitution.

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\textsuperscript{46}, 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\textsuperscript{47}, it has been held that there is not substantial difference between the phrases

\textsuperscript{43}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.
\textsuperscript{44}(1604) 5 Co Rep 91.
\textsuperscript{45}The Fourth Amendment reads “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no warrants shall issue but upon a probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
\textsuperscript{46}(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.
\textsuperscript{47}AIR 1978 SC 597.
“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 the law under which the violation has taken place is just, fair and reasonable.

A landmark development in this regard would definitely be the case of P.U.C.L. v. Union of India48, 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 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.

This clarification by the Court was merely as part of its efforts to show that there ought to be no violation without accountability. In this regard, several important points were made. These were as follows:

1. Tapping should only be authorized by certain senior officials who may be made accountable subsequently.
2. Only such information ought to be collected and retained as is pertinent to the issue at hand.
3. The order to tap telephones must be periodically reviewed by a board and the order to renew tapping should not be resumed without ministerial sanction.
4. Records should be made so as to facilitate greater accountability.
5. A Review Committee should be set up so as to investigate the validity of orders as to violations of privacy.

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

3. PRIVACY AND ITS PROTECTION:

Universal Declaration of Human Rights, 1948, which specifically protected territorial and communications privacy. Article 12 “No-one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks.” 49 Privacy is a fundamental human right recognized by the International Covenant on Civil and Political Rights 50 and in many other international and regional treaties.

Fortunately, the right of privacy is included in the constitution of nearly every country in the world. Often, when it is not included, ordinary laws and provisions cover the matter such as in Ireland and India. 51

The Preamble to the Australian Privacy Charter provides that,

"A free and democratic society requires respect …of speech. . .Privacy is a basic human right and the reasonable expectation of every person." 52

Most recently-written Constitutions such as South Africa's and Hungary's include specific rights to access and control one's personal information.

Interest in the right of privacy increased in the 1960s and 1970s with the advent of information technology (IT). The surveillance potential of powerful computer systems prompted demands for specific rules governing the collection and handling of personal information. The genesis of modern legislation in this area can be traced to the first data protection law in the world enacted in the Land of Hesse in Germany in 1970. This was followed by national laws in Sweden (1973), the United States (1974), Germany (1977) and France (1978). 53

---

52 "The Australian Privacy Charter", (1994.) published by the Australian Privacy Charter Group, Law School, University of New South Wales, Sydney
53 David Flaherty,( 1989)"Protecting Privacy in surveillance societies", University of North Carolina Press,
Two crucial international instruments evolved from these laws. The Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data \(^{54}\) and the Organization for Economic Cooperation and Development's Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data \(^{55}\) articulate specific rules covering the handling of electronic data. The OECD guidelines have also been widely used in national legislation, even outside the OECD countries. Bulgaria endorsed in January 2002 its new Personal Data Protection Act\(^ {56}\). Poland approved in May 2002 the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Slovenia amended its Data Protection Act in 2001 to establish an independent supervisory authority\(^ {57}\). A National Internet Advisory Committee in Singapore released a Model Data Protection Code for the Private Sector in February 2002\(^ {58}\). Peru enacted a data protection law in August 2001 covering credit-reporting agencies, and both Peru and Mexico passed new freedom of information laws in 2002\(^ {59}\).

Most legal systems will be a mixture of these approaches\(^ {60}\), something that can be seen in the US. For example, in the United Kingdom, several steps have been taken with regard to the issue of Internet privacy. The Data Protection Act, 1998 was enacted\(^ {61}\) on July 16, 1998 came into force on March 2000 for implementing the European Union’s Data Protection Directive. This is the key to the issue of Internet privacy in Great Britain. This form of legislating has been backed up by Court decisions in a number of sensitive matters.\(^ {62}\) In Japan, the Ministry of International Trade and Industry has released several

\(^{54}\) Convention fn the Protection of Individuals with regard to the Automatic Processing of Personal Data Convention , ETS No. 108, Stasbourg, 1981. &lt;http://www.coe.fr/eng/legaltxt/108e.htm&gt.;

\(^{55}\) Supra n 31 &lt;http://www.kantei.go.jp/jp/it/privacy/houseika/dai11/11siryou5.html&gt;

\(^{56}\) The global reach of privacy invasion.

\(^{57}\) Activity of the European Union Summaries of Legislation &lt;http://europa.eu.int/scadplus/leg/en/lvb/e22110.htm&gt;

\(^{58}\) see at &lt;http://www.privacyinternational.org/survey/phr2003/countries/singapore.htm&gt;

\(^{59}\) Mexico's new freedom of information law &lt;http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB68/

\(^{60}\) L. Kably. (27th November 1999)"The Millennium Dollar Issue :Coming of Cyber Age “, The EconomicTimes, p.5

\(^{61}\) Great Britain, Data Protection Act 1998, Chapter 29, London, HMSO

\(^{62}\) Stepehen Graham, John Brooks, and Dan Heery Towns on the Television : Closed Circuit TV in British Towns and Cities; Centre for Urban Technology, University of Newcastle upon Tyne
guidelines pertaining to the protection of computer processed personal information in the private sector in 1997\(^{63}\).

Besides the systems mentioned above, there was a belief that civil and penal law instruments were ineffective and that threats to individual privacy would not be eliminated, until preventive instruments were mobilized. In addition, there was a need to address the delicate problem of citizen/user consent. According to Directives 2002/58 EC\(^{64}\) and 1995/46/EC the data subject’s consent’ shall mean any freely-given specific and informed indication of his wishes by which the data subject signifies his/her agreement to personal data relating to him/her being processed\(^{65}\). The ECHR is silent with regard to the issue of consent and waiver of rights, which is disturbing, since firms often take users’ consent to render transactions legitimate\(^{66}\). European Data Protection legislation, although very flexible with regard to consent, has at least some explicit answers to the possible abuses of consent\(^{67}\).

### 3.1 SOME COMPARATIVE POSITIONS\(^{68}\)

In India, the Information Technology Act -2000 encompass a wide range of issues spanning from legal recognition of electronic signatures and online contracts. However, aspects such as Internet privacy are still viewed as non-issues. A possible way out is to view the right to privacy on the Internet as being protected partly by the Constitution and partly by the tort law on Defamation, which also exists as a crime under Section 499 of the India Penal Code. Tort relief is important since the Constitutional provisions only


\(^{64}\) see [http://www.ovum.com/go/content/c.36927](http://www.ovum.com/go/content/c.36927)


\(^{66}\) The UK Data Protection Act 1998 was passed to implement the general Data Protection Directive 1995. In recitals 1 and 2, the Directive made explicit reference to the ECHR, including respect for the private domain.

