Volume-4, Issue-12, Dec-2015 • ISSN No 2277 - 8160

Research Paper Law

Privacy Rights and Data Protection In Cyber Space with Special Reference to E-Commerce.

Mahantesh B Madiwalar Research scholar Kuvempu University Department of Law and Lecturer S J R College of Law, Bangalore

Prof(Dr.) B S Reddy Professor of law and Registrar Evaluation Karnataka State Law University, Hubballi

ABSTRACT

Privacy is one of the most urgent issues associated with information technology and digital media. 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 recognized under Part III of the Indian Constitution. Here an important point should be note that Indian Constitution does not include the 'right to privacy' as fundamental right. Its existence, therefore, as a constitutionally guaranteed fundamental right is debatable. Nevertheless, the judiciary has, no 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 .

India's e-commerce business expected to reach $50 to 70 billion by 2020. This is the witness that all the business activities shall hold by plastic cards, it creates threatens to privacy rights.

KEYWORDS : Data protection law, Vulnerabilities of data, , E-Commerce

Introduction

"The right to privacy refers to the specific of an individual to control the collection, use and disclosure of personal information"[4]. Personal information could be in the form of personal interest, habits and activities, marital status of individuals, educational information, and financial records and also medical records; it includes mail and telephone convergence. Due to the technological innovation it is very easy to access and communicate to others.

This follows that with the increasing use of internet, need for changes in law is inevitable. This internet stores huge amount of data for different kind of people with different requirement. It is a witnessed that vast using of internet becomes growth in e-commerce hence internet is itself global.

Consumer regards with Privacy

Identity Theft

'Consumers may be victims of identity theft as a free flow of information example in US in this year 700,000 people have stolen their identity'.[5] This identities theft is a real and growing problem.

This identity theft can be correlated with to the loss of privacy. The information of individuals is passes freely through online and offline and it is more freely misuse it.

Information sharing and telemarketing fraud

This is the area in which biggest personal information is misused. This costs consumers $50 billion a year[6]. The free availability of personal information increases the ability of fraudulent telemarketers to victimize consumers. Unethical telemarketers have made unauthorized charges on the customer's credit card accounts. Example in the US the one of the biggest telemarketing company Brand Direct obtains account information from some of the nation's banks. It then offer customers to get thirty- day free memberships for clubs, at the end of thirty days, the customer's credit card would be automatically charged. This is situation how telemarketing companies doing their business. May be the company is liable for fraud against customers but the customer's information have been already shared with different telemarketing companies definitely it will causes violation of individual privacy rights which has been recognized under Indian Constitution.

On line Data Collection

Consumers are clearly concerned about their private personally identifiable and financial information are being handled through the Internet medium. They still have to learn that information about their activities, ranging from online browsing to grocery shopping. It easy to made companies to get information easily without their permission.

On line levels of privacy

It is globally true that, the no online activities or services are guaranteed to protect their right to privacy.

Public activities

Engaging and participating in public activities over the internet there is no expectation of privacy. In real sense it is not illegal for anyone to view or disclose information in the form of electronic is readily accessible to the public.

The internet service providers they are keeping personal information in their directories. Some 'ISP's[7] may share personal information to others on the wishes of individual interest. So this reason the consumers must read their agreements to determine their ISP's policies.

Private E-Mail Services

Generally all online service providers offer "private" electronic mail services for their subscribers. Under the Information Technology Act, 2000 section 66 deals with Hacking with Computer system. The ISP may view private email if it suspects the sender is attempting to damage the system or harm another user.

Even these regulations made by the different Acts but the personal information or emails are always interrupted by unknown persons. We are not able find out the wrong doers.

Limited access activities.

It is believed that the internet users if they are access limited it will safeguard the privacy. While those members who have access may mutually send communication within these borders, internet service providers describes the activities and communications within the "walls" of these forums as private.

