PRIVACY RIGHTS AND DATA PROTECTION IN CYBERSPACE WITH SPECIAL REFERENCE TO E-COMMERCE

Mr. Mahantesh B. Madiwalar*
Prof. Dr. B.S. Reddy**

Abstract

The development of information and technology in the communication sector witnessed the emergence of several issues relatively legal and ethical[1], for these issues still today we are unable to find solutions. Of this such technology is, however, liable to misused by both, individuals and state machinery.

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[2].

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.

Key words: Data Protection law, vulnerabilities of data, privacy law, e-commerce

* Research Scholar, Department of Law, Kuvempu University Shimoga;Lecturer S.J.R. College of Law, Bangalore.
** Former Registrar (Ev. and Admn.)Karnataka State Law University, Hubbali.

1 Dr.Nehaluddin,*"The issues of personal privacy and internet-A critical analysis of Indian position and international scenario"* June 2008, *available at*http://works.bepress.com/nehsluddin_ahmad/1.

2 *Id.*

Introduction

Data protection and privacy rights are two important rights conferred by any of the civilized nation. Every individual and organization has a right to protect and preserve their personal and sensitive and commercial data and information[3].

This is an internet age; we can take India into new heights of excellence in education, medicine and communication, and public services. Indians being known for their hard work and dedication they create global reputation. Development in one sector always impact on other sectors or life.

"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.

Now information plays a valuable role its having financing value, also most of the information is transmitting for monetary benefits, example, if consumers purchased any articles in supermarkets and payment made by plastic debit or credit cards, the consumers personal information will be stored by computers then that company would transfer that information for commercial benefits without notice to consumer, this is how information is circulating from one hand to another hand and more over most of telemarketing activities has been done by this plastic cards and most of the money misuse will happens in this sector only. 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.

Invading privacy

Recently the leakage of *Radia* tapes, the wire taps were ostensibly for income tax investigation that leads to privacy compromise of several individuals. This led to the start of privacy debate in the country. In today's online world data collection is ubiquitous. Google collets data of all users visiting it; face book collects and

---

[3] http://perry4law.org.

[4] Aashit Shah and Nilesh Zacharias "*Right to Privacy and Data Protection*".

shares the acts of surfing, emailing, chatting, blogging, buying, ticketing, banking, reading news papers and so on result in sharing of one's personal data with the respective. When we get back from websites all our transactions are get locked, and perhaps forever, unless of course, the laws force them not to retain data beyond a certain period.[5]

In the advancement in computer technology are making it easy to do what was impossible not long ago. This behavior is determined by individual's transactions with various educational, financial, governmental professional and judicial institutions. Major uses of this information include direct marketing and credit check services for potential borrowers or renters. To the individual the result of all this information sharing is most commonly seen as increased 'junk mail'.

This, the law of privacy has not kept pace with the technological development. It must be noted that the right to freedom of speech and expression and right to privacy are two sides of the same coin. One person's right to know and be informed may violate another's right to be let alone. For harmonization of these two things necessary restrictions are implied. The law of privacy endeavors to balance these competing freedoms.[6]

E-commerce transactions and privacy

In the international level the OECD[7] has made principles in 1980, in an effort to create a comprehensive data protection system throughout Europe, the OECD issued its "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data.The seven principles governing the OECD's recommendations for protection of personal data were:

1. Notice: data subjects should be given notice when their data is being collected;
2. Purpose- data should only be used for the purpose stated and not for any other purposes;

---

5 Dr. Kamalesh Bajaj *"Companies have to take responsibility for individual data privacy"* wed. Feb-9.2011.

6 *Supra* note 3.

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.

3. Consent- data should not be disclosed without the data subject's consent;
4. Security- collected data should be kept secure, from any potential abuses;
5. Disclosure- data subjects should be informed as to who is collecting their data;
6. Access- data subjects should be allowed to access their data and make corrections to any inaccurate data;
7. Accountability- data subject should have a method available to them to hold data collectors accountable for following the above principles.

These principles basically aim to provide, promote and protect information Privacy, fully informed 'Contract Formation' to the consumers with reasonable terms of his interest, privacy protection, Payment Security and security of personal information, Redressal Mechanism, Liability Clauses, Denial of Unsolicited E-Mails to the consumer without his consent and Consumer Awareness to consumers in the protection their basic rights in e-commerce transactions.[8]

The national perspective

'On line shopping is a new incline that gains momentum in the recent years in India'[9] there are mainly four types of shopping in India **1.** The sellers bring their products in streets for sale. **2.** The consumers have to visit the shop and purchase the goods. **3.** The concept of super market and mall culture where consumers are free to pick their products from the shop and goes for billing. **4.** The consumer can order goods form online. Here the seller uses the internet as medium for business transaction. The internet provides sellers to open their shops through web portals, which can be operated by home and get the goods are delivered to his home. In India this new trend attracts youth, middle class and upper class people these 'E-Consumers dealt with the same consumer protection Act of 1986.'[10]

On the other way round this field became easy target for the wrong doers. The means of fake websites and role of hackers were

---

[8] *International Journal on Consumer Law and Practice*, Vol I 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] Anita A.Patil, "*The era of e-consumerism and issues concerned*" Indian Bar Review, Vol.XLI (2) 2014.

threat to this modern trend[11]. The reasons for growth of e-consumer is time consumption, faster and cheaper, easy transaction and home delivery.

Consumer regards with privacy

Identity theft

In the daily transactions most of the consumers are unaware of the reuse of personal information they provide to others during daily transactions. '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'.[12] 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[13]. 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.

Online 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

---

11 *Id.* pp. 124-125.
12 *Supra* note 1, p. 5.
13 *Supra* note 1, pp. 6.

shopping. It easy to made companies to get information easily without their permission.

Online levels of privacy

It is globally true that, the no online activities or services are guaranteed to protect their right to privacy. We can categorized these activities in three general groups that are a) public activities b) private electronic mail services, and c) limited access activities. The level of privacy one can expect from an online activity is often governed by the nature of the activity.

(a) 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. For example if user sends any news message to a public news group or forum or online newsletter, that information is readily accessible or public access.[14] It is commonly, the user's online name, electronic mail address, and information about service providers are usually available for inspection as part of the message itself.

The internet service providers they are keeping personal information in their directories. Some 'ISP's[15] may share personal information to others on the wishes of individual interest. In addition to their online directories, service providers may also sell their membership lists to direct marketers. So this reason the consumers must read their agreements to determine their ISP's policies.

(b) 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. "Whoever with the intention to cause or knowing that he is likely to cause wrong full loss or damage to the public or any person destroys or alters any information residing in a computer resource

---

14 *Supra* note 1, pp. 8.

15 ISP:Internet service provider is an organization that provides for accessing using or participating in the internet service provider may be organized in various forms, such as commercial, community-owned, non-profit otherwise privately owned.

or diminishes its value or utility or affects it injuriously by any means, commits hacking".[16]

In US the Federal Communications Privacy Act makes it unlawful for anyone to read or disclose the contents of an electronic communication. Some exceptions

1. The ISP may view private email if it suspects the sender is attempting to damage the system or harm another user.
2. For the purpose of inspection the ISP can disclose the e mail.
3. If the employer owns the email system then the employer can inspect the employee email.
4. The law enforcement authorities can excess emails only after getting permission from court.
5. The ISP can disclose the email in the circumstance of serious injury to any person requires disclosure of the information without delay. Under US Patriot Act 2001[17].

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.

(c) 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. However chatline users may capture, store, and transmit these communications to outsiders. We can say that these activities are subject to the same monitoring provisions governing private e-mail which may not, under all circumstances, be so "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. It is available

---

[16] "*First Analysis of the Personal Data protection Law"* Final Report, prepared by CRID-University of Namur.(Centre de recherché information, droit etsociete).

[17] 'The US Patriot Act of 2001', was passed and signed by President George Bush on October 26, 2001, it stands for *Uniting and strengthening America, by providing appropriate tools required into intercept and obstruct terrorism Act2001.*

from list brokers, look-up or reference business, public databases, and credit reporting agencies, advertisers, and many others. Now most of the consumers purchasing the good from online this is the main reason that marketers can easy to get all the Information which has been stored in the computers. Example, in US 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. For this sophisticated business and order to get their marketing messages across the world, they collect and analyze detailed personal and financial information about consumers. Much of the information is compilation without knowledge of individual's, as business become more competitive, and seek innovative ways to reach new customers and market to existing ones, for that individual's zone of privacy may become increasingly eroded. [18]

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[19]. 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.