\(^{67}\) Frank A. Koch, European Data Protection - Against the Internet? [http://www.privacy.org/pi/conference/copenhagen/koch.html](http://www.privacy.org/pi/conference/copenhagen/koch.html)

\(^{68}\) L. Kabaly, \((27^\text{th}}\) November, 1999), “The Millennium Dollar Issue: Coming of Cyber Age”, The Economic Times, p.5. Information in the private sector in 1997. Further, the Japan Information Processing Development Centre has developed a privacy seal-granting programme.
provide a remedy to Governmental violations of the right to privacy while individuals may be sued only under Tort law or under the Indian Panel Code. It is unfortunate, however, that the violation of an individual’s privacy per se is still not viewed as an offence in India.

In the United States, pressure to deal with privacy issues are growing and in June 1998, the Federal Trade Commission submitted a report to Congress which has materialized into the Children’s Online Privacy Protection Act which is to come into effect from April 21, 2000. Intrusions into the privacy of a child can now be undertaken only after obtaining parental consent. This has been sought to be extended to adults as well by means of the Online Protection of Privacy Act. Moreover, private bodies such as the Better Business Bureau have sought to meet the lacuna by providing a list of recommended sites so as to increase consumer confidence in e-commerce.

In the United Kingdom, several steps have been taken with regard to the issue of Internet privacy. The Data Protection Act, 1998 was enacted on July 16, 1998 for implementing the European Union’s Data Protection Directive.69 This is the key to the issue of Internet privacy in Great Britain. This form of legislating has been backed up by Court decisions in a number of sensitive matters. For example, in the recent Source Informatics case, a UK court held that prescription information collected in anonymous form by doctors is subject to patient confidentiality and cannot be disclosed.

In Japan, the Ministry of International Trade and Industry has released several guideline pertaining to the protection of computer processed personal .70

3.2 UNREASONABLE RESTRAINTS ON BASIC LIBERTIES

Bernstein v. United States Dept. of State

69 Supra 68 http://www.privacy.org/pi/conference/copenhagen/koch.html
70 A report was by the Ministry of Public Management, Home Affairs, Posts and Telecommunications of Japan. Joichi Ito President and CEO Neoteny Co., Ltd. http://joi.ito.com/joiwiki/PrivacyReport
we have seen the basic issue of privacy involving state restriction and regulation on the practice of cryptography. This issue came up for discussion before the United States judiciary in the case of Daniel Bernstein v. United States Dept of State. In this case, the court examined in substantial detail, cryptography and liberty-related issues. The case assumes great importance for the simple reason that it was the first to raise the issue of restraint on cryptography as an unreasonable fetter on certain basic liberties. It will be pertinent to note that while this case was decided on constitutional principles of the United States, a very similar analogy can be drawn in the Indian context, where the nature of fundamental rights is very similar to the basic liberties guaranteed under the American constitutional scheme.

The facts of the case in Daniel J. Bernstein v. United States Dept. of State were relatively straightforward. The plaintiff was a professor who worked and carried on research in the area of cryptography and encryption. He had developed a new method of encryption and had developed it into a programme which he called Snuffle. He intended to publish the source code of the same and present it in academic circles. He also wanted to make the information public on the Internet.

The US Arms Export Control Act authorises the President to control the import and export of defense articles and services by including such items on the defense list called the US Munitions List (the USML). Once an item has been included on the said list, a person desirous of importing or exporting the same requires a license from the government before he can do so. The International Traffic in Arms Regulations of the United States authorizes the United States Secretary of State to implement the provisions of the aforementioned Act. The ITAR provides for a process known as the commodity

---

72 The case was initially filed in the District Court of Northern California (No. C-95-0582 MHP). The court found in favour of the plaintiff. Thereafter, the plaintiff filed two other similar suits, which were in substance on the same issue as the first. In all three cases, he was successful in the District Court.
73 Hereinafter referred to as the “AECA”.
74 22 U.S.C s2778(b).
75 This is, of course, provided the item does not fall within the exceptions mentioned therein. See, 22 U.S.C s2778(b).
76 22 C.F.R s 120-130. Hereinafter referred to as the ‘ITAR’
Jurisdiction Procedure. In such a process, on an application, the relevant authority determines whether an article or a service is covered by the USML and whether a license is required to import or export the same\(^\text{77}\).

It would be pertinent to note that under the United States Munitions List, several cryptographic items and services find place\(^\text{78}\). A detailed list of such items is to be found, and several such items, used for commercial purposes on a wide scale, are excluded from the list. These are primarily those used in ATM machines and other such electronic instruments.

Upon developing his programme and the process, the plaintiff submitted a commodity jurisdiction request through the process mentioned earlier. His request was specifically to determine whether his programme written in C (a computer language) and his academic paper describing the programme were on the USML. The ODTC replied to this stating that the programme, not being a ‘stand-alone cryptographic algorithm’ would be subject to the restrictions in the AECA. The plaintiff, however, was not clear as to the academic paper. As a result, he sent in another commodity jurisdiction request, which included in addition to the actual programme, a request for determining whether the academic paper and written instructions relating to usage and programming for usage were also subject to the same restrictions. At this point, the ODTC clarified that only the actual programme was subject to the restriction and not all the mentioned items.

While the commodity jurisdiction may have permitted the plaintiff to publish the aforementioned academic paper, ‘export’ under the ITAR is defined to include the disclosure of technical data to a foreign person, irrespective of whether the disclosure occurs in the United States or abroad. This, undoubtedly, would have also prevented him

\(^{77}\)This is generally done by the Office of the Defense Trade Controls (EDTC)

\(^{78}\) The list reads as “Cryptographic systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems...”. The wide wording of the list is obvious. Thus, apart from cryptographic items specifically excluded, all others would automatically find place in the list and, therefore, require licenses for their import or export.
from publishing his findings in any scientific journal, which could be accessed by foreign nationals.

In light of these developments, the plaintiff filed petition challenging the AECA and the accompanying regulations of the ITAR as unconstitutional since they operated as a prior-restraint on speech, violative of the First Amendment. He also challenged them as being vague, overbroad and granting arbitrary discretion to the concerned authorities.

A primary objection was raised on behalf of the defendants that the AECA precluded any judicial review of regulations issued under the section and of action taken under\textsuperscript{79}. The court reviewed the provisions of the Act and concluded that what the Act sought to achieve was nothing more than a prevention of judicial review of any policy decision, which was best left to the executive and administrative authorities\textsuperscript{80}. Accordingly, it concluded that what was being done in the present case was a judicial review of the constitutionality of the Act, which was not prohibited by the Act and was within the competency of the court. Thus, it dismissed the preliminary objection of the defendants.

The court also concluded that it was not seeking to question either the inclusion of the items onto the USML or the commodity jurisdiction determination made by the ODTC. Thus the court laid down that in the course of the proceeding what it was seeking to review was the colourable constitutional claim of the plaintiff\textsuperscript{81}.