Information gathering practices

The revolution of information in this world and progress in business activities in this global arena and growth of data mining and target marketing have contributed to a change in data collecting. The consumer's information has the potential of being bought and sold like any other valuable commodity. Example, in U S Consumers probably has more choices of products and services offered them by business than consumers anywhere else in the world. They respond to those offers, especially when they connect directly with the individual's personal life situation and interests.

Offline Information Gathering
There are currently more than thousands companies are involving in comprehensive database about their individuals and personal information. Rather than engaging in mass marketing, they target on gathering as much information as possible about specific people to engage in "profile" marketing[8]. By compiling layer upon layer of information about specific individuals, they are able to produce a profile based on income lifestyle, and an enormous variety of other factors.

Online information gathering
The internet
The collected information is sent over the vast network comprising the Internet may pass through dozens of different computer systems on the way to its final destination. Each of these different computer systems may be managed by a different systems operator, and each system may capture and store online data. These online activities will be monitored by different service providers and by the various operators of any sites on the internet which they visit.

Perils of Online profiling ,Cookies, Clickstream Data
"transaction-generated information,"[9] these sources are valuable revenue for data collection activity. Most of the information is gathered through the Internet by advertising mechanisms. This internet advertising allows a web-based business to reach those consumers they are most likely to be interested in its goods and services. This online profiling allows traders to target their advertising to those who have shown an interest in their products or services. Information about how a consumer uses the web, including the sites visited, may be collected by web sites themselves, or may be collected by advertising networks or marketing companies. This data is often referred to as "click stream data"[10]. This Click stream data, which may or may not be enough to identify a specific individual, can be collected at varies points during a user's online activity.

The cookies are tracking the consumer's movements on computer. When user goes online, the type of information that may be collected includes; site visits, search terms, online purchases. The companies collecting the consumer information by these cookies they are unique, small text files that web sites "write" on a user's hard drive. These cookies are enable web sites to capture data about users' online activities.

When consumer visits a web site, cookies may be placed on their computer. The cookie will allow the web site to determine whether a user is a repeat visitor and can customize the experience for the visitor. The cookies can also be used to then record and store clickstream data from the user's session and then store the information in a manner that links it to an individual cookie. If a user repeatedly visits a site, the cookie is then used to call up preferences and data relating to the user.

Regulatory measures
Data protection Act of U K (DPA)
In India we often refer to the Data Protection Act of UK as standard to emulate. This act follows the EU guidelines on Privacy and is built eight Data Protection Principles and Seven Privacy Right Principles namely.

Data Protection Principles under DPA
All Data shall be fairly and lawfully processed
- Data shall be processed for limited purposes for which the data subject has authorized
- Collective of Data shall be Adequate, Relevant and not excessive
- Data shall be kept accurate and up to data
- Data shall not be kept longer than necessary
- Data shall be processed in accordance with the individual's rights
- Data shall be kept secure
- Data shall not be transferred to countries outside European Economic area unless country has adequate protection for the individual

EU Guidelines
Based on the OECD guidelines on privacy the European Union came out with its own data protection principles to their countries on February 2, 1995.
- Information may be stored and used only for the purposes for which it is collected.
- Information must be accurate, up-to-date.
- Information may be processed only with the individual's consent.

The new Data protection law in EU
On 25 January 2012, the European Commission unveiled a draft legislative package to establish a unified European data protection law.

The proposed new EU data protection regime extends the scope of the EU data protection law to all foreign companies processing data of EU residents.

Data Protection law in US
In United States there is no such type of data protection regime and there no data protection legislation and thus there no supervisory authority also; rather each sector has specific legislations, regulations and self regulation, to be complied with. In order to be categorized as safe destination for data US entered into Safe '*Harbor principles*'[11]

Data Protection law in India
Indian Constitution and Right to Privacy
Communication, speech and expression undoubtedly constitute some of the most basic liberties of individuals and, to a large extent, can be considered inalienable.[12] In India these rights are recognized in Part III of the Indian Constitution, here an important point is that the right to privacy is not fundamental right. In the year of 2004, the Indian Supreme Court interpreted that Article 19(1) (a) of the Constitution of India to include by implication the right to information within the constitutional guarantee of freedom of speech and expression.

