

ISSN: 2582 - 2942



LEX FORTI

LEGAL JOURNAL

VOL- I ISSUE- VI

AUGUST 2020

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of LexForti Legal Journal. The Editorial Team of LexForti Legal Journal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of LexForti. Though all efforts are made to ensure the accuracy and correctness of the information published, LexForti shall not be responsible for any errors caused due to oversight otherwise.



ISSN: 2582 - 2942

EDITORIAL BOARD

EDITOR IN CHIEF

ROHIT PRADHAN

ADVOCATE PRIME DISPUTE

PHONE - +91-8757182705

EMAIL - LEX.FORTII@GMAIL.COM

EDITOR IN CHIEF

MS.SRIDHRUTI CHITRAPU

MEMBER || CHARTED INSTITUTE

OF ARBITRATORS

PHONE - +91-8500832102

EDITOR

NAGESHWAR RAO

PROFESSOR (BANKING LAW) EXP. 8+ YEARS; 11+ YEARS WORK EXP. AT ICFAI; 28+ YEARS WORK EXPERIENCE IN BANKING SECTOR; CONTENT WRITER FOR BUSINESS TIMES AND ECONOMIC TIMES; EDITED 50+ BOOKS ON MANAGEMENT, ECONOMICS AND BANKING;

ISSN: 2582 - 2942

EDITORIAL BOARD

EDITOR

DR. RAJANIKANTH M

ASSISTANT PROFESSOR (SYMBIOSIS
INTERNATIONAL UNIVERSITY) - MARKETING
MANAGEMENT

EDITOR

NILIMA PANDA

B.SC LLB., LLM (NLSIU) (SPECIALIZATION
BUSINESS LAW)

EDITOR

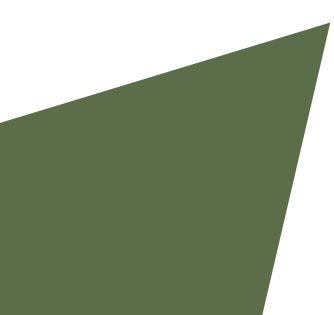
DR. PRIYANKA R. MOHOD

LLB., LLM (SPECIALIZATION CONSTITUTIONAL
AND ADMINISTRATIVE LAW)., NET (TWICE) AND
SET (MAH.)

EDITOR

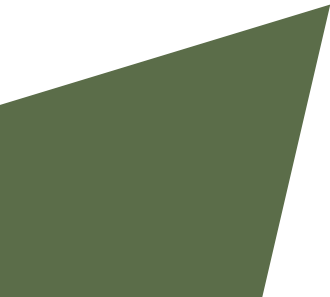
MS.NANDITA REDDY

ADVOCATE PRIME DISPUTE



ABOUT US

LexForti is a free open access peer-reviewed journal, which gives insight upon broad and dynamic legal issues. The very objective of the LexForti is to provide open and free access to knowledge to everyone. LexForti is highly committed to helping law students to get their research articles published and an avenue to the aspiring students, teachers and scholars to make a contribution in the legal sphere. LexForti revolves around the firmament of legal issues; consisting of corporate law, family law, contract law, taxation, alternative dispute resolution, IP Laws, Criminal Laws and various other Civil issues.



Legal Dimensions of Cyber Privacy & Data Protection in India

Satyam Singla & Somya Agarwal

ABSTRACT

First half of 2017 witnessed more than 5,000 cyber-crimes as per CERT. Ironically, merely one or two of the crimes were able to make it to the newspaper headlines. Cyber-crime is one of the latest branches of crime. It evolves over a period of time with the advancement in technology. Almost every such crime involves a computer or a network or internet. In the present era, Internet has become an indispensable tool of our life. It would be unjust to question its utility or significance in today's world. It is appropriately said that improvement accompanies a cost. Each wrongdoing leaves a social and negative effect thus does the most as of late developed wrongdoing. One of the major concerns relating to the same is privacy. In India, cyberspace is governed by Information Technology Act, 2000 but the same is silent on the issue of privacy in cyberspace. Privacy being a fundamental right needs to be protected. Due to lack of measures to curb the attacks, India has witnessed many failures concerning privacy in context with cyberspace. Laws in India are not sufficient enough to tackle the existing problem. When we talk about cyberspace, existing laws have a number of loopholes. For instance, a person cannot be made liable for aiding a person to get access to the data of the victim under section 43(g) of the said act. Also scope of the section 66E of the same act is very limited as it covers only body areas under privacy. The proposed bill on the same issue i.e. Data Protection Bill, 2013 makes a person liable when the consent of other party has been obtained through coercion. However it does not take into consideration the other aspects where the consent has been obtained through misrepresentation or undue influence. This paper would majorly focus upon identifying the gap areas in the existing laws because of which the privacy of an individual is compromised. Paper talks about the steps or measures which can be taken in order to combat the present situation. How existing laws can be amended to suit the present scenario because innovation in law is necessary for societal development.

INTRODUCTION

Privacy is one of those issues which are very difficult to define. At times privacy is seen as a way of drawing the line at how far the society can intrude into a person's affairs. The right to be left alone is a part of the right to enjoy life. The right to enjoy the life is, in turn, a part of the fundamental right to the life of an individual. Privacy can be defined as the rightful claim of individual to determine the extent to which he wishes to share of himself with others. It also means his right to control dissemination of information about himself.

In the case of *Olmstead v. United States* (1928)¹ the court held that privacy is the most comprehensive of the rights of man and it is the right most valued by civilized man, and therefore, should be reflected in constitution.

The current focus on the right to privacy is based on some new realities of the digital age. The digital network enters the most proximate spaces and challenges the normally accepted notions of the private. The term cyber or cyberspace has today come to signify everything related to computers, the Internet, websites, data, emails, networks, software, and data storage devices. With the passage of time, Internet becomes a basic need of an individual. We are heavily dependent on it, for social and political interactions. The online environment is quite vulnerable and is at a greater risk of being subjected to threats. Due to our increased dependency on cyberspace, it has also paved way to more threats and privacy issues.

WannaCry Ransomware attack of May, 2017 is a perfect example of how the privacy of an individual in cyberspace is vulnerable. The WannaCry virus infiltrated the NHS computer system and left it completely disabled for most of the week resulting into huge losses and data breach.

WHY IT WAS A NEED TO DECLARE PRIVACY AS A FUNDAMENTAL RIGHT?

With radical change in the means of communication and communication networks, the need for privacy and its recognition as a right has come to forefront. Protection of privacy or personal data is essential because of personal liberty and dignity. The need to protect the privacy of the being is no less when development and technological change continuously threaten to place the person into public gaze and portend to submerge the individual into a seamless web of inter-connected lives.

¹ 277. U.S. 438, (US:1928)

““Big Brother” would be watching us and privacy would be a thing of past.” Orwell’s fear stands somewhat true in this era of information and communication revolution. Legal protection for privacy existed in western countries for hundreds of year. In 1361, Justices of Peace Act in England provided for the arrest of peeping toms and eavesdroppers. Similar acts and statutes were formulated across the world for example: in 1776 in Sweden, in 1858 in France, in 1889 in Norway and in 1890 in US.

Thus, second most populated country of the world seriously required to take some bold steps to protect the privacy of an individual. Right to privacy is an important natural need of every human being as it creates boundaries around an individual where the other person’s entry is restricted

INDIAN LEGAL FRAMEWORK

In India, the discussion on right to privacy started in 1954 with M.P. Sharma² case which was followed by the year 1964 with Kharak Singh. Hon’ble Supreme Court in the former one, rejected to consider right to privacy as a fundamental right. Also, Supreme Court in People’s Union for Civil Liberties v. Union of India (1997)³ held that telephone tapping, a form of “technological eavesdropping infringed the right to privacy but denied to regard it as a fundamental right.

However, India is a signatory to the International Covenant on Civil and Political Rights 1966 (ICCPR), Article 17 of which includes protection of privacy. But treaties are not enforceable under the India Law until and unless they are incorporated into domestic law. Information Technology Act, 2000 was formulated by the government to curb the increasing problems related to cyberspace and internet. Data protection is one of those components which were taking into the consideration while formulating the law.

The government of India in the year 2013 came up with The Personal Data (Protection) Bill but the bill still remains a bill. It clearly states that “Notwithstanding anything contained in any other law for time being in force, no person shall collect, store, process, disclose or otherwise handle any personal data of another person except in accordance with the provisions of this Act.” It can be considered as the exhaustive provision as it takes into the account each and every possible aspect of data protection. But it can’t be enforced in the country till it takes the shape of an act.

² M.P. Sharma v. Satish Chandra, District Magistrate, Delhi 1. SCR 1077, (SC: 1954)

³ 1. SCC 301, (SC: 1997)

Judgment given by the Supreme Court on August 24, 2017 can be regarded as a blessing in disguise. The Supreme Court in the case of Justice K.S. Puttaswamy (Retd.) and Anr. v Union Of India And Ors clearly stated that right to privacy is now a fundamental right under article 14,19 and 21 of The Constitution of India. Court also held that protection of privacy or personal data is essential because of personal liberty and dignity.

However the same judgment is silent about various aspects which are:

1. The entire judgment is silent on the question as to what **court understands with the word 'privacy'**.
2. Court has not defined the **role of state** in establishing and implementing this right.
3. There is an ambiguity about the absoluteness of the right. Court has held that right to privacy is subjected to certain restrictions⁴. But none of the restriction has been clearly defined by the court.

INFORMATION AND TECHNOLOGY ACT, 2000

The Information Technology Act, 2000 does not deal with the issue of privacy directly but a few provisions of the statute have bearing on the right to privacy. Section 72 of the IT Act entitled "Penalty for breach of confidentiality and privacy" directly deals with 'confidentiality' and 'privacy' of individuals.

PRIVACY, TRUST AND SECURITY IN CYBERSPACE

Internet in India got a boom in 2000s. With the globalization of economic, political and social activities along with increasing use of the Internet, it was pertinent that there will arise various issue regarding security, privacy. What all happened then was purely expected. A wide range of issues need to be addressed regarding privacy and protection of personal data. These pertain to preserving the privacy rights of individuals without hampering the free flow of information and the extent to which the authorities are free to use personal data.

Protecting one's privacy means protection of right to control how personal information is collected and promulgated. Protection of privacy also includes protection against identity theft or the use of an individual's personal information for fraudulent purposes.

With the technological advancement in subsequent decades, internet has become the fastest growing means of communication. It facilitates communication through emails, chats, browsing etc. There is an increasing reliance on computers concerning all facets of life. All this has changed

⁴ Court held that national security is more important and if the authorized person of government or government itself can justify the act, no action lies against them if they have collected the data without taking consent of the person whose data has been in such situation taken.

the structure of society in a way that the computer today occupies a very important place in our lives. This lead to cyber paradox i.e. on one hand, the computer and the internet have accorded extreme privacy and on the other hand the same tools of technology allow the gagging of privacy. Even if one state has robust privacy laws, it cannot currently guarantee equivalent levels of protection once the data flow beyond its borders.

Commercial exploitation of personal data without consent of the person whose personal data is used, is already leading to an enhanced legal protection for privacy. Snooping into someone's intellectual work is a complete violation of his right to privacy. In this way, the personal liberty of an individual is lost. Private space is the very basic necessary of every human being which is being hampered in cybercrimes. Privacy in cybercrimes is at stake in various ways. Privacy is threatened by businesses and other entities that collect and manipulate personal data, criminals who steal such data or stalk people over the Internet, and governments that pursue surveillance or allow intrusive law-enforcement practices.

Sophisticated electronic capabilities to collect, analyze, manipulate, and disseminate information, as well as to enable tracking, surveillance, and interference with communications, create unprecedented challenges to privacy. Such technologies are becoming more effective, available, and affordable internationally. The other example when privacy right is infringed is when application which one downloads from stores asks permission regarding access of contacts, camera, location and all. One should think that why an application requires such private information. In this way one doesn't know that whatever the data collected goes where. The information collected after seeking permissions as mentioned above would travel to deep web and became a subject matter of commercial activity which further implies that the end points are not visible.

Encryption and decryption are the two major threats to the security of a computer. We know that TCP/IP is the protocol which is responsible for the encryption and decryption of data when the data is on the way on internet. TCP protocol divide the single set of data into different packages and then sends the same data packs to the destination. IP protocol helps the different packages to bind together again and thus made the data feasible again. Cyber world and its related crimes have no territorial barriers, and this make everything complex because evidence is very hard to come by.

What is of far greater serious concern is that cyber worms can turn everything upside down alone with a laptop as his weapon sitting in a basement or in a bathroom connecting it with a mobile

phone. Presence of threats like hacking, cookies, web bug, spamming can infringe individual's privacy in cyberspace.

An annual survey conducted by the Graphics, Visualization and Usability Center of the Georgia Institute of Technology showed that 70% of the web users surveyed cited concerns about privacy as the main reason for not registering information with web sites. 86% indicated that they wanted to be able to control their personal information. A study by TRUSTe revealed that 78% of users surveyed would be more likely to provide information to sites that offered privacy assurance.

The question now arises is that whether word "Secure" written in URL bar of any webpage ensures that the personal data or any data one has entered is completely secure? Whether the privacy policy, Terms and Conditions regarding personal data are enough to ensure data privacy or not? The W3C i.e. World Wide Web Consortium has a platform for personal privacy project i.e. P3P which offers specific recommendations for practices that will let users define and share personal information with web sites that they agree to share it with.

The same question arises when one hears about the ransomware attacks. Attacks like WannaCry and Locky acts as major threats to the privacy of an individual. The scope of cyberspace is not only limited to the emails and internet only. It also includes electronic devices such as cell phones, ATM machines as are controlled by internet etc. WannaCry is a kind of ransomware which in recent times considered affecting most number of people in the world. However in context of Indian scenario, it did not affect people at a very large scale. Every year several attacks happened with the motive to steal the sensitive data of an individual. These attacks aimed at stealing private information, financial loss, and data diddling.

IT (Use of Electronic Records & Digital Signature) Rules, 2004 clearly directed government that whatever software they use for collecting the data of general public, it is the responsibility of the concerned government to ensure that software must further ensure that the electronic record is easily accessible by the authorized persons and must be preserved properly for its lifetime.

There are two major terms used in the above statement. One is the term 'authorized' and other is 'properly'. These two terms however seems completely different but they can be linked with each other. A person having the proper authority should only be permissible to access the personal data of an individual but whether that authorized person is using that information cautiously or not, it is the responsibility of the government to check the same.

Certain sections of Information Technology Act, 2000 talks about data protection whether directly or indirectly. But the aim of the act remains unfulfilled with the evolution of technology, with the

evolution of cybercrime. The act cannot be termed as an exhaustive act as it doesn't take into the consideration some acts.

For example **Section 43(g) of Information Technology Act, 2000** reads as:

*“Penalty and compensation for damage to computer, computer system, etc. -If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network,-
(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder”*

Words ‘computer’, ‘computer system’, ‘computer network’ are defined under section 2(i), 2(j), 2(l) of IT Act, 2000 respectively. From mere reading the definitions, it becomes clear that computer, computer system or computer network does not take data into consideration consequently this section doesn't hold a person liable for any kind of assistance provided to any other person to facilitate access to ‘computer resource’ which includes ‘data’ as defined under section 2(1)(k) of IT Act, 2000.

For example, If a person ‘A’ aids ‘B’ in getting access to one ‘C’'s laptop and at the same time in getting access to data stored in the laptop. Though ‘A’ should be made liable for both the acts in the interest of natural justice and common law but this provision of the act will held ‘A’ liable only for the assistance provided by him in getting access to the computer. Therefore, the gap remains which has to be bridged and hence, this section cannot stand alone to tackle the situation of privacy.

Article 43A titled ‘Compensation for Failure to Protect Data’ of The Information and Technology (Amendment) Act, 2008 reads as

“Where a body corporate, possessing, dealing, or handling any sensitive personal data or information in a computer resource which it owns, controls or operates is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.”

This section does not include a situation where the body corporate is not negligent in implementing reasonable security practices but still they are unable to protect the data. Though the data of the party who trusted them has remained unprotected, but the act in this situation will not make the body possessing such data liable.

For instance, if data of Mr. X is being handled by ABC Corporation, and despite of maintaining reasonable security practices the corporation is not able to protect the data and somehow the data leaked or stolen, Mr. X cannot sue ABC Corporation under this section. This poses a major threat to the data protection.

It also does not include a situation where the data of a person is held by an individual and not by a 'body corporate'. Body corporate as defined by the section is "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities. For example in case of a legal guardian such as father-son, if father (legal guardian) is negligent in implementing reasonable security practices, he can't be made liable under the said section. The entire Information Technology Act, 2000 is silent on the aspect of sensitive personal information i.e. nowhere in the act, the basis for differentiating personal information with sensitive personal information are mentioned. Thus 'sensitive personal information' is very subjective in nature. Courts in each case have to decide that whether the subject matter of the case comes under the ambit of sensitive personal information or not?

According to the report of NCRB⁵, published in year 2016 for the year 2015, total number of cases registered for cybercrimes was 11,592. But there are only 20 cases registered in the same year for the offence of breach of confidentiality and privacy. Both the facts are in contrast to each other. The reason for the same is that people in country are still not aware about the consequences of breach of privacy in cyber space. Reason for this can also be the fact that it is nearly impossible for a normal citizen to tell or to identify whether his privacy in the cyberspace has been infringed or not, