A STUDY ON RIGHT TO PRIVACY AND DATA PROTECTION IN THE CYBER SPACE[1]

KUMAR N H

Assistant Professor

Law Vidyodaya Law College, Tumakuru, Karnataka

"The Internet is a wonderful system but it has some problems. One of the most serious problems is hackers, people who know a lot about computers and use this to get into other people's computer systems. Loss of privacy is another major worry where the network is concerned". - **Bill Gates**

ABSTRACT

In the Information Technology World as the usage of computers became more and more popular, there is an expansion in the growth of technology as well, and the term 'Cyber' became more familiar to the people. The evolution of Information Technology (IT) gave birth to the cyberspace, wherein internet provides equal opportunities to all the people to access information, data storage, analyse etc. Due to the increase in the number of netizens, misuse of the technology in the cyberspace was clutching up which gave birth to cyber crimes. This research paper deals with all the relevant aspects towards the best protection of data as well as privacy of the individuals in a cyberspace and best use of the technology with the help of legislative initiation.

Key words: Right to Privacy, Data Protection, Cyberspace, IT Act, Constitution of India.

INTRODUCTION

The Right to Privacy is one of the inalienable human rights enjoyed by every human being as a part of their right to life without any persons' intervention. Data of every individual are the part of their privacy, which prohibits others to intervene. Privacy and Data are the two faces of the same coin. Today, we are all living in the Information Technology era and the technology helps us in all the fields of our day today activities. It is because of this Information Technology with Cyberspace or Internet, today it is proved that the whole 'Globe is just like a Village'. Jurisdiction of the Cyberspace is the whole World. Our tangible paper documents and information, visible data are converted into intangible material and uploaded and stored in cyberspace. In this speedy growth of Information Technology, violation of the individuals' privacy right is very easy and quite common, and it has been creates a fear in the minds of the people, that, on what extent personal and individual data are safe and how law working towards the best protection of the right to privacy and data protection.

[1] KUMARA. N. H., Assistant Professor of Law, Vidyodaya Law College, Tumakuru, Karnataka.

CONCEPT OF PRIVACY

The word 'Privacy' is derived from Latin word 'privus' meaning 'single, separated or deprived from the rest, solitude'.[2] The concept of privacy is not uniform around the Globe due to various reasons such as historical, cultural and religious beliefs and practices resulting to different value system in the societies.

The term 'privacy' has been described as the rightful claim of the individual to determine the extent to which he wishes to share of himself with others and his control over the time, place and circumstances to communicate with others. It means his right to withdraw or to participate as he/she sees fit. It also means the individuals' right to control dissemination of information about himself, it is his own personal possession. Privacy has also been defined as a zero-relationship between two or more persons in the sense that there is no interaction or communication between them, if they so choose. Numerous legal and moral philosophers have suggested that privacy is valued because it satisfies a number of primary human needs.[3] In a historical sense privacy is a civil liberty essential to individual freedom and dignity. The right to privacy is the hallmark of a cultured existence, as in the word of Louise Brandeis, J. "The right most valued by civilized men". Winfield has referred to the right to privacy as the absence of unauthorized interference with a person's speculation of himself or his property from the public.[4] The Right to privacy is the "right to be let alone", and focused on protecting individuals.[5]

Hirshleifer emphasise that the concept of privacy is not to be misunderstood as idea of secrecy. Rather the concept might be described as autonomy within society. It is broader concept than secrecy. It reflects the particular kind of social structure together with supporting social ethics.[6]

The concept of Privacy has been recognised as human rights in various International Conventions like Universal Declaration of Human Rights,[7] International Covenant on Civil and Political Rights,[8]European Human Right Convention,[9] Inter-American Convention on Human Rights.[10]

RIGHT TO PRIVACY AS A FUNDAMENTAL RIGHT

Right to privacy has not been enumerated as Fundamental Rights in Part III of the Indian Constitution. 'Privacy' is not a subject matter of any of the three lists in Schedule VII of the Constitution of India. Therefore