Using these databases, it is easy to possible to recognize the people by what many would consider private aspects of their lives, including their medical conditions, their ethnicities, those selected candidates can be targeted not only by direct marketers, but by lawyers, insurance companies, financial institutions, and anyone else who has funds to pay for the information. These things are not free for example an unlisted phone numbers can be purchase for $49. A social Security number costs $49. And a bank balance costs $45.

Online information gathering

The internet

The collected information is sent over the vast network comprising the Internet may pass through dozens of different computer

---

18 *Supra* note 1, pp. 11.

19 "*Profile Marketing*": It is a direct marketing multichannel business that is focused on delivering a service that is not bound by industry software, hardware, and knowledge.

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,"[20] 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. For example, if consumers visited supermarket web-sites, might find themselves viewing customized banner ads on future websites they visit even non purchase ones. Online profiling is a unique practice, but it is nevertheless a recognizable analog of long-established and accepted offline marketing.

Online advertisement is collection of anonymous transactional data that is used to create customized websites or targeted advertisement.

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"[21]. 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

[20] The information is not transforming from e-mails but "passively". The consumer's information is surf by the internet and retrieves the information or documents from websites.

[21] 'ClickStream', it is the process of collecting, analyzing and reporting aggregate data about which pages visitor visit in which order. It can include a user's computer internet protocol address(IP), the type of browser used, a user's activities during his or her last visit to a website, and activities conducted on other websites.

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.

In addition to merchant cookies, advertising companies which provide banner advertisements on multiple web sites may also place cookies on a user's computer. Therefore, if a user visits a travel sites may also place cookies on a user's computer. When the consumer visits travel sites automatically the cookies identifying and provides banner advertisements this is so called third party cookie will then record the user's interest in travel. Next time when the customer visits new site like new site, he or she may see a banner ad for vacations or for an airline- this is because the advertising company's cookies will be recognized and customized banner ad will pop up on a new and unrelated site. Thus, on line profiling through third party cookies can occur across web site. The information gathered from cookies is minimal privacy risks.[22]

Regulatory measures

Data protection Act of UK (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

1. All data shall be fairly and lawfully processed.
2. Data shall be processed for limited purposes for which the data subject has authorized.
3. Collective of data shall be adequate, relevant and not excessive.
4. Data shall be kept accurate and up to data.
5. Data shall not be kept longer than necessary.

[22] *Supra* note 1, pp. 12-13.

6. Data shall be processed in accordance with the individual's rights.
7. Data shall be kept secure.
8. 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 and must be maintained in a form that does not permit identification of individuals longer than necessary for those purposes.
- Information must be accurate, up-to-date, relevant, and not excessive in relation to the purposes for which it is stored.
- Information may be processed only with the individual's consent, legally required, or protect the public interest or the legitimate interests of private party, except when those interests are outweighed by the individual's interests.

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. It provides for a harmonization of the data protection regulations throughout the EU, thereby making it easier for non E U companies to comply with these regulations.[23]

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

[23] *Supra* note 21, pp. 85.

into Safe '*Harbor principles'*[24] with EU companies who agree to adhere to Safe Harbor requirements and publish privacy policy statement that it adheres, to Safe Harbor. The department of Commerce maintains a list of all such organizations.

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.[25] 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. The judiciary has, on opined that the right is implicit in the right under Article 21, (case *Rajagopal* v. *TamilNadu*) which provides that no person shall be deprived of his life and personal liberty without procedure established by law, it means that right to privacy is acquired Constitutional status.

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. Consequently, the government enacted a national legislation called the right to information Act 2005, the character of the Act was broad and covered under its ambit "information held by or under the control of any public authority"[26]

Data protection under Information Technology Act 2000/2008

1. To make unauthorized use or access of data is punishable under Section 66.
2. To make unauthorized use or access of data is liable for payment of compensation up to Rs 1 crore under Section 43.

---

[24] "*Safe Harbor",* is the name of policy agreement established between US Department of commerce and EU in November 2000, to regulate the way that US Companies export and handle the personal data (such as names and address) of European citizens. http://searchcio.techtarget.com.

