Data Privacy & Right to Information: The Phenomenon of Strategic Control & Conflicting Interests

Sharique M. Rizvi[1]

ABSTRACT

Data Protection along with a natural right to peruse a trade in a social system by no means can dilute the right to individual freedom and privacy; although, there is an inherent conflict between Right to Privacy on the one hand & the Right to Information on the other, a law pertaining to data protection should primarily reconcile these conflicting interests. Thus, the data of individuals and organizations should be protected in such a manner that their privacy rights are not compromise; In the authors' opinion is an opportune time to initiate a serious debate on Individual's Private Right over the Public Right, which can be better coined as Data Protection Vs. Right to Information.

Keywords: Data Protection, Right to Information, Right to Privacy, Freedom of Information, Private and Public Data

1. Introduction

We are living in the world of information explosion where in the sources and receivers of information are in numerous, distinctively it has to be assured that the information that is disseminated and collected is of what quality. The consideration to the same takes us back to the times in the Second World War where prophesies of Nostredamus where significantly used by the friend nations against the Nazi Germany. As a significant observation this was a phase where there was nothing but information all around prevailing with lots of apprehension about the personal, social and economic security. The states and people where largely ill informed or misinformed to match the conflicting interests of the warring parties. Largely there was untiring effort on either side to collect and disseminated information which was classified, benefits to which was significantly transferred to intelligence people and groups which had the capability to deliver closely held information to the interested parties. This gave rise to a new breed of information traders who became infamous - Doubles Agents destined to be slain anyhow. The phenomenon of strategic dominance, which started in the Second World War, did not end with it, but continued further in the Cold War period, till, crumbled the mighty USSR.

The overwhelming desire of getting classified information about the end user for vested interests by the business corporation clubbed with the availability of such information on media and with institutions having easy access or willingness to part with made privacy an issue of the highest concern for large population. It would be worth mentioning that trespassing in to individual privacy is not only restricted to the business organisations but the same has often done by state and it enforcement agencies working on

[1] Indian Institute of Information Technology, Allahabad, India (E-mail:shariq@iiita.ac.in, Telephone: +91-9415634002)

mere apprehensions. The above-mentioned situations in their totality present forth a grim face of reality of the challenge being encountered by individuals at the hands of the business organisations, media and the state enforcement agencies.

The situation mentioned signifies on the subjected vulnerability of the individual privacy while operating in the public sphere, to ensure and support the integrity of the personal information in public domain, media or network and third party institution. Which at some point of time under a given consideration of a nature or due to inherent incapability can be allured and manipulated to part or retrieve the information pertaining to an individual considering it (the individual's information) as an acquired asset behaving as owners rather than a trustee to the same. This information in the public domain having primary attribution in the individual information pattern can be established with marginal efforts. A backward linkage with such information available in the media at large, invokes a concern for individual privacy. As an inevitable extension to the concern there should not only be a consideration on rights to information but a due diligent thought and action should be put in context to the clause of responsibility in maintaining the information in the public media and towards protection of such classified information form access and unlawful usage.

In 1990, the United Nation adopted Guidelines for the regulation of Computerised Data Files, nor have the initiatives come to halt with the promulgation of the Directive, have gathered strength and momentum largely because of the possible impact of the European approach to trans border data flow outside areas having "adequate protection". The U.S. position, a framework "Data Protection" covers the standards to be applied when handling information about people and the practices to be followed to achieve and maintain those standards.

As computing developed, so worries surfaced in countries, that the use of new machine might weaken or undermine individual human rights, The human right commission suggests that data movement might be curtailed or controlled on human right grounds gave rise, in its turn, to fear of a different kind, fears that trade between different partners would be fettered if information could not flow freely. The development of data protection standards proved to be the response to these fears. The standards are now embodied in enforceable laws in many countries, which reflect the importance of these issues, as they affect the freedom of the individuals, the free movement of information and the freedom to trade. In 1998, U.K. Data protection Act in its national and international context set out the relevance of that context to its interpretation.

2. The European Directive

The Ten Principles [11] recommended by *"Younger Report"* in the handling of personal information where computers are used, these principles are concentrated particularly on security and access to data rather than issues arising from dissemination of information and should form basis of a voluntary Code of Practices adopted by computer users

- The purpose of holding data should be specified
- There should be authorised access only to data
- There should be minimum holdings of data for specified purpose
- Person in statistical survey should not be identified
- Subject access to data should be given
- Their should be security precautions for data
- Their should be security procedures for personal data
- Data should only be held for limited relevant periods
- Data should be accurate and up to date
- Any value judgment should be coded

The best way forward, following *"Younger Report", "Lindop Report"* [11] ensures appropriate privacy safeguards in the operations of the computers in both public and private, recommended that the legislation should be supervised by an independent data protection authority, proposed principles for information use covering the same areas and in particular

a. Data subjects should know what personal data relating to them are handled, why those data are needed, how they will be used, who will use them, for what purpose, and for how long.
b. Personal data should be handled only to the extent and for the purpose made known when they are obtained, or subsequently authorised.
c. Personal data handled should be accurate and complete, and relevant and timely for the purpose for which they are used.
d. No more personal data should be handled than are necessary for the purpose made known or authorised.
e. Data subject should be able to verify compliance with these principles.

3. Object of the Directive

The [13] Member States shall guard the fundamental rights and autonomy of natural persons and in particular their right to privacy with admiration to the processing of private data. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for motives connected with the protection afforded. The Directive shall influence to the processing of personal data completely or partially by automatic means, and to the processing or else by automatic means of personal data and shall offer that personal data must be processed fairly and lawfully, collected for specified, explicit and rightful purposes and not further processed in a way incompatible with those purposes. The extra processing of data for statistical or scientific, historical purposes shall not be considered as mismatched afforded that Member States provide suitable safeguards. Sufficient, pertinent and not disproportionate in relation to the purposes for which they are composed and/or additionally processed, precise and, where required, kept up to date, every sensible step must be taken to make sure that data which are imprecise or incomplete, having regard to the purposes for which they were composed or for which they are additionally processed, are deleted or resolved. Reserved in a form, which allows recognition of data subjects for, no longer than is required for the purposes for which the data were composed or for which they are additionally processed. Member States shall put down suitable safeguards for individual data stored for longer time for historical, statistical or scientific use.

4. The Data Subject's Right to Object

Member States [13] shall award the data subject the right at to object at any time on convincing rightful grounds relating to his particular situation to the dispensation of data relating to him, saves where or else given by national legislation. Where there is a necessary objection, the processing prompted by the controller may no longer occupy those data, to point, on request and free of charge, to the dispensing of personal data relating to him which the controller expects being processed for the reasons of direct marketing, or to be communicated before personal data are revealed for the first time to other parties or used on their behalf for the purposes of direct promotion, and to be specifically offered the right to object free of charge to such revelations or uses. Member States shall take the essential measures to ensure that data subjects are awake of the existence of the rights

5. Protection, Processing and Free Movement of Personal Data

The Eight Principal

The [11] personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an "adequate" level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The objectives, laid down in the Treaty, on European Union, include making closer union among the peoples of Europe, developing relationships between the States belonging to the Community, ensuring financial and social progress by general action to eliminate the fence which split Europe, encouraging the stable improvement of the living conditions of its peoples, preserving and strengthening harmony and freedom and promoting equality on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.
"The society at large should enjoy any benefits, and be protected from prejudice, which may flow from the handling of personal data"

Cross-Border Data Transfer
"A person who discloses data to a person in a country or territory or otherwise makes the information contained in the data available to a person in a country is taken to transfer the data to that country or territory" This was an appropriately broad definition of a "transfer" and would have included personal data being communicated over telephone or via the Internet. It has been suggested that a transfer must essentially involve a loss of control over the data but it is respectfully submitted that this definition is wrong; a data controller may still retain control over the relevant personal data even if it has been transferred overseas. A transfer might be viewed as a partial loss of control over data
"A law in contravention of the requirements of the Constitution will be unconstitutional and invalid, hence to keep its validity it must be in compliance with the letter and character of the Constitution"

The Indian way
The attention-grabbing and much needed directive for providing protection to the information has set in motion the legislative wing of the Constitution of India is facing a situation where it has to decide whether it would bring amendments to the existing Information Technology Act, 2000 or to enact a separate law. The real issue to be addressed presently is more important and overlooked perspective relating to Data Protection.

A regulation on data protection should address the Constitutional matters before any statutory passing course of action is to be set in motion:

- Privacy Rights of Individuals in Cyber Space.
- Directive of Freedom of Information (19 (1) (a))
- Directives of Right to know of people at large (21)

If these subjects are sidelined in providing Data Protection then it may have disastrous consequences because the laws providing protection for information will be susceptible to the attack of illegally on the ground of violation of Articles 19(1) (a) and 21 of the Constitution.

The conflict between Right to Privacy is on the one side and the Right to Information on the other side. A law relating to data protection should first and foremost resolve these contradictory interests. Thus, the data related to individuals and organizations should be sheltered in such manner that their privacy rights are not compromised. As India is party to the International Covenant on Civil and Political Rights, provides for 'Right of Privacy' under article 17 and article 12 of Universal Declaration of Human Rights, 1948 is parallel article 17 of International Covenant does not depart opposing to any part of our public law. Article 19 & Article 21, of the Constitution on India therefore to be interpreted in compliance with the International Laws [3], "The right of the individuals to be protected against interference into his personal life, relationships and those of his family by straight physical resources or by Publication of Information" In milieu to Human Rights Conventions, it has to be rearranged that it is a part of a pack up of rights which

lie on top and cross, but all of which support the same core importance to state and protect the dignity individuals

5. Constitution of India, Right to Privacy

Article 19 Protection rights regarding freedom of speech, etc

i) All citizens shall have the right to [1]
(a) Freedom of speech and expression

ii) Nothing in sub-clause (*a*) of clause (1) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub-clause in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence [1]

Article 21, Protection of Life and Personal Liberty

No person shall be deprived of his life or personal liberty except according to procedure established by law. [1] Article 21 of the constitution of India grants the right to privacy on the citizens & netizens. This is not clearly pointed out in it, but the Supreme Court has articulated the same by way of judicial explanation.

It is private in nature and only the concerned citizens have a right to control it subject to the limitations imposed by the law. India is a party to the International Covenant on Civil and Political Rights, 1966. [15], Article 17 (ICCPR) grants for the "right of privacy". Article 17 of the ICCPR does not go converse to any part of our public law. Article 21 has, consequently to be read in compliance with the international law.

In *Kharak Singh v State of UP (1963)* [4] Mr. Justice Subba Rao, while stating the minority view, put down the basics for the progress of law of privacy in India and observed that the concept of "liberty" in article 21 was broad enough to include privacy.

In *Gobind v State of MP (1975)* [5] The Supreme Court examined that "right to privacy" must include and shelter the personal relationship of the home, the family, marriage, motherhood, reproduction and child bearing.

In *R. Rajagopal v State of TN (1994)* [6] The Supreme Court apprehended that the right to privacy is a "right to be let alone". None can make public anything relating to the above issues without his consent, whether honest or else and whether congratulatory or vital. If he does so, he would be infringing the right to privacy of the person concerned and would be accountable in an action for compensation.

In *P.U.C.L. v Union of India (1997)* [3] The Supreme court apprehended that the right to hold a telephone conversation in the privacy of individual's home or office with no interference could certainly be argued as right to privacy. Telephone tapping would, thus, contravene article 21 of the Constitution of India.

In *Mr. X v Hospital Z (1998)* [7] The Supreme Court apprehended that the right to privacy, apart from contract, also arise out of a meticulous particular affiliation, which may be commercial, matrimonial or even political. Public revelation of even true personal data may amount to an attack on the right to privacy.

There is also a right of individual privacy in Indian law. Unlawful assaults on the status and name of a person can invite an action in tort and / or criminal law. The Public Financial Institutions Act of 1993 codifies India's custom of maintaining privacy in bank transactions.

The Indian government is presently taking into account the idea of passing a detailed law on data protection under the proposal of the Ministry of Communication and Information Technology. Neither [40] the Indian nor the US constitution clearly identifies the right to privacy. In India, in the *Kharak Singh vs State of Uttar Pradesh* and *Gobind v State of Madhya Pradesh* cases the Supreme Court accepted a right to privacy resulting from constitutional rights to speech, to personal liberty, and to move freely within the country. This right was not observed as a total right to privacy, nor it address information privacy. The US constitution also does not offer any clear right to privacy, but provides a *region of privacy* recognized in its *partial shade* releases from the case law surrounding the bill of rights that grant direction on its meaning.

6. Right to Information in India

The Constitution of India has recognized Democratic Republic, and democratic system requires a well-versed community and transparency of information which are essential to its performance and also to hold corruption and to hold Governments and their mechanism answerable to the governed and disclosure of information in real practice is likely to clash with other public safety including professional operations of the Governments, best use of restricted economic resources and the protection of privacy of sensitive information.

The Right to Information offer for setting out the sensible system of right to information for citizens and netizens to safe and sound access to information under the direct of public establishment, in order to support transparency and responsibility in the working of every public authority but it is necessary to complement these contradictory interests while preserving the supremacy of the democratic model, now therefore, it is convenient to afford for delivering certain information to citizens who wish to have it.

7. Data Governance

All communications are being made with the help of Computers & Internet. Information stored in electronic form is inexpensive and easier to store. The aim of the data governance is to make the interaction of the citizens with the government offices irritate free and to share information in a free and visible form. It further makes the right to information a meaningful reality. In a democracy, people rule themselves and they cannot govern themselves properly unless they are aware of public, political, economic and other matters to tackle them. To allow them to make an appropriate decision on those issues, they must have the benefit of a variety of opinions on those issues. This plurality of opinions, views and ideas is crucial for enabling them to make judgment on those issues, to know, what their right interest is, to make them responsible citizens, to safeguard their rights, as also the interests of the society and the state.

The right to obtain information in a democratic system is accepted and it is a natural right curving from the perception of democracy. With the enacting of the Information Technology Act, 2000 more clearness is expected in government role by keeping people conscious of the State's table, plans, intentions and accomplishments. Section 7 of the Act is an facilitating section, which offers that if any law permitted that documents, report or information are required to be hold for any definite period, then, that requirement shall be believed to have been satisfied if the similar is retained in electronic form. To allow them to make a appropriate decision on those issues, they must have the benefit of a variety of opinions on those issues. This plurality of opinions, views and ideas is crucial for enabling them to make judgment on those issues; this section can be effectively used for government and public offices as well as for citizens.

8. United Kingdom

Data Protection Act "Act 1998"

An Act [9] to make provision for the disclosure of information held by public authorities or by persons providing services for them and to amend the Data Protection Act 1998 and the Public Records Act 1958, and for connected purposes. The purpose of data protection is to protect individuals' data subjects from the

unauthorised and unreasonable use or disclosure of information about themselves (personal data). The main aspects of data protection are privacy and respect for the individual. This means, not prying into someone's personal details without good reason such as asking for personal information that is not necessary for the purpose for which it will be used, allowing the individual to have access to that information and treating the information with respect in terms of what it is used for and who else it is disclosed to. The Data Protection Act 1998 introduced in UK law the provisions of the EC Data Protection Directive (95/46/EC) [11] and made new provision for the regulation of processing of information relating to individuals.

9. Freedom of Information

There is not anything in the Freedom of Information Act 2000 [17], which disagree with the requirements of the 1998 Act. Indeed, the thought is that the two Acts will function in cycle under the direction of the Information Commissioner. This means that, requirements for access to personal information will be dealt with under the necessities of the 1998 Act and requests for access to other kinds of information will be dealt with under the Freedom of Information Act 2000.

10. European Human Rights Convention

The principles of data protection are echoed in Article 8 of the European Convention on Human Rights. [18] It declares that:

- Everyone has the right to respect for their private and family life, their home and their correspondence
- There shall be no interference by a public authority with the exercise of that 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 well-being of the country
- For the prevention of disorder or crime
- For the protection of health or morals
- For the protection of the rights and freedoms of others
- When considering the effects of the 1998 Act it is therefore as well to consider also the provisions of Article 8.

11. The Combined Effect of Data Protection, Freedom of Information and Human Rights

The Golden Rules

These are some basic leading doctrine, which surface from all of this legislation, which, can help in reaching compliance.

These basic principles are:

- Treat everyone as you would wish to be treated: fairly, politely and without discrimination
- Be open in all your work, while respecting justifiable confidentiality. Only ask for personal information if you really need it and do not disclose it to others without good reason.
- Make sure all decisions (especially those that deny someone something) can be seen to be fair and reasonable:
    - Ensure everyone involved has had an opportunity to state their case
    - Explain clearly why the decision has been taken
    - Explain how the decision can be reviewed

Never express opinions about people – orally or on paper, on computer or elsewhere - that cannot be substantiated by the facts.

In *Halford V. United Kingdom*, [20] The court held that Alison Halford, the Assistant Chief Constable of Merseyside, had her right to private life violated by the bugging of her office telephone.

In *Gaskin V. United Kingdom*, [21] The court held the right to private life could require a public authority to open its file and provide information to an individual about his past, subject to making proper decisions to balance this right with the expectation of a public interest in privacy of others.

Privacy Safeguards in Russia

There are no special laws on privacy in Russia [10]; according to the Federal Act "On information, informatiszation and protection of the information" governmental data resources are open for general use except for documented information of limited access, data relevant to state secrets and confidential information. Personal data is considered as confidential information. The Act states, "Private data information pertinent to facts, actions and situation of citizen's life which may be used for recognition purposes, shall be classified according to the Act as classified information. Collection, storage, use and sharing of the information relevant to the private life as like as the information march into personal secret, family secret, secrecy of communication, telegraph, secrecy of telephone conversation, postal, and other communications of natural person without consent, shall be prohibited, apart from for those applied on the basis of court warrant". Movement of non-governmental organizations and private persons related to data processing and provided that data to users is issue of mandatory licensing. The listing of personal data and the method of protection should be predetermined by national act (the law on personal data), which has not been accepted in Russia yet. For the time being the concept "personal data" become visible in new acts, in the Tax Code, wherein the patronymic, name, surname, date, place of birth, gender, place of residence, and passport data or other data identifying the taxpayer, and nationality are categorized as personal data.

A different Russian law needs confidentiality of personal data. The Federal Act "On statements of civil status" embraces some principles of personal data protection. The labor legislation includes values of personal data protection of employees. The Labor Code guarantees personal data protection, they bound the collection of data by content and size, ensure accomplishment of employees' privileges while using and transmitting their personal data, protect the right of access, copying and rectification of own data, etc.

The listing of confidential data was defined by the Presidential Decree, Confidentiality of information has been talk about in various acts significant to professional secrets: "On banks and banking activity", Doctrine of legislation of the Russian Federation with regard to citizens' Family Code, health protection, Tax Code, etc. Russian federal acts establish over 30 types of classified data.

Civil Code usually creates forms of protection of privacy by people themselves. Privacy of communication is secured by the Federal Act "On communication" the act states that "limitation of privacy of communication is only acceptable on the basis of a judge's warrant".

Protection for citizens' rights throughout criminal inquiries are stipulated by the Federal Act "On operational examinations in the Russian Federation", the act says that a constitution that carry out these procedures must secure people's privacy. The Act utters as well: "If one trusts that a few actions of bodies that conduct operational investigation caused violation of rights or liberty, he has the right to appeal to higher structure... prosecutor or court". The Federal Act on Federal Security Services of the Russia has like terms.

If one was not provide evidence to be accountable during the legally recognized method than all materials acquired within this operational inquiry must be archived for a period of one year, in fulfillment with the Act on operational investigations and than removed. However this proviso is almost repealed by the following accumulation "…if not other is obligatory by official benefit or justice".

Leakage of data that influence privacy without one's approval, except otherwise stipulated by national acts, is legally barred. The Act on Federal Security Services of the Russian Federation holds no claim of data removal but specifies that this information shall not be convey to anyone else.

12. United States of America

Fourth Amendment of the United States Constitution [23]

In *Olmstead v. United States (1928)* [24]
Mr. Justice BRANDEIS (dissenting views)
"The right to be let alone-the most comprehensive of rights and the right most valued by civilized men", To protect, that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth.

In *United States v. Lopez (1995)* [25]
As the Chief Justice said in concurring in the result in Lopez v. United States, [24] "the fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual; . . . indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments [30] . . .."

Other Cases:

- Katz v. United States (1967) [27]
- Berger v. United States (1967) [28]
- Zurcher v. Stanford Daily (1978) [32]
- United States v. Karo (1984) [30]
- California v. Greenwood (1988) [31]
- Florida v. Riley (1989) [32]
- Kyllo v. United States (2001) [33]
- United States v. White (2003) [34]
- Hudson v. Michigan (2006) [39]

13. Safe Harbor Provision

The [36] European Union invites the United States to explain the power and policies of the Federal Trade Commission in the online privacy area.

- It had control in the event movements of employment-related information, violated the U.S. safe harbor principles?
- It has control over non-profit privacy seal plans?
- FTC Act functional similarly to off-line and online data?
- What would occur if the FTC's control overlapped with other law enforcement agencies?

The Federal Trade Commission act in response by, it affirmed that it was authorized under the Federal Trade Commission Act to examine and put on trial violations of misleading practices. "The Commission has taken the point it may confront mainly egregious privacy put into practice as unreasonable if such practices engage children, or the use of extremely susceptible information, such as monetary accounts & records and medicinal records etc. The Federal Trade Commission will give main concern to referrals of non - obedience with self - regulatory course of action received from organizations such as TRUSTe and BBB Online..." Main concern will be given particularly to recommendations from the European Union regarding alleged violation of safe harbor principles acceptable by the European Union. The note cited its

complaint against GeoCities and the resolution reached pertaining to Internet falsification of information. Similarly, it noted its objection and approval agreement with ReverseAction.com, an online auction site that secured its consumers' personally identifying information from contenders and then sent unsolicited e-mail communication to the said consumers. The Federal Trade Commission informed that it had a Consumer Response Center to obtain complaints from consumers.

With respect to employment data, the Federal Trade Commission assured the E.U. that it did have statutory and case law authority to investigate and promulgate enforcement actions in employment-related data situations. It does note, however, that conventional labor disputes would be passed on to the National Labor Relations Board for its final resolving. Regarding "seal" programs, the Federal Trade Commission do have jurisdiction over seal programs governing dispute resolution means and that it would implement appropriate rules in cases of falsification. It will do so whether the body is a profit or non-profit body. The Federal Trade Commission will seek remedies against both online and offline personals with respect to customer privacy. It mentioned its action against Touch Tone Information, Inc., which supposedly obtained illegitimately consumers private financial information.

Pertaining to overlapping control with other law enforcement agencies, the letter noted that the Federal Trade Commission has "Strong operational relationships with various other law enforcement agencies, plus the federal banking agencies and state Attorneys General." Investigations are synchronized and suitable referrals are made. Thus, the Federal Trade Commission believes that it can meet up the standards of the safe harbor provisions of the Federal Trade Commission, and institute suitable enforcement measures to assure compliance.

14. Safe Harbor Requirements for US Companies

To sum up, the agreement [13] allows the most United States corporations to officially state that the company has joined a self-regulatory group that adheres to the following seven Safe Harbor Principles or has executed its own privacy policies that match with these principles. A self-certifying organization must do the following:

- Notify individuals about the purposes for which information is collected and used
- Give individuals the option of whether their information can be revealed to a third party
- Make sure that if it conveys personal information to a third party, and the third party also offers the same level of privacy protection
- Let individuals right to use to their personal information
- Take sensible security safety measures to protect collected data from loss, mishandling or leakage
- Take reasonable steps to guarantee the reliability of the data collected
- Encompass in place a sufficient enforcement mechanism.

While the formation of the Safe Harbor Principles, business has certified over 300 companies as become certified for the safe harbor. That includes over 6% of the Fortune 500 companies.

15. Unlawful Access to Stored Communications

US Code, Title II, 2701 [39] is to protect data stored in transit and at the point of destination from being accessed and disclosed, this usualy involved data stored in RAM or computer discs and other similar device

US. Code, Title I, 2701 [38]

1. Prohibits any person from intentianally accessing without authorization a facility through which an electronic commincation servicxe is provided or intentionally exceeding authorization to access facility and therby abtaining, altering, or peserving authorized access to a write or electronic communication while it is in electronic storage in a such a system

2. Prohibits a person or entity providing an electronic communication srvice to the public from knowingly divulging to any person or entity the contents of any communication while in electronic storage by that service
3. A person or entity providing remote computing service to the public is prohibited from knowingly divulging to any person or entity the contents of any communication that is carrried or maintained on that service

DoubleClick Inc., Privacy Litigation
DoubleClick [39] is Internet Advertising Products and Service Provider specializing in analysing, compiling, collecting nonpersonal identifying information about net users and target online advertizing through it, promises its clients to place ads in front of viewers who match their clients' demographic target and put billions on online ads, by palcing cookies on the hard drives of its users computer, DoubleClick is able to colect the information. The user may opting out to prevent use of cookies of DoubleClick by denying permission or by reconfiguring their computers and browsers to block thses cookies to be stored. The plaintiff alleges that these action constitutes an invasion of their privacy and violation of federal and state laws. DoubleClick urged that clints concented to the gathering of the information, and it met the requirments of the prior concent exception. DoubleClick's motion to dismiss is granted.

16. Concluding Remarks

The conclusion can be better represented through *"Adultery is not a crime while seduction is"*, the conflict between Right to Privacy is on the one side and the Right to Information on the other side. A law relating to data protection should first and foremost resolve these contradictory interests. Thus, the data related to individuals and organizations should be sheltered in such manner that their privacy rights are not compromised. As India is party to the International Covenant on Civil and Political Rights, Article 17 therefore grants for 'Right of Privacy'. Article 12 of the Universal Declaration of Human Rights, 1948 is parallel. Article 17 of the International Covenant does not depart opposing to any part of our public law. Article 19 & Article 21, of the Constitution on India therefore to be interpreted in compliance with the International Laws [3], "The right of the individual to be protected against interference into his personal life, relationships and those of his family by straight physical resources or by Publication of Information" In milieu to Human Rights Conventions, it has to be rearranged that it is a part of a pack up of rights which lie on top and cross, but all of which support the same core importance to state and protect the dignity individuals. This is a natural right elegant from the perception of social equality with the transient of the Information, the right to get information in a democracy is accepted thus in Technology Act, 2000 more precision is expected in government meaning by keeping people conscious of the State's plan, policies, objectives and accomplishments. Section 7 of the Act is an facilitating section, which grants that if any law authorized that credentials, records and information are required to be maintained for specific period, then, that obligation shall be deemed to be satisfied if it is maintained in electronic form. To permit them to make a proper decision on those matters, they must have the advantage of an array of views on those issues. This plurality of views, opinions, observations and thoughts is vital for allowing them to make decision on those issues; this section can be successfully used for government and public offices as well as for citizens.

The [40] First Amendment provides a right of relationship and the Fourth Amendment prohibits unreasonable search and seizure, both of which relate to facets of privacy. There is no Data Protection Law in India, while numerous data protection laws exist in the US. In May 2000, the Indian government accepted the Information Technology Act (IT Act 2000), a set of laws to provide a broad regulatory atmosphere for electronic commerce. However, the Act has no provision for personal data protection. On the next side in the US, in some sector special privacy laws exist for protecting student education records, children's online privacy, individual's medical records and private financial information. In both countries self-regulatory efforts are facilitating to define improved privacy surroundings.

The directive for providing protection to the information is much needed and the legislative and the Constitution of India is facing a situation where it has to bring improvements to the existing Information Technology Act, 2000 or to enact a separate law for Data Protection. The laws on data protection must address the Constitutional problems also before any statutory enactment procedure is to be place in suggestion or passed by the parliament.

References

1. Constitution of India.
2. Information Technology Act 2000, India.
3. PUCL v Union of India, [(1997) 1 SSC 301].
4. Kharak Singh v State of UP, AIR 1963 SC 1295.
5. Gobind v State of MP [(1975) 2 SSC 148].
6. Rajagopal v State of TN [(1994) 6 SSC 632].
7. Mr. X v Hospital Z, [(1998) 8 SSC 296].
8. The Right to Information Act, 2005, No 5 of 2005, India.
9. Data Protection Law in India: a constitutional perspective by Praveen Dalal.
10. International Law and Cyber Crime, Boda Marsh Seminar on Cyber Liability 25 – 26 November, 2002, Pune, India.
11. Data Protection Law & Practices, Rosemary Jay & Angus Hamilton.
12. Cyber Law, Text & Cases, 2nd Edition, Ferrera, Lichtenstein, Reader, Bird, Schiano, Thomson.
13. Directive 95/46/Ec of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
14. Universal Declaration of Human Rights (1948).
15. International Covenant for Civil and Political Rights of 1966 (Article 17).
16. Data Protection Law, Act 1998, United Kingdom.
17. Freedom of Information Act, 2000, United Kingdom.
18. European Human Rights Convention.
19. Human Right Act 1998, Introduction – Data Protection, Freedom of Information and Human Rights, http://www.charity-commission.gov.uk
20. Halford V. the United Kingdom - 20605/92 [1997] ECHR 32 (25 June 1997).
21. Gaskin V. the United Kingdom - 10454/83 [1989] ECHR 13 (7 July 1989).
22. Constitution of Russia.
23. The Bill of Rights, United States Constitution.
24. Olmstead V. U.S., 277 U.S. 438 (1928), 277 U.S. 438, No. 533. Argued Feb. 20 and 21, 1928, Decided June 4, 1928, U.S. Supreme Court.
25. United States *V.* Alfonso LOPEZ, Jr., 514 U.S. (1995), Court of appeals for the fifth circuit, (April 26, 1995), US. Supreme Court, SSC.
26. United States v. Lopez, 514 U.S. 549 (1995), SSC.
27. KATZ v. U.S., 386 U.S. 954 (1967), 386 U.S. 954, No. 895. March 13, 1967, U.S. Supreme Court.
28. Berger V. New York 388 U.S. 41 No. 615 Argued: April 13, 1967, Decided: June 12, 1967, No 615, U.S. Supreme Court.
29. Zurcher V. Stanford Daily, 436 U.S. 547 (1978), Argued January 17, 1978, Decided May 31, 1978, ALR.
30. United States V. Karo, 468 U.S. 705 (1984), 468 U.S. 705, The Tenth Circuit, No. 83-850. Argued April 25, 1984 Decided July 3, 1984, US. Supreme Court.
31. California V. Greenwood, 486 U.S. 35 (1988), 486 U.S. 35, FOURTH APPELLATE DISTRICT No. 86-684. Argued January 11, 1988, Decided May 16, 1988, US. Supreme Court.
32. Florida V. Riley, 488 U.S. 445 (1989), 488 U.S. 445, No. 87-764. Argued October 3, 1988 Decided January 23, 1989, US. Supreme Court.
33. Kyllo *V.* United States, Court of appeals for the ninth circuit, No. 99-8508. Argued February 20, 2001--Decided June 11, 2001.
34. United States *V.* White Mountain Apache Tribe, Court of appeals for the federal circuit, No. 01-1067. Argued December 2, 2002--Decided March 4, 2003.
35. Hudson *V.* Michigan, Court of appeals of Michigan, Argued January 9, 2006—Reargued May 18, No. 04–1360. 2006—Decided June 15, 2006, US. Supreme Court, SSC.

36. Safe Harbor Provisions, European Union.
37. Privacy Regulation, US/EU Safe Harbor Agreement: What It Is and What It Says About the Future of Cross Border Data Protection, Mozelle W. Thompson, Peder van Wagonen Magee1**,** Federal Trade Commission Washington, DC.
38. US. Code, Title I, 2701.
39. Doubleclick Inc. Privacy Litigation, 154 F. Supp. 2d 497; 2001 U.S. Dist. LEXIS 3498, Master File No. 00 Civ. 0641 (NRB), United States District Court for the Southern District of New York, 154 F. Supp. 2d 497; 2001 U.S. Dist. LEXIS 3498, March 28, 2001, Decided March 29, 2001, Filed.
40. Privacy Perceptions in India and the United States: An Interview Study Ponnurangam Kumaraguru y, Lorrie Faith Cranor *y* and Elaine Newton.