Coming to the merits of the case, the court opined that in view of the second clarification made by the ODTC, the academic paper was clearly not included on the USML and that the plaintiff was at liberty to publish the same without any license. The primary question in the case revolved around determining whether the computer programme which was in

\textsuperscript{79} 22 U.S.C. s 2778(b)(h). “The designation by the President (or by an official to whom the President’s functions under subsection (a) of this section have been duly delegated), in regulations issued under this section, of items as defense articles or defense services for purposes of this section shall not be subject to judicial review”

\textsuperscript{80} The inclusion of an item onto the USML, for instance, would be a matter of policy, dependent on the specific necessities of national security best left to the discretion of the administration and the government.

\textsuperscript{81} The court, in reviewing the concept of colourability, concluded that the concept was very ambiguous. For such a claim, however, the court rightly pointed out that there must be a cognizable interest that the plaintiff seeks to protect and that the claim cannot be frivolous, merely to invoke jurisdiction of the court.
the form of computer code, could be classified as a mode of speech and expression and if so, whether the requirement of licensing was an invalid prior restraint on free speech. The defendants sought to draw a distinction between speech and conduct and submitted that the code, in so far as it only resulted in the computer performing certain functions was conduct and not speech of any form.

The court, in looking at this claim, came to the conclusion that all speech was ultimately a form of conduct and that the distinguishing factor of speech was that it consisted of a “….sophisticated and complex system of understood meanings.” Thus, the functionality of a language would not convert it into a form of conduct; it would remain a language in essence. Thus, it was immaterial whether the language instructed the machine directly or whether it informed human conduct. In reaching this conclusion, the court also relied extensively on copyright law where it is a concluded position that computer programmes are a form of “expression”. The position is similar in India, where copyright protection is available for computer programmes. Thus, the court concluded that for the purposed of the First Amendment, the source code of the encryption programme of the plaintiff constituted “speech”.

An important contention that was raised on behalf of the defendants was that the First Amendment did not restrict milk governmental regulation of conduct, if the same ran afoul of the freedom of speech, incidentally. The court, however, rejected this argument and concluded that since the government action was aimed at directly curbing free speech, it was not incidental and, therefore, the exemption would not hold good. It will be of importance to note that this is similar to the position taken by the Indian


---
82 In reaching this decision, the court relied on the US Supreme Court ruling in Ward v. Rock Against Racism, 491 U.S 781, where the court held that music was liberty-protected speech though it was wholly functional in essence.
83 They relied on the Supreme Court’s decision in United States v. O’Brien, 391 U.S 367

In this case, the court ruled that an incidental restriction would be valid if:

- a) it was within the competence of the authority making them,
- b) it was in furtherance of important/substantial government interest,
- c) if such interest was un related to the suppression of free speech and
- d) the incidental restriction was no more than was essential
Supreme Court on several occasions. The courts in India, in determining the restriction on any of the fundamental rights, apply the test of ‘direct, inevitable consequence’ to determine whether the restriction is incidental or substantial.

In discussing the question of whether the restriction was unconstitutional, the court was very brief. It opined that since the position was that all prior-restraints came with a strong presumption of invalidity and since the programme was speech for the purpose of the constitution, the claim was valid and, accordingly, it was upheld. On the question of whether the statutory provision suffered from the vice of ‘substantial overbreadth’, the court held that it was not an issue that needed to be determined by it. The court also opined that the claim of the plaintiff that the statutory provisions were vague was not frivolous and, therefore, permissible.

The District Court, it must be remembered, did not rule on any substantive issue other than the fact that the plaintiff claims were justified and not frivolous. It did not read down the statutory provisions or set them aside as unconstitutional. It merely concluded that the plaintiff had a legitimate case made out.

Subsequently, the court granted the plaintiff summary judgment in the case. Later, when the government introduced certain changes to the ITAR procedures, but retained the basic restrictions, the plaintiff filed another complaint challenging the validity of the modified rules. Once again he was granted a summary judgment on grounds identical to the ones outlined above.

These decisions of the District Court were appealed by the defendants, in the US Ninth Circuit Court of Appeals. The court in the appeal restricted itself primarily to the

---

84 See Bennett Coleman v. Union of India, (1972) 2 SCC 788.
85 See, R.C. Cooper v. Union of India, AIR 1970 SC 564; Maneka Gandhi v. Union of India; (1978) 1 SCC 248.
86 See, Bernstein v. Dept. of State, 945 F. Supp 1279 (N.D. Cal 1996), referred to as Bernstein II.
87 See, Bernstein v. Dept. of State, 974 F. Supp 1288 (N.D. Cal 1997), referred to as Bernstein III.
88 Bernstein v. Dept. of Justice, Case Number 97-16686, filed on 5-6-99. In this case, the court affirmed the decision of the District Court, but examined the merits of the case afresh. Its reasoning was slightly more restricted than that of the previous court.
question whether the license requirement constituted an unconstitutional prior restraint on the liberties granted by the First Amendment. The court agreed with the District Court’s finding that any prior restraint licensing requirement had to be looked at with suspicion and, in the process, observed that there was a two-fold reason for the same. One, that it would result in self-censorship and two, that it would mask unnecessary arbitrary censorship by the government for illegitimate purposes.

The court examined the issue at two levels; one whether the plaintiff was entitled to bring a facial challenge against the licensing requirement and two, whether the restriction was constitutionally invalid on merits. At this point, it would be relevant to understand the concept of facial challenge. It is, basically

One of standing and involves the plaintiff being allowed to challenge the validity of the licensing regime, even before obtaining a license and also allowing him to further the cause of those not party to the suit. Thus, he may challenge the validity though his conduct has not been specifically proscribed by the regime.

The court, at the very outset, observed that the licensing regime armed the authority concerned with unbridled discretion to issue licenses and single out individuals for discrimination. The court then went on to examine the issue whether the programme in the form of the source code, constituted “speech” and answered the question in the affirmative.

---

89 The court relied on the US Supreme Court’s finding in Lakewood v. Plain Dealer Publishing Co. 486 U.S 750

90 The court observed that source code was utilized by computer programmers in the same way as mathematicians and economists used scientific data. The defendants did not directly challenge the fact that the source code was a form of expression, rather they maintained that it was not speech for the purpose of the First Amendment. The court rejected this argument on two grounds. Firstly, the court observed that the source code was not a direct command to the computer whereby it was instructed to perform certain functions. It was on the other hand directed at other programmers, and only once it was converted into object code could it be fed into the computer. Secondly, the court observed that the mere fact that the code had some functionality connected with it, could not result in it no longer being speech. Thus, the court basically followed the District Court in ruling that the programme was speech for the purpose of the First Amendment.
Coming to the issue of prior restraint, the court relied on the US Supreme Court’s decision in Freedman v. Maryland\textsuperscript{91}, where it was held that a prior restrain could be valid if it satisfied the three criteria of:

a) being for a limited duration of time,
b) providing for expeditious judicial review and
c) the burden of proof being shifted onto the censor to establish that the restriction was for a valid and necessary purpose.

The court observed that the procedure for restraint under the AECA and the ITAR did not meet any of these requirements. It did not provide for a fixed period of operation. It specifically barred any judicial review on the inclusion of items onto the USML. Consequentially, there could be no burden on the censoring authority to move the court to impose the restriction. The court observed that, in light of the discretion and the criteria not being met, the procedure was without any proper safeguards and was an invalid prior restraint on the individuals’ right to speech and expression under the First Amendment. The court concluded that the restriction placed on the expression of the software and the instructions to use the same were unconstitutional.

Of importance to the present discussion are the concluding remarks made by the court, which can be viewed as obiter dicta. The court observed that it’s decision was to be taken in specific and not as a general proposition. Thus, not all software would constitute expression. The court observed that if the restriction on the process of encryption had been specific in time, place and manner and neutral as to content, it might have been valid if for genuine purposes. The second and more important observation made by the court was that the government’s restriction affected more than the individual’s First Amendment rights.

The court observed that with the development of electronic communication and technology, individual privacy had become diluted gradually. The usage of encryption,

\textsuperscript{91} 380US.51
the court observed, was integral to the issue of privacy and the government’s policy could, therefore, be looked at as violative of the constitutionally guaranteed right to privacy\textsuperscript{92}. The court, however, took note of the fact that this issue, not being one that it was called to adjudicate upon, could only be decided upon at a future date. The court accordingly granted declaratory relief in favour of the plaintiff and struck down the sections of the AECA and the ITAR as unconstitutional. However, it refused to grant an injunction against the defendants from using the same, since it felt it unnecessary.

This case presented, for the first time, the legal and constitutional issues involved in the practices of encryption and cryptography. Several of the propositions laid down in this case are applicable mutatis mutandis in the Indian context too. Thus, for the purposes of Article 19(1)(a) of the Indian Constitution, encryption and cryptography can be looked at as implicit form of ‘…. Speech and expression’ contained therein. It can also be viewed as an integral part of the right to privacy said to flow from the right to life and personal liberty in Article 21. Any restriction on the same, however, will be permissible if it is a ‘procedure established by law’ and provided it is reasonable, right, just, fair and has the specific force of law. In the case of the right to freedom of speech and expression in Article 19(1)(a), it also must fall within one of the areas of permissible restriction on cryptography exists in the Indian context at present and whether it would be valid.

3.3 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.

\textsuperscript{92} The availability and use of secure encryption may offer an opportunity to reclaim some portion of the privacy we have lost. Government efforts to control encryption thus may well implicate not only the First Amendment rights of cryptographers intent on pushing the boundaries of their science, but also the constitutional rights of each of us as potential recipients of encryption’s bounty. Viewed from this perspective, the government’s efforts to retard progress in cryptography may implicate the Fourth Amendment, as well as the right to speak anonymously.
Section 72 of the Act, establishing an Information Technology Offence of “Breach of Confidentiality and Privacy” reads as under:

“72. Breach 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 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.
4. 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.

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 ciphers. 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." 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. 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

94 “Encryption basically involves running a readable message known as “plaintext” 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.D. Cal.1996)
96 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.”
fraud and ensuring authenticity. Thus, the primary purpose of encryption and cryptography remains: ensuring that messages transmitted remain secure from interference by third parties.

These subjects have 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. While cryptography may be looked at as essential to ensure privacy for communication, to the government it represents a legitimate security threat.

Any state agency, even 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

\[97\] This is by means of digital signatures

\[98\] 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

\[99\] “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.
kept away from those involved in activities prejudicial to the state’s security\textsuperscript{100}. 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.

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.

**4.1 RESTRICTIONS ON CRYPTOGRAPHY IN INDIA: THE 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\textsuperscript{101}, 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\textsuperscript{102}. 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

\textsuperscript{100} For instance, in India, under the Telegraph Act, 1885, the state is allowed to intercept information under certain specific conditions.


\textsuperscript{102} *Ibid*
‘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. 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-co-operation 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

---

103 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.”
necessarily arises, is whether the procedure under Section 69 is sufficient to thwart the right to privacy.

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. 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.*

**4.2 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, 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 at the other, is the more important issue of cryptography as an integral part of the right to privacy. 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 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.
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 re supreme to function, mere legislation in the absence of a political will, would be futile.\textsuperscript{106}

5. REGULATION MODELS

It is safe to assume that the privacy of individuals is certainly a concern of the law. Taking this as a given, we can go on to examine what the legal and policy response is and what it ought to be.

Fundamentally, there are various approaches that may be taken:

- Legislation
- Self-Regulation
- Reliance on Trustworthy Third Parties who will set and enforce standards

Most legal systems will be a mixture of these approaches, something that can easily be seen in the US.

5.1 The OECD Principles\textsuperscript{107}

The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Information were developed, way back in 1980, to help harmonise national privacy legislation and, at the same time, prevent interruptions in international flows of data. These principles still have much relevance today and can be guides for the direction that may be taken by states for privacy protection.

\textsuperscript{107} Privacy Online: OECD Guidance on Policy and Practice
http://www.oecd.org/document/49/0,3343,en_2649_34255_19216241_1_1_1_1,00.html
The Guidelines consist of 8 Basic Principles of National Application:

1. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. (The Collection Limitation Principle)

2. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date. (The Data Quality Principle)

3. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. (The Purpose Specification Principle)

4. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified except:
   a) with the consent of the data subject; or
   b) by the authority of law. (The Use Limitation Principle)

5. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data. (The Security Safeguards Principle)

6. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identify and usual residence of the data controller. (The Openness Principle)

7. 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
i) within a reasonable time;
ii) at a charge, if any, that is not excessive;
iii) in a reasonable manner; and
iv) in a form that is readily intelligible to him;

c) to be given reasons if a request made under sub-paragraphs (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.

(The Individual Participation Principle)

8. A data controller should be accountable for complying with measures which give effect to the principles stated above. (The Accountability Principle)

These principles have been set out by the OECD as guides for nations to legislate upon and achieve international harmony of principles. Have these been transformed into legal systems? What are the difficulties, the pulls and the pushes of legislating in the Information age? These are the matters this paper seeks to cover.

5.2 THE US POSITIONS

The Federal Trade Commission (FTC) has played a key role in the development of the response of the US federal legal system to the issue of information privacy. In 1998, it brought out a report \(^ {108} \), Privacy Online: A Report to Congress, which was the result of a three-year privacy initiative. The Report recognized four core principles of fair information practice:

\(^ {108} \text{Supta n 7.} \)
• Consumers must be given notice of an entity’s information practices; (The Notice/Awareness Principle)

• They must have a choice with respect to the use and dissemination of information; (The Choice/Consent Principle)

• They should have access to any information collected about them; (The Access/Participation Principle) and,

• Finally, consumers must have sufficient security from the data collector. (The Security/Integrity Principle)

It was acknowledged that these principles are essential to ensuring that user privacy interests are adequately protected.