[2] Jack Hirshleifer, 'Privacy: Its Origin, Function and Future', Available at: <http://www.econ.ucla.edu/workingpapers/wp166.pdf >Accessed on 01 May, 2018.
[3] V.D Dudje, Information Technology and Cyber Laws, 2004 Edition, P-7.
[4] Simon Davies, Unprincipled Privacy, University of New South Wales Law Journal, Volume 24, P-284.
[5] Warren and Brandeis, 'The Right to Privacy', (1890) Harvard Law Review, IV(5).
[6] See Supra Note at 2.
[7]Article 12: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.
[8] Article 17(1): No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Article 17 (2): Everyone has the right to the protection of the law against such interference or attacks.
[9] Article 8: Right to respect for private and family life: (1) everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
[10] Article 11: Right to Privacy 1.Everyone has the right to have his honor respected and his dignity recognized. 2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation. 3. Everyone has the right to the protection of the law against such interference or attacks.

it will come under entry 97 of List I (Union List). It states: "any other matter not enumerated in List II (State List) and List III (Concurrent List) ……." Thus only the Parliament is competent to legislate on privacy since it can be interpreted as any other matter not enumerated in List II and List III.

'Right to Life and Personal Liberty' under Article 21 of the Constitution protects the Right to Privacy of the individuals as a Fundamental Right. Article 19(1)(a) provides the Right to Freedom of Speech and Expression, which implies that a person is free to express his will about certain things within the limits.

The Supreme Court in Kharak Singh v. State of Uttar Pradesh case,[11] uphold the right to privacy as a 'common law right of citizens to enjoy the liberty of their houses'. In the words of SUBBA RAO, J.,: "Further, the right to personal liberty takes in not only a right to be free from restrictions placed on his movements, but also free from encroachment on his private life. It is true our constitution does not expressly declare a right to privacy as a Fundamental Right, but the said right is an essential ingredient of personal liberty. Every democratic country sanctifies domestic life...."[12]

Further, in the case of Govind v. State of Madhya Pradesh,[13] it was more incline to consider the right to privacy as fundamental right. It is reflected in the opinion of MATHEW, J., that; "Rights and freedoms of citizens are set forth in the Constitution in order to guarantee that the individual, his personality and those things stamped with his personality shall be free from official interference except where a reasonable basis for the intrusion exists. … in this sense, many of the fundamental rights of citizens can be described as contributing to the right to privacy".[14]

The emergence of new rights to privacy as the fundamental right created conflict between the fundamental right to free speech and expression and fundamental right to privacy. The court resolved or balanced the rights in case of R. Rajagopal v. State of Tamil Nadu.[15] The Supreme Court held, it is "implicit in the right to life and liberty guaranteed to the citizens" of this country by Article 21. It is a "right to be let alone." A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child bearing and education among other matters.[16]

In the case of Mr. X v. Hospital Z[17] the Apex Court continued to balance the conflict by recognizing that the medical records are generally considered to be private information of the individual. This right is subject to exception in the case where the non discloser of medical information could endanger the lives of other citizens.

Further, in the case of People's Union for Civil Liberties v. Union of India,[18] the Supreme Court held that Telephone tapping without the proper safeguards in terms of proper procedure established by law is in violation and invasion of individual's right to privacy. The Apex court in this case ordered the creation of a review

[11] (1964) 1 SCR 332, 333, 349, 351 (SB): AIR 1963 SC 1295: See also Wolf v. Colorado, (1049) 338 US 25
[12] M.P.Jain, Indian Constitutional Law, Sixth Edition, 2011, P-1236
[13] (1975) 2 SCC 148, 157-158: AIR 1975 SC 1378.
[14] See Supra Note at 12.
[15] AIR 1995 SC 264: (1994) 6 SCC 632.
[16] See Supra Note at 12, P-1237.
[17] AIR 1999 SC 495.
[18] (1997) 1 SCC 30: AIR 1997 SC 568.

committee to review all surveillance measure authorized under the Act. The court ordered that the procedure has to be tested on the ground of Article 14, 19, 21.

Further, in case of District Registrar and Collector v. Canara Bank,[19] the Apex Court ruled that the right to privacy exists and any unlawful invasion of privacy would make the offender liable to consequences as per law. The constitutional recognition of this right protects the privacy issue of individuals against the unlawful government invasion. Though right to privacy is not an absolute right and may lawfully restricted for the public order i.e., prevention of crime, disorder, protection of health, morals, protection of rights and freedom of others.

In Justice K.S.Pttaswamy (Retd) and Anr v. UOI and Ors,[20] the Supreme Court declares 'privacy to be a fundamental right', and the Supreme Court has overruled the verdicts given in the M.P.Sharma case in 1958 and the Khark Singh case. In this case Dr. D. Y. CHANDRACHUD, J., held that the right to privacy is "protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution."