[25] 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.

[26] RadhaRaghavan and Ramya Ramachandran, "*Data Protection Law in India: An Overview,"* Posted on January 29, 2013. *Also available at*http://lex-warrier.in/2013/01/indias-data-protection-law-an-overview.

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

Section 72A: Punishment for disclosure or information in breach of lawful contract

Any person including an intermediary, who while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person?

With intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punishable with imprisonment for a term which may extend to two years, or with a fine which may extend to five lakh rupees, or with both.[27]

With the both act of IT Act 2000, and IT Act 2008, there will be provisions for punishment of a corporate and its executives for any offences under the Act. Since these offences include under Section 66 and other Sections, this represents the adverse consequences of not following the data protection principles. These provisions are contained under Section 85 which is stated as follows:

Section 85: Offences of companies

1. Where a person committing a contravention of any of the provisions of this Act of any rule, direction or order made there under is a company.
   Every person who, at the time the contravention was committed, was in charge of, and was responsible to the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:
   Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.
2. Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made there under has been committed

[27] *Supra* note 21, pp. 86-87.

by a company and-it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary, or officer of the company, such director, manager, secretary, or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and be punished accordingly.

Conclusion and suggestions

Buoyed by strong growth in Internet consumption on mobile devices, the number of people online in India is forecast to touch 500 million by end of this year, over taking the US as the second largest Internet market in the world.[28]

The current situation, despite the existence of the legislative framework and the efforts of national and international data protection authorities and bodies, privacy abuse continues on a vast and persistent scale[29], because the current legislations would not be able to enforce effectively. We can quote the different causes, in recent years the purchasing parity was increased due to the internet. Many of the of the consumers they don't want to take extra burden because now a days if consumer purchase goods from internet next day goods will come to his doorstep, so that consumers they save time and energy. One side this system has provided more benefits, but the other way round without knowledge of consumers their information is transferred and misused by different companies or within the companies. Individual's information is vulnerable.

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.

Now most of the countries in the world have been accepted that this privacy infringement problem is not concerned with any one particular county, it is the problem of whole world. It determines that privacy infringement will be found globally acceptable. This is the reality that must be faced. In many countries like India, laws have not kept up with the technology, leaving significant gaps in protections. Our challenge to integrate computer technology in

---

28 'Deccan Herald', '*India to have over 300 million internet users by year–end'* Saturday, November 22, 2014, p. 15.

29 *Supra* note 20, pp. 53.

such a way that, the technology advances and protects those values rather than doing damages to them.

References

I. Paula Selis, *Protecting personal information through commercial best practices.* Office of the Attorney General 900 Fourth Avenue, Suite 2000, settle, Washington 98164-1012.

II. Deccan Herald, *Government may ban Gmail, Yahoo! for official use*, Saturday, September13,2014,p-9.

III. Prof.(Dr.) Paramjit s. Jaswal, Consumer activism, *competition and consumer protection,* Rajiv Gandhi National University of Law, Punjab.

IV. "Telephone Regulatory Authority".

V. 'THE HINDU' by *"Comscore"* dated 24/8/2013.

VI. Halen Nissenbaum, *Protecting privacy in an information age: the problem of privacy in public.* Stanford University Press, 2010.

VII. *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.

VIII. *International Journal on Consumer Law and Practice,* volume I, 2013, pp. 65-67.

IX. 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.

X. "*First Analysis of the Personal Data Protection Law"* Final Report, prepared by CRID-University of Namur.

XI. 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.

XII. *"Cyber Crimes and the Society",* Post Graduate Diploma in Cyber Laws & Cyber Forensics, DistanceEducation Department National Law School of India University, p. 84.

XIII. George K. Kostopoulos, *"Cyberspace and cyber security"* CRC Press, Taylor & Group Boca Raton London New York, 2013 edition.

XIV. Yee Fen Lim, "*Cyberspace Law"*, Commentaries and Materials, Oxford University Press, 2007.

XV. Deccan Herald, '*India to have over 300 million internet users by year–end*.' Saturday, November 22, 2014, p.15.

XVI. The Financial Express, 'United States/cyber-security,Is Kim Jong Un innocent? America was too quick to blame North Korea for the hack attack on Sony, Saturday3rd January 2015, p. 12.