5.2.1 Adults

As regards the personal information of adults, the FTC has suggested that self-regulation is the least intrusive and most efficient means to ensure fair information practices, given the rapidly evolving nature of the Internet and computer technology. The Commission believes that legislative intervention will not be justified at this stage.

Let us examine the validity of this approach of industry self-regulation.

It must be understood that a self-regulatory scheme will be effective only to the extent that businesses choose to become part of it. While there are a large number of businesses that are likely to get on to the bandwagon (either because they are already committed to responsible privacy practices or because they hope to gain some commercial advantage from doing so), a large number of businesses will be opposed to regulation, self-imposed or otherwise, when there is no sanction for breach. It is very optimistic to expect that all of them will participate in any scheme that provides more than mere window-dressing. Furthermore, those who might otherwise have been prepared to participate in an effective scheme may be deterred from doing so by the fact that they will be placed at a cost disadvantage in comparison to their less responsible competitors.¹⁰⁹

Another important consideration is that the absence of legal sanction will exist in the context of a culture where data protection is still regarded by many as a new-fangled notion, which is inimical to legitimate pursuit of profit. A purely voluntary scheme, without an effective oversight mechanism, is unlikely to generate the level of public confidence which is required to facilitate the growth of an embryonic electronic commerce industry and or to create and encourage the free flow of personal information\textsuperscript{110}.

Therefore, this approach is questionable on numerous counts.

5.2.2 Children
While suggesting self-regulation for protection of information privacy of adults, the FTC proposed a much more legalistic approach to the protection of data privacy of children under the age of 13. The US Congress duly obliged and today legislation is in place and is being implemented.

In October 1998, the Children’s Online Privacy Protection Act of 1998 (COPPA) was signed into law. The Act, passed by Congress just four months after the Commission’s 1998 Report, has been operative since April 21, 2000, and requires that operators of Web sites directed to children\textsuperscript{111} under 13 or who knowingly collect personal information from children under 13 on the Internet:

\begin{itemize}
  \item provide a notice on the web site of its information practices\textsuperscript{112};
\end{itemize}

\textsuperscript{110} Ibid
\textsuperscript{111} To determine whether a Web site is directed to children, the FTC considers several factors, including the subject matter; visual or audio content; the age of models on the site; language; whether advertising on the Web site is directed to children; information regarding the age of the actual or intended audience; and whether a site uses animated characters or other child-oriented features. See, “How to Comply With the Children’s Online Privacy Protection Rule” at <http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm>.
\textsuperscript{112} An operator must post a link to a notice of its information practices on the home page of its Web site or online service and at each area where it collects personal information from children. An operator of a general audience site with a separate children’s area must post a link to its notice on the home page of the children’s area. The notice must be clearly written and understandable; it should not include any unrelated or confusing materials. It must state the following information:
provide parents notice of their information practices;\textsuperscript{113} 

obtain prior, verifiable parental consent for the collection, use, and/or disclosure of personal information from children (with certain limited exceptions);\textsuperscript{114} 

give notice to parents before giving information to third parties;\textsuperscript{115}

- The name and contact information (address, telephone number and e-mail address) of all operators collecting or maintaining children’s personal information through the Web site or online service.

- The kinds of personal information collected from children (for example, name, address, e-mail address, hobbies, etc.) and how the information is collected — directly from the child or passively, say, through cookies.

- How the operator uses the personal information.

- Whether the operator discloses information collected from children to third parties. If so, the operator also must disclose the kinds of businesses in which the third parties are engaged; the general purposes for which the information is used; and whether the third parties have agreed to maintain the confidentiality and security of the information.

- That the parent has the option to agree to the collection and use of the child’s information without consenting to the disclosure of the information to third parties.

- That the operator may not require a child to disclose more information than is reasonably necessary to participate in an activity as a condition of participation.

- That the parent can review the child’s personal information, ask to have it deleted and refuse to allow any further collection or use of the child’s information. The notice also must state the procedures for the parent to follow. Ibid.

\textsuperscript{113} The notice to parents must contain the same information included on the notice on the Web site. In addition, an operator must notify a parent that it wishes to collect personal information from the child; that the parent’s consent is required for the collection, use and disclosure of the information; and how the parent can provide consent. The notice to parents must be written clearly and understandably, and must not contain any unrelated or confusing information. An operator may use any one of a number of methods to notify a parent, including sending an email message to the parent or a notice by postal mail. Ibid

\textsuperscript{114} Before collecting, using or disclosing personal information from a child, an operator must obtain verifiable parental consent from the child’s parent. This means an operator must make reasonable efforts (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child receives notice of the operator’s information practices and consents to those practices.

Until April 2002, the FTC will use a sliding scale approach to parental consent in which the required method of consent will vary based on how the operator uses the child’s personal information. That is, if the operator uses the information for internal purposes, a less rigorous method of consent is required. If the operator discloses the information to others, the situation presents greater dangers to children, and a more reliable method of consent is required. The sliding scale approach will sunset in April 2002 subject to a Commission review planned for October 2001.

\textsuperscript{115} An operator must give a parent the option to agree to the collection and use of the child’s personal information without agreeing to the disclosure of the information to third parties. However, when a parent agrees to the collection and use of their child’s personal information, the operator may release that information to others who use it solely to provide support for the internal operations of the website or service, including technical support and order fulfillment. Ibid.
• upon request, provide a parent with the ability to review the personal information collected from his/her child;
• provide a parent with the opportunity to prevent the further use of personal information that has already been collected, or the future collection of personal information from that child;
• allow parents to revoke their consent, and delete information collected from their children at the parent’s request;
• limit collection of personal information for a child’s online participation in a game, prize offer, or other activity to information that is reasonably necessary for the activity;
• establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal information collected; and
• get new consent when information practices change in a material way.\footnote{An operator is required to send a new notice and request for consent to parents if there are material changes in the collection, use or disclosure practices to which the parent had previously agreed. For example if the operator changes business, this is a material alteration and the personal information collected from a child cannot be used without taking parental consent once again. Ibid.}

As can be seen, these are strict and well defined rules. This does not mean that the approach to regulation of privacy of children’s personal data is purely legalistic. The COPPA also includes a safe harbour provision under which industry groups or others may seek FTC approval for self regulatory guidelines. Web site operators who participate in such approved programmes may be subject to the review and disciplinary procedures provided in those guidelines in lieu of formal FTC investigation and law enforcement. The safe harbour would serve both as an incentive for industry self-regulation, and as a means of ensuring that the Act’s protections are implemented in a manner sensitive to industry specific concerns and developments in technology. This is quite different from the purely self-regulatory approach with respect
to adults. Here, there is incentive to enter into self-regulatory arrangements, since a failure would result in the operator falling under the hammer of the law automatically.

5.2.3 Seal Programmes
An encouraging development in the US, for online privacy in general, is the emergence of online seal programmes. These programmes require their licensees to abide by codes of online information practices and to submit to various types of compliance monitoring in order to display a privacy seal on their Web sites. Seal programmes offer an easy way for consumers to identify Web sites that follow specified information practice principles, and for online businesses to demonstrate compliance with those principles. One example is TRUSTe, about which we can go into some detail.

TRUSTe, is an independent, non-profit organization and was the first online privacy seal programme. TRUSTe’s license agreement, which governs licensees’ collection and use of personally identifiable information, has taken a more comprehensive approach to privacy by requiring licensees to follow standards for notice, choice, access and security based upon the COPPA Guidelines
This method of bringing in a trustworthy third party is an innovative and positive step. Unfortunately, only a small minority of commercial Web sites has joined these programmes to date.\textsuperscript{117} This can be attributed, in a large part, to the absence of any sanction for failure to comply with basic principles of consumer privacy.

5.2.4 Future Action in the US
The FTC believes that the action plan towards data privacy, keeping the self-regulatory approach in mind, ought to be as follows:

- Educating operators — Specifically, the challenge is to educate those companies that still do not understand the importance of consumer privacy and to create incentives for further progress toward effective, widespread implementation.

\textsuperscript{117} The use of TRUSTe may be seen on the popular which quite obviously deals with huge amounts of personal information.
• Industry based initiatives — Industry groups must continue to encourage widespread adoption of fair information practices. For example, large corporates could undertake that they will forgo advertising on sites that do not adhere to fair information. This type of business-based initiative is critical to making self-regulation meaningful as it extends the reach of privacy protection to small and medium-sized businesses where there is great potential for e-commerce growth.

• Consumer education — Industry must work together with government and consumer groups to educate consumers about privacy protection on the Internet. The ultimate goal of such efforts, together with effective self-regulation, will be heightened consumer acceptance and confidence. Industry should also redouble its efforts to develop effective technology to provide consumers with tools they can use to safeguard their own privacy online.

It is possible that the criticisms of the self-regulatory approach expressed above may be overcome with an integrated approach of this nature.

5.3 Data protection in the UK

The UK has a much more legalistic approach to protection of personal data in general as compared to the US. The Data Protection Act, 1998 came into force recently, on the March 1, 2000. It lays down rules for processing personal information and applies to paper records as well as those held on computers. The Rules provide that anyone processing personal data must comply with the eight enforceable principles of good practice:

That data must be:
• fairly and lawfully processed;
• processed for limited purposes;
• adequate, relevant and not excessive;
• accurate;
• not kept longer than necessary;
• processed in accordance with the data subject’s rights;
• secure;
• not transferred to countries without adequate protection.\textsuperscript{118}

6. THREAT TO PRIVACY:
The Internet is a rich source of information about online net user. Web sites collect much personal information both explicitly, through registration pages, survey forms, order forms, and online contests, and by using software in ways that are not obvious to online consumers\textsuperscript{119}. Through cookies and tracking software, Web site owners are also able to follow consumers, online activities and gather information about their personal interests and preferences. Computers linked together by high speed networks with advanced processing systems can create comprehensive dossiers on any person without the need for a single central computer system. New technologies developed by the defense industry are spreading into law enforcement, civilian agencies, and private companies.\textsuperscript{120}

While many of the uses to which this information is now put were theoretically impossible in earlier days, technological constraints made their application not only difficult but also prohibitively expensive. Today the scenario is such\textsuperscript{121} that it is not only possible but also commercially attractive for businesses to conduct surveillance on a large scale as they discover that there are more and more new ways in which they can use personal information to gain advantage in the marketplace\textsuperscript{122}. The data collected proves extremely valuable to businesses because not only is it possible for them to target market products and services that are increasingly tailored to their visitors’ interests, but also permits them to boost their revenues by selling advertising space on their Web sites\textsuperscript{123}. It emerged to mark a variety of software products designed to assist Web sites in collecting and analyzing visitor data and in serving targeted advertising.

\begin{flushright}
\textsuperscript{118} This is an interesting provision, similar to many others present in other European countries. It would be interesting to know whether the US would fall under this category.
\textsuperscript{119} Moira Peterson, ”Privacy protection in Australia :The need for an effective Private Sector Regime “
\textsuperscript{120} Snell, Jason. Macworld. (Dec. 1997) ”The wrong side of the Net.” (Internet privacy concerns) (net User) (Internet/Web/Online Services Information,v14 n12 p189
\textsuperscript{121} A major difference today is that information can be generated indirectly at very low cast and its significance is not fully understood by data subject .
\textsuperscript{122} How Halifax (May 1999), plc is preparing to comply with the new Act. Privacy Laws and Business , 48,14-16.
\textsuperscript{123} Ibid
\end{flushright}
A computer operator with access to electronic information data banks can quickly and easily rearrange facts, incorporate new material, compile multiple databases and make other transformations of information. Whether one has the right to do so is a question of law and legal policy, but the medium supplies the capability. Technology development has to be considered as a double-edged sword in its application to the privacy and security fields. While ICT technologies are used for the delivering new services or enhancing existing service, they can simultaneously create new risk for privacy. These technologies are not originally conceived for such purpose, provide powerful tools to the different players to commit privacy invasive abuses.

Examples of such technologies are: 1) Internet data interception and tracing technologies (2) Cookies (3) Profiling based on data collection and data mining technologies (4) Record linkage (5) Surveillance camera technologies (6) Mobile phone digital cameras (7) Web cameras in private or public space (8) Mobile communication technologies in combination with user location computation technologies (including those that are Satellite based such GPS (9) Smart tag or Radio frequency identity (RFID) (10) Biometric technologies.

Internet user may feel manipulated by these practices or complain that their privacy has been invaded. Unfortunately, though, these individuals may be victims without legal recourse. Most cases involving privacy rights that empower an individual to control the use and discourse of personal information rest on statutory, as opposed to common law, authority, and involve information held by the government.

---

125 Ibid at 108. See Eric D. Randall, Marketers Kill Corporate Creativity, USA Today, Nov. 9, 1992, at 5B.
129 Willis Ware, Lessons for the Future: Dimensions of Medical Record Keeping, in Health Records: Social Needs and Personal Privacy 43 (Task Force on Privacy, U.S. Department of Health and Human Services (1993)).
130 George B. Trubow, (1990),Protecting Informational Privacy in the Information Society, 10 N. Ill. U. L. Rev. 521, 521
131 “A development of the 1970's, was spawned by the remarkably constant improvement and growing pervasiveness of the digital computer and electronic data banks.”

Nimmer & Krauthaus, supra 138, at 123.
It is not surprising that only about 25\%\(^{132}\) of Internet users go beyond merely browsing\(^{133}\) for information to actually purchasing goods and services online, acts which require them to give out personal information.\(^{134}\) This position does say a lot – businesses have as great a stake in protecting this private information as individuals do and online business will thrive only when there is trust in business practices and the electronic environment\(^{135}\). Therefore, user upset with the exploitation of personal information by the private sector are forced to look to the common law. The tort of invasion of privacy through the publication of private facts may provide an answer\(^{136}\). Obviously, the privacy issues, which arise in this scenario are different not only in scale but also in their nature from those that arose in the past.

6.2 NATIONAL SECURITY AND PRIVACY:

The security /privacy balance was affected even before September 11,2001 . There are widespread violations of laws relating to surveillance of communications, even in the most democratic of countries. The U.S. State Department's annual review of human rights violations finds that over 90 countries engage in illegally monitoring the communications of political opponents, human rights workers, journalists and labor organizers\(^{137}\). In France, a government commission estimated in 1996 that there were over 100,000 wiretaps conducted by private parties, many on behalf of government agencies\(^{138}\).


\(^{134}\) This does not imply that personal information can not be collected by sites when there is mere browsing..


\(^{136}\) See, Trubow, supra note 144, at 7. Furthermore, [a] compelling argument can be made that a collection of personal information sold as a dossier or profile violates the appropriation [of name, likeness or personality] tort as ‘appropriation of some element of the plaintiff's personality for commercial use. When dossiers and profiles maintained by credit bureaus and other such agencies are sold, the subject's personality is certainly being used for a commercial purpose.


\(^{138}\) supra note 21
Japan, police were recently fined 2.5 million yen for illegally wiretapping members of the Communist party\textsuperscript{139}.

The United Nations took immediate action right after the attacks, September 11, 2001, and adopted on September 12, 2001, UN Resolution 1368 that calls for increased cooperation between countries to suppress and prevent terrorism\textsuperscript{140}. The Committee of Ministers of the Council of Europe issued a similar declaration, and the North Atlantic Treaty Organization reasserted its own Article 5, which declares that an attack on any NATO nation constitutes an attack on all\textsuperscript{141}.

Along these latter lines, the Organization for Economic Co-operation and Development together with the G-7, and European Commission called for an extension of its mandate to act against terrorist financing\textsuperscript{142}. Looking at the Internet, the European Commission went so far as to consider a requirement that every European Union member nation pass laws making cyber attacks a terrorist offense\textsuperscript{143}.

The United Kingdom passed a law permitting the retention of data for law enforcement purposes in contravention to existing data protection rules\textsuperscript{144}. The United States passed a number of laws, including the USA-PATRIOT Act\textsuperscript{145}, which increases surveillance powers and minimizes oversight and due process requirements.

Since independence, India has numerous preventive laws such as MISA, TADA and POTA (which was scraped only in the third week of Sept 2004) authorizes the national security agencies to perform interception of communications, search and seizure in a arbitrary manner.

\textsuperscript{139} Wire tapping http://www.epic.org/privacy/wiretap/

\textsuperscript{140} UN Security Council Resolution 1368 (2001) September 12, 2001

\textsuperscript{141} Justice Elizabeth Evatt AC, Dr Keith Suter, Nicole Abadee, Nick McNally, European Journals of International Law Posted on November 07, 2001 at 23:57:
http://www.ejil.org/forum_WTC/messages/17.html

\textsuperscript{142} Europa (15 Oct. 2001) Action by the European Union following the attacks on 11 September
MEMO/01/327 - Brussels, http://europa.eu.int/comm/external_relations/cfsp/news/me01_327.htm In accordance with the Plan of Action adopted by the Extraordinary European Council held in Brussels on 21 September, it has set in train a series of measures in those areas where it must and can make an effective contribution

\textsuperscript{143} Ibid


\textsuperscript{145} EPIC The USA PATRIOT Act http://www.epic.org/privacy/terrorism/usapatriot/
Almost every country that changed its laws to reflect the changed environment, increased the ability of law enforcement and national security agencies to perform interception of communications, and transformed the powers of search and seizure, and an increase in the type of data that can be accessed\textsuperscript{146}.

If government is hell-bent on assembling and mining massive databases of our credit card purchases, car rentals, library books, airline ticket purchases, and so on, then banks, airlines, hotels, Internet service providers, and other private businesses we deal with have no choice but to routinely transfer our private information to the government against our wishes\textsuperscript{147}. They cannot promise to safeguard our privacy as they otherwise could.

But inherently "invasive" technologies like these can threaten fundamental values of privacy and liberty if misused. No one wants to be treated like a human bar code by the authorities, or monitored around the clock by the Homeland Security Department. Thus, we need a framework by which to distinguish appropriate and inappropriate uses or surveillance-enabling technologies\textsuperscript{148}.

Thus, government must not have access to our private information without going through the appropriate legal process\textsuperscript{149}.

**6.2 International Standards**

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


\textsuperscript{149} The US Supreme Court developed a doctrine known as 'substantive due process' that extended constitutional protection over some types of personal behaviour. This doctrine served as the basis for the constitutional right to privacy. The due process clauses in the fifth and fourteenth amendments barred the government from depriving any person of life, liberty or property without due process of law.
have established a higher barrier so that companies cannot routinely trade databases and
cannot get involved in the wholesale invasion of personal privacy.

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.

8. CONCLUSION

The current situation is that, despite the existence of the legislative framework and the
efforts of national and international data protection authorities and bodies, privacy abuse
continues on a vast and persistent scale. This paper notes the widening gap between the
privacy protection and practice exploiting the use of personal data and suggest that this is
due in part to problems of enforcement of the legislation because current legislation
doesn’t take sufficient account of the huge growth in on line information system and
service. Personal data no longer resides in a controlled environment of well define
monolithic databases, but is increasingly dispersed in networks across organization and
frontiers.

In this context, it is fair to say that no generally applicable norms specifying standards to
determine privacy infringement will be found globally acceptable. This is a reality that
must be faced. In many countries like India, laws have not kept up with the technology,
leaving significant gaps in protections. Finally, in the absence of adequate enforcement,
the mere presence of a law may not provide adequate protection. Our challenge is to
integrate computer technology and human values in such a way that the technology
advances and protects those values rather than doing damage to them.

Figuring out what the safeguards ought to be, and where our zone of privacy actually lies,
is a matter of policy, law, and ultimately, social norms”. Legal and social questions have
to be dealt with to allow individuals to have a say in what information is collected about

150 Thomas B. Riley
Douglas Kellner, PRIVACY AS A HUMAN RIGHT - THE WAVE OF THE FUTURE
University of Texas at Austin http://www.gseis.ucla.edu/courses/ed253a/dk/INFO1.htm
from the issue of PC World magazine, http://www.pcworld.com/resource/article/0,aid,68769,00.asp
152 European Union Annual Report on Human Rights - 2001 Luxembourg, 8 October 2001 -
York: St. Martin's Press.
them and how that information is going to be used. This concern about privacy is part of a larger concern about control, about people having control over their own lives. Anyhow, future technologies with still unknown potential, and bearing risks for the liberty of the individual, should be dealt with in the light of a ‘precautionary’ approach (a process that includes information gathering, broad consultation, participative procedures of decision-making, etc.

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. All these developments suggest a need for an International Privacy Rights Bill. It is essential that such an instrument be agreed upon as a defense against the darker forces of technology that could erode our basic democratic rights.

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.
Bibliography:

Books

2. Edward F. Dolan Your Privacy: Protecting It in a Nosy World Publisher: Cobblehill; (February 1995)
9. Philip E. Agre (Editor), Marc Rotenberg (Editor) Technology and Privacy: The New LandscapePublisher: MIT Press; Reprint edition (July 3, 1998)
12. Raymond Wacks ,Law, Morality, and the Private Domain, Published 2000 Hong Kong UniversityPress
23. Michael J. Quinn Ethics for the Information Age , Published 2005 Pearson/Addison-Wesley
28. Colin J. Bennett, Rebecca Grant, Vision of Privacy: Policy Choices for the Digital Age, University of Toronto Press, Toronto, Ont. Canada 1999
32. S Saxby (Ed), The Encyclopaedia of Information Technology Law, Sweet and Maxwell, 1990
34. I Lloyd, Information Technology Law, Butterworths, 1993

Articles

7. ThirdAge Media. "Fight for Your Privacy."  
10. By John GeralsUS e-surveillance worries privacy groups, vnunet.com, in Silicon  
11. Thomas B. RileyDouglas Kellner PRIVACY AS A HUMAN RIGHT - THE  
    WAVE OF THE FUTURE University of Texas at Austin  
   http://www.gseis.ucla.edu/courses/ed253a/dk/INFO1.htm
12. Bruce Hoffman and Peter Chalk  
    with Timothy E. Liston and David W. Brannan, Security in the Nation's Capital  
    and the Closure of Pennsylvania Avenue: An Assessment 2002  
   http://www.rand.org/publications/MR/MR1293-1/
    the Nation's, Esq ,2002 http://www.rand.org/publications/CT/CT194/
14. Privacy act, security market, surveillance camera, anonymous proxy web  
   http://www.exclassics.org/national_security_agency.html
15. SECURITY, TECHNOLOGY, AND PRIVACY: SHAPING A 21ST CENTURY  
    PUBLIC INFORMATION POLICY , GEORGETOWN LAW  
   http://www.law.georgetown.edu/webcast/eventDetail.cfm?eventID=12
17. Gail Repsher EmeryReport card: Agencies improve, but cyber security efforts  
    fall short Washington Technology Staff Writer 12/09/03  
   http://www.washingtontechnology.com/news/1_1/security/22296-1.htm
18. fcw.com Data mining aims at national security BY Dan Caterinicchia March 4,  
19. pcworld.com Consumer Watch: National Security vs. Online Privacy From the  
    January 2002 issue of PC World magazine  
   http://www.pcworld.com/resource/article/0,aid,68769,00.asp
20. DR. LARRY PONEMON ETHICS & PRIVACY ,Case Study: National Security  
    vs. Student PrivacyHow one CIO might have handled a privacy breach — and  
    how he might have saved his job.  
   http://www.darwinmag.com/read/120103/privacy.html
   http://www.privacyinternational.org/survey/phr2003/threats.htm#Beyond%20Sept  
   ember%202001%2020001
    Privacy International  
23. Counter-Terrorism Proposals, Electronic Privacy Information Center,  
   http://www.epic.org/privacy/terrorism/usapatriot/
24. What is the Computer Ethics  
   http://66.102.11.104/search?q=cache:w4tJ72PDHI4J:www.blackwellpublishing.c  
   om/content/BPL_Images/Content_store/Sample_chapter/1855548445%25CCEA

26. Privacy perspective from utilitarianism and metaphysical theories Current security management & Ethical issues of information technology Year of Publication: 2003


34. T Forester and P Morrison, Computer Unreliability and Social Vulnerability, 1990 Futures


45. 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]

46. EU/US Data Privacy Pact Continues To Ebb 04/06/00.
   Newsbytes News Network, April 6, 2000, by Sylvia Dennis
   [http://www.findarticles.com/cf_dls/m0NEW/2000_April_6/61411406/p1/article.jhtml]

47. The National Academy of Public Administration Health-Care Surveillance Must Balance Privacy, Security , Nov.02
   [http://www.napawash.org/pc_local_state/innovations/innovations_Nov02.html]
   By Gail C. Christopher, Executive Director, Institute for Government Innovation at Harvard University's John F. Kennedy School of Government & Robert J. O'Neill, Jr., President, National Academy of Public Administration

   [http://www.gsu.edu/~lawppw/lawand.papers/dbessho.html]


50. Does the Constitution Contain a Right to Privacy? by Harry Browne May 9, 2003
    [http://www.harrybrowne.org/articles/PrivacyRight.htm]

    [http://emoglen.law.columbia.edu/CPC/archive/terror//07HOME.html]


53. Technology cyber times November 23, 1997VIEWPOINT / By AMITAI ETZIONI .Some Privacy Please, for E-Mail

54. Human Rights In Islam; by AA Maududi published by The Institute of Islamic Information and Education
    [http://www.usc.edu/dept/MSA/humanrelations/humanrights/]

55. Willis Ware, Lessons for the Future: Dimensions of Medical Record Keeping, in Health Records: Social Needs and Personal Privacy 43 (Task Force on Privacy, U.S. Department of Health and Human Services (1993)).

Journals/ News

2. 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)
10. EU gives America access to airline passenger details By Stephen Castle18 December 2003 http://news.independent.co.uk/world/americas/story.jsp?story=474274
12. EPIC Poverty and Privacy http://www.epic.org/privacy/poverty/
27. Dan Verton, Congress man Say Data Mining Could Have Prevented 9-11, Computerworld, August 26, 2002  
   http://www.computerworld.com/governmenttopics/government/policy/story/0, 10801,73773,00.html
28. Access to Indian Parliament by RFID Wednesday, July 21 2004  

Reports

3. European Union Annual Report on Human Rights - 2001 Luxembourg, 8 October 2001 -  
   http://www.rand.org/natsec_area/products/privconf.html
   Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions Toronto, Canada Pages: 69 - 72 Year of Publication: 2000

Statutes

7. USA PATRIOT Act
12. The Indian Information Technology Act 2000