CONCEPT OF INFORMATION TECHNOLOGY AND CYBER SPACE

The technology relating to computer system[21], their hardware, software and network, internet, and various applications running on the internet, is broadly referred to as Information Technology.

The Oxford Dictionary defines 'Information Technology' as: "The study or use of computers [22], telecommunication systems, and other devices for storing, retrieving and transmitting information."[23]

The virtual space in which all of IT-mediated communication and action are taking place is often referred to as 'Cyber Space'. Cyber Space cannot be spatially located; it has no geographical boundaries. It is made up intangible objects, such as your website, blog, social networks, email accounts, personal information and reputation. Cyberspace can be thought of as a global electronic village with instantaneous communication and no geographical barriers.[24]

CONCEPT OF DATA

The Cambridge English Dictionary defines 'Data' as information[25] in the form of facts or numbers, collected and examined scientifically to be used for the decision making. At computer age it is information in electronic

[19] (2005) 1 SCC 496.
[20] (2017) 10 SCC 1
[21] Sec. 2(l) of IT Act, 2000, define "computer system " means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;
[22] Sec 2(i) of IT Act, 2000, define "computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;
[23] Anirudh Rastogi, Cyber Law-Law of Information Technology and Internet, P-1.
[24] Ibid, P-2.
[25] Sec 2(v) of IT Act, 2000, define "information" includes [data, message, text,] images, sound, voice, codes, computer programmes, software and data-bases or micro film or computer generated micro fiche;

form[26] that is in stored and used by the computer with the help of sophisticated software to analyse a situation and take decision.

The IT Act 2000 under Section 2(1)(o) defines "Data means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer."

The Data Protection Rules[27] defines the 'Personal Information' as it is any information of natural person, which is capable of identifying that person directly or indirectly with the help of other information available or likely available to body corporate.

The Rules[28] defines the 'Sensitive Personal Data or Information' of a person as such personal information which consists of information relating to:

- ✓ Password;
- ✓ Financial information such as Bank account or credit card or debit card or other payment instrument details;
- ✓ Physical, physiological and mental health condition;
- ✓ Sexual orientation;
- ✓ Medical records and history;
- ✓ Biometric information;
- ✓ Any detail relating to the above clauses as provided to body corporate for providing service; and
- ✓ Any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise

Provided that, any information that is freely available or accessible in public domain or furnished under any law for the time being in force shall not be regarded as sensitive personal data or information.

As defined under Iceland Data Protection Act[29] 'Personal data' means, Any data relating to the data subject (identified or identifiable), i.e. information that can be traced directly or indirectly to a specific individual, deceased or living.

'Sensitive personal data' means data on origin, skin colour, race, political opinions, religious beliefs and other life philosophies; data on whether a man has been suspected of, indicted for, prosecuted for or convicted of a punishable offence; health data, including genetic data and data on use of alcohol, medical drugs and narcotics; data concerning sex life (and sexual behaviour); and data on trade-union membership.[30]

[26] Sec 2(r) of IT Act 2000, define "electronic form " with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;
[27] Sec 2(i) of The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[28] Ibid, Sec 3.
[29] Act No 77/2000 on the Protection and Processing of Personal Data ('Data Protection Act'), which implemented EU Data Protection Directive 95/46/EC Available at: <http://www.dlapiperdataprotection.com>, Accessed on 01 May,18.
[30] Ibid.

Key elements of 'Data':[31]

i. It is a representation of information, knowledge, fact, concept or instructions;
ii. The preparation of such representation is being done or has been done in formalised manner;
iii. Such representations are intended to be, are being or have been processed in a computer system or computer network; and
iv. Such representations may be in any form or stored internally in the memory of the computer.

The following points should be noted with reference to the term 'Data':[32]

i. Data constitutes a 'Computer resource' under Sec 2(1)(k)[33], an 'Electronic record' under Sec 2(1)(t)[34], and 'Information' under Sec 2(1)(v)[35] of the IT Act.
ii. Controller[36] may, under Sec 29 of the IT Act, access Data in a computer system for the purpose of investigating into a suspected contravention.
iii. Unauthorized downloading, copying and extracting of Data is a contravention under Sec 43(b) and an offence under Sec 66 of the IT Act, if, committed with a dishonest or fraudulent intention.
iv. Unauthorized damage to Data is a contravention under Sec 43(d), and an offence under Sec 66 of the IT Act, if, committed with a dishonest of fraudulent intention.
v. Sec 43 of the IT Act recognizes the existence of a 'Computer virus' in the form of Data.
vi. The act of obtaining unauthorized access to certain restricted Data may constitute an offence of 'Cyber terrorism' under Sec 66F of the IT Act.

PRIVACY AND DATA PROTECTION

Privacy and Data protection are not similar concepts, though they share some common features. They are just like twins, but not identical. Data protection does not raise privacy issues and not prohibitive if they are legitimately processed as per the directions of appropriate authorities. The scope of data protection is narrow as well as broad than privacy as both concepts aim to protect partially the rights and values of others. Though privacy is the starting point to identify and determine the principles of data protection. Privacy rights are personal rights whereas data protection has proprietary value also.

Privacy and data protection require that information about individuals should not be automatically made available to other individuals and organisations. Each person must be able to exercise a substantial degree of control over that data and its use. Data protection is legal safeguard to prevent misuse of information about individual person on a medium including computers. It is adoption of administrative, technical, or physical deterrents to safeguard personal data.

[31] Supra at 22, P-74.
[32] Ibid, P-75.
[33] "computer resource " means computer, computer system, computer network, data, computer data-base or software;
[34] "electronic record " means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;
[35] Supra at 24.
[36] Sec 2(m) of IT Act, 2000, define "Controller " means the Controller of Certifying Authorities appointed under sub-section (7) of section 17;

Privacy is closely connected to data protection. An individual's data like his name, address, telephone numbers, profession, family, choices, etc. are often available at various places like schools, colleges, banks, directories, surveys and on various websites. Passing of such information to interested parties can lead to intrusion in privacy like incessant marketing calls.

Privacy Invading Technology:

The technological innovations are eroding the roots of the privacy rights. The privacy invading technology may be the following:

1. **GUID – Globally Unique Identifier:** This is software that is embedded in the computer's hardware which helps in eavesdropping of all the computers connected through LAN (Local Area Network).
2. **E-mail and document bugs:** This technology helps to unveil and know whether the recipient has read the addressed e-mail or document.
3. **Online digital profiling:** International online advertising companies inserts advertisements on web pages with cookies tagged on them. If it is once clicked it will start building up the user's profile as he moves from one site to another. This is how the advertising companies, known as profilers builds a comprehensive profile of the user's surfing habits.
4. **Cookies:** An individual browsing the web leaves electronic trials wherever he or she passes. The software program known as the 'cookie' may be transmitted from a website to the user's computer and remain there until the site is next accessed, at which time details of the user and his/her previous visits to the site will be automatically transmitted.
5. **Spy ware:** Spy ware refers to programs used to log virtually anything that a user does on the computer. This spy ware program records all things without the user's knowledge. These programs can record key stokes, website visits, programmes run, internet connections, instant messages, incoming and outgoing e-mails, chat conversations passwords entered, windows viewed, filed and documents accessed and screenshots of the computer desktop.
6. **Cameras:** Digital cameras are small and cheap, there is no need to buy film, unwanted photographs can be deleted, and thousands of images can be easily stored on a computer and with use of the internet and photographs can be shared with other people, throughout the globe. At the same time, the video camera can do incredible damage. As the cameras are so small, people are more likely to carry cameras with them at all times. Again as there is no need for film, it does not cost anything to snap picture after picture.
7. **Web-bugs:** A web-bug, also known as a web beacon, is a file object that is placed on a web page or in an e-mail message to monitor user behaviour, functions as a kind of spy ware.
8. **Carnivore:** Carnivore is a tangible, portable device, tantamount to a phone tap that acts as a 'sniffer' allowing the investigation Bureau to intercept and collect criminal suspect e-mail without their knowledge or consent.

9. **Echelon:** Unlike carnivore, which simply monitors ISP traffic, echelon is rumored to be capable of scrutinizing telephone cells, faxes and any other communications that occur through the airwaves. Echelon uses advanced voice recognition and data modeling software and it is capable of processing massive amounts of data.
10. **RFID – Radio Frequency Identification Technology:** This simply yet remarkable technology consists of a small microchip, a protective sheath or container and a miniature embedded antenna, these components taken together are referred to as RFID tags. These are quite small, now just the size of a grain of rice. RFID has been used to monitor everything from commercial purchases, to the physical movements of government officials and to the misadventures of naturally curious children.
11. **Biometrics technology:** Biometrics is the term used for many ways that we humans can be identified by unique aspects of our bodies. Finger prints are the most commonly known biometric identifier. Other biometric identifiers are hand prints, vein dimensions, body, the way that we walk, our voices.
12. **Video voyeurism:** A new phenomenon of 'video voyeurism' has emerged in recent times where images of private area of an individual are captured without his knowledge and then widely transmitted without this consent. Thus, video voyeurism has been a piracy night mare.[37]

INFORMATION TECHNOLOGY ACT

The IT Act is the first legislation which came into force in the year 2000 and is the only Act which covers the key issues of data protection, albeit not every matter. The IT Act 2000 (Amendment 2008) (IT Act) provides civil and criminal remedy in case of any violation relating to data protection.

Section 43 of the Act lays down specifically various kinds of acts committed by any person who without the prior permission of the owner or in charge of the computer, computer system or computer network[38] does any of the following activities having potential to affect directly or indirectly the issue of privacy and data protection. The Section impose penalty by way of compensation on any such person. The various acts enumerated under the Section are as follows;

a) Accesses or secure access to any computer, computer system or network or computer resource,[39]
b) Downloads, copies or extracts any data, computer data or information including any information stored in removable storage medium,[40]
c) Introduces or causes to introduce any computer contaminants like computer virus into any computer system,[41]
d) Damages or cause to damage any computer, computer system or computer network, data or computer data base or any other programme,[42]

[37] Griffin S Dunham, Journal of Cyber Law, Volume-2, Pp -21-36
[38] Sec 2(j) of IT (Amendment) Act 2008 define "computer network" means the inter-connection of one or more computers or computer systems or communication device through—
i. the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and
ii. terminals or a complex consisting of two or more inter-connected computers or communication device whether or not the interconnection is continuously maintained;
[39] Information Technology Act, 2000, Sec 43(a).
[40] Ibid, Sec 43(b).
[41] Ibid, Sec 43(c).
[42] Ibid, Sec 43(d).

e) Disrupt or cause to disrupt of any computer,[43]

f) Denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means,[44]

g) Provides assistance to any person to access a computer, computer system or computer network in contravention of the provisions of this act, rules, regulation etc.[45]

h) Charges the services availed of by a person to the account of another person by tempering with or manipulating any computer, computer system or computer network.[46]

i) Destroy, deletes or alters any information or diminish the value or utility of information or affects it by any means,[47]

j) Steals, conceal, destroy or alters or causes any person to do so with the intention to cause damages.[48]

As per Section 43A, if the Body Corporate involved in processing, dealing or handling any "sensitive personal data or information", is negligent in implementing, maintaining the "reasonable security"[49]which causes the wrongful loss or wrongful gain to any person, then, such Body Corporate will be liable to pay compensation by way of damages to the person so affected.

Chapter XI of the IT Act list out kinds of offences. Some of the offences directly or indirectly dealing with the issue of privacy and data protection are as follows:

1. Hacking is a serious threat to privacy and data maintained by body corporate or government agencies or individuals. Section 66 states that whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits the offence of hacking. The punishment for hacking is imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.
2. Section 66 B provide punishment to any person who retains or receive dishonestly any stolen information shall be punishable with imprisonment extended to a term of 3 years or fine extending to one lakh or both. Section 66 C punish the person who fraudulently or dishonestly make use the electronic signature, password or any other unique identification feature of any person to imprisonment for three years extended and fine of one lakh.
3. Further Section 72 provides that the penalty of Rs. 1 Lakh or imprisonment of a term which may be extended to 2 years or both, in case where any person who under the Act lawfully has been authorized secured access to any information without the consent of the person concerned and discloses such information to any other person. This section makes liable to Body Corporate or even public sector for

[43] Ibid, Sec 43(e).
[44] Ibid, Sec 43(f).
[45] Ibid, Sec 43(g).
[46] Ibid, Sec 43(h).
[47] Ibid, Sec 43(i).
[48] Ibid, Sec 43(j).
[49] Ibid, Sec 43A Explanation (ii) "Reasonable security practices and procedure" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law, such reasonable security practices and procedures, as may be prescribed by the Central government in consultation with such bodies or associations as it may deem fit;

the violation of privacy and data related information. Further, Section 72A provides the punishment of imprisonment of term extend to 3 years or fine of Rs. 5 Lakhs or both, in case any person or intermediary while providing the services under the lawful contract has secured access to personal information about the another person and knowingly intent to cause wrongful loss or wrongful gain by disclosing the information without the consent of the person concerned or breach the lawful contract relating to such material.

EXCEPTION TO PRIVACY RULE

Section 69 of the IT Act creates exception for the Central government or the State government relating to the issue of privacy. The Act enumerates the grounds on the basis the State can order the agency of the appropriate authority to intercept, monitor or decrypt any information received, stored or transmitted. The grounds are mentioned under the Act are (a) Interest of the sovereignty or integrity of India, (b) Defence of India, (c) security of State,(d) Friendly relation with foreign state, (e) Public order, (f) Preventing incitement to the commission of any cognizable offence. The Act requires the proper procedure to be adopted before making use of the exception i.e., the reasons of interception, monitor or decrypt should be reasonable and justified as per the law. Any of the above grounds or more than one ground is justified enough for the use of exception. The Section allows the subscriber or intermediary or any person in charge of the computer resources to facilitates and give assistance to provide access to or secure access to the computer resources generating, transmitting, receiving or storing such information, or intercept, monitor, or decrypt the information, provide information stored in computer resources.[50]

Section 69B empowers the Central Government or the State Government to monitor and collect traffic data or information to enhance cyber security and for the identification, analysis and prevention of intrusion or spread of 'computer contaminant'[51] in the country. In this regard the intermediaries[52] or any person in charge of the computer resource shall facilitate the online access to the computer resource generating, transmitting, receiving or storing such traffic data[53] or information.

In case the intermediary intentionally or knowingly creates barrier then it may be punished with an imprisonment for a term which may extend to 3 years and liable to fine.[54] Central Government has laid down the procedure in The Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009.

[50] Ibid, Sec 69(2).
[51] Ibid, Meaning of the term has been referred to Section 43 (i) which means any set of computer instructions that are designed (a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; (b) by any means to usurp the normal operation of the computer, computer system, or computer network.
[52] ITA Act 2008 Sec 2(w) define "intermediary ", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online auction sites, online-market places and cyber cafes;
[53] IT Act 2000, Sec 69B Explanation – 'Traffic data' means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communication origin, destination, route, time, data, size duration or type of underlying service or any other information.
[54] Ibid, Sec 69B(4).

NATIONAL POLICY OF PRIVACY

Understanding the need to analyse the Privacy Rules, the Planning Commission and Government of India, formed a committee under the Chairmanship of Justice A. P. Shah, former Chief Justice of Delhi Court. After brainstorming session the committee submitted its report[55]and proposed a national privacy policy. The guiding principles of the proposed National Policy are as follows;

1. **Notice:** Data controller shall give notice to individuals a clear, concise and simple language notice to individual during collection and later on also. During the collection of data such notice should incorporate the (1) kinds of personal information; (2) purpose for collection; (c) use of information; (d) whether disclosure to third party or not; (e) security safeguards against loss of information; (e) process of access and correction of own personal information; (f) contact details of privacy officers. Later on the requirement of notice in the following cases; (a) data breach to be notified when applicable; (b) notification relating to the sue of information other than the purpose; (c) notify the change in privacy policy of controller; (d) any other information as per appropriate authority.
2. **Choice and Consent:** Option of in or out has to be given to the individuals regarding every stage of data collection, processing, and disclosure except in case of authorised agencies.
3. **Collection limitation:** Limited information should be collected as per the purpose of collection in lawful manner and with the consent of data subject.
4. **Purpose limitation:** Personal data collected and processed under direction of controller should be adequate and relevant to the purpose for which it is processed. Retention of data should be in compliance with the National Privacy Principle.
5. **Access and Correction:** Individual shall access information about them held with Controller. Right to access also include right to correction, amendments or deletion in case of inaccurate information.
6. **Disclosure of information:** Disclosure to third party allowed after the consent of data subjects. Disclosure to law enforcement agencies must in accordance with the law.
7. **Security:** Data controller to secure personal information against loss, unauthorised access, destruction, use, processing, modification, deanonymization, unauthorised disclosure or other reasonably risks.
8. **Openness:** data controller should take all necessary steps to implementing and adopting policies, practices, procedure and system in proportion to the sensitivity of data.
9. **Accountability:** data controller to comply with measure which gives effect to privacy principles.[56]

CONCLUSION

“Every breath you take and every smile you fake, Every move you make and every step you take, Every claim you stake, and Every vow you break I’ll be watching’ you” These words appear to come, from a disgruntled lover, but very aptly they describe the situation on the Internet. There is inherent and serious threat to one’s privacy in cyberspace. So there is a need for apt legislation and creative interpretation of law, to deal with

[55] Report of the Group of Experts on Privacy, by Chief Justice A P Shah, Available at: <http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf> Accessed on 01, May 18.
[56] Online Privacy and Data Protection Law, Available at: <epgp.inflibnet.ac.in> Accessed on 01 May, 2018.

violation of privacy rights on the "information superhighway".

Actually, there is need for separate Act, because the IT Act 2000 was enacted for E-Commerce business purpose. Like the Data Protection Act, 1998 of UK, we must also need more powerful and stringent Act, which was in pending has THE DATA (PRIVACY AND PROTECTION) BILL, 2017 yet to be pass in both the houses. IT crime is also called as White Collar Crime, because educated or intellectuals involved in it. By knowing the importance of IT, for the all-round development of the Country there is a urgent need for new specific Act. Today's position is the government facilitative for the use of IT, but lack behind proper precaution and protection. It is agreed that we are in the era of IT and our accessibility cross boarded. So enactment of specific Act is must for get more advantages of IT and protection from the third persons.

REFERENCES

Books:

1. Bainbridge David, '1st Encyclopaedia of Information Technology Law - Data Protection Law', Second Edition, Universal Law Publishing Co, 2007.
2. Benassi, P: 'TRUSTe: An Online Privacy Seal Program', Communications of the ACM, vol. 42, 2, 56-59.
3. Boli Kathy, Law and Internet Culture, Cambridge University Press, Newyork.
4. Cavoukian A , 'Data Mining: Staking a Claim on your Privacy', (Information and Privacy Commissioner's Report, Ontario, Canada), 1998.
5. Clarke R, 'Information Technology and Dataveillance', Communications of the ACM, vol. 31,1988.
6. deCew J.W., 'In Pursuit of Privacy: Law, Etchics, and the Rise of Teachnology', (Cornell University Press, Ithaca, New York),1997.
7. Diana Rowland and Elizabeth, 'Macdonals, Information Technology Law', Oxford Publications, Ireland
8. Dudeja V.D, 'Information Technology and Cyber Laws', common wealth Publication, New Delhi
9. Etzioni O, 'The World Wide Web: Quagmire or Gold Mine?', Communications of the ACM, vol,39, 1996.
10. Fried, C, 1970, 'Privacy, A Rational Context', Chap.IX in Anatomy of Values, (Cambridge University Press, New York).
11. Gavison R, 'Privacy and the Limits of the Law', Yale Law Journal, vol.89, 1980.
12. Jain M.P, 'Indian Constitutional Law', LexisNexis Butterworths Wadhwa Publication, 2011 Edition, Nagpur.
13. Lloyd Ian. J, 'Information Technology Law', Oxford University Press, 5th Edition, New York
14. Matthan Rahol, 'Law Relating to Computer and Internet' Butterworth's Law publication, New Delhi.
15. Mishra. R.C, 'Information warfare and Cyber Security', Authors Press, New Delhi
16. Rastogi Anirudh, 'Cyber Law – Law of Information Technology and Internet', LexisNexis, 2014, India.
17. Sharma Vakul, 'Information Technology – Law and Practice'. Third Edition, Universal Law Publishing Co, 2010.

Websites:

1. http://www.cyberspacelaws.com/crimes.asp
2. http://www privacy international.org
3. http://scotland on sunday.scotsman.com
4. http://us.wikipedia.org
5. http://www.aidslaw.org
6. http://www.privacyindia.org
7. http:/www.microsoft.com-glossary.mspx
8. http://www.un.org/Overview/rights.html
9. http://www .epgp.inflibnet.ac.in
10. http://www.planningcommission.nic.in/reports/genrep/rep_privacy.pdf
11. http://www.dlapiperdataprotection.com