Data Protection under Information Technology Act 2000/2008
- To make unauthorized use or access of data is punishable under Section 66.
- To make unauthorized use or access of data is liable for payment of compensation up to Rs 1 crore under Section 43.

Under the Information and Technology law with above Sections 43 and 66 tow new Sections 43A and 72A has been proposed to specifically addressed the data protection

Section 43A: Compensation for failure to protect data

Where a 'body corporate'[13], possessing, dealing or handling any 'sensitive personal data'[14] or information in a computer resource which it owns, controls or operates.

Section 72A. Punishment for Disclosure or information in breach of lawful contract.

These provisions are contained under Section 85 which is stated as follows.

Conclusion and Suggessions:
In present scenario the Information Technology is developing more and more and in the same way the cyber crimes. We are totally imbalanced because with the speed of technology our laws are not competent, so that we need such type of law which will prevent cyber crimes as well as protect consumer's privacy rights.

The Indian Information and Technology Act 2000/2008, has sufficient clauses to punish privacy infringers. In the same way day to day the technology is also developing more and also in E-Commerce most of the cases have been recorded, this is the right time for us to think on another legislation i.e. data protection law.

REFERENCES

1. Paula Selis, Protecting personal information through commercial best practices. Office of the Attorney General 900 Fourth Avenue, Suite 2000, settle, Washington 98164-1012. 2. Deccan Herald, Government may ban Gmail, Yahoo! for official use, Saturday,September,13,2014,p-9. 3. Prof.(Dr.) Paramjit s. Jaswal, Consumer activism, competition and consumer protection, Rajiv Gandhi National University of Law, Punjab. 4. "Telephone regulatory authority". 5. 'THE HINDU' by "Comscore" dated 24/8/2013. 6. Halen Nissenbaum, protecting privacy in an information age: the problem of privacy in public. Stanford University Press, 2010. 7. Organization for Economic Cooperation and Development. This organization has group of 30 member countries committed to the fostering of Good Governance and market economy and consists of EU Countries, USA, Canada, Australia, Japan, Korea etc it was came in to force on 1980, India as a cooperation program with OECD as developing nation and is not a member 8. International Journal on Consumer Law and Practice, Volume I, 2013, pp-65-67. 9. M. Mahindra Prabhu and P. Rajadurai, the ways to empower the e-consumer in the alarming field of online shopping, 25years of Consumer Protection Act: Challenges and the way Forward, Editor Prof(DR.) Ashok R. Patil, Chair on Consumer Law and Practice, National Law School of India University. 10. "First Analysis of the Personal Data protection Law" Final Report, prepared by CRID-University of Namur. 11. Dr. Nehaluddin Ahmad, "The issues of personal privacy and internet-A Critical analysis of Indian position and International scenario" Senior Lecturer, Faculty of Business and Law Multimedia University, Jalan Ayer Keroh Lama,75450 Melaka Malaysia. 12. "Cyber Crimes and the Society", Post Graduate Diploma in Cyber laws & Cyber Forensics, Distance Education Department National Law School of India University, p-84. 13. George K. Kostopoulos, "Cyberspace and cyber security" CRC Press, Taylor & Group Boca Raton London New York, 2013 edition. 14. Yee Fen Lim, "Cyberspace Law", Commentaries and Materials, Oxford University Press, 2007. 15. Deccan Herald, 'India to have over 300 million internet users by year –end.' Saturday, November 22, 2014, p-15. 16. The Financial Express, 'United States/cyber-security,Is Kim Jong Un innocent? America was too quick to blame Norht Korea for the hack attack on Sony, Saturday3rd January 2015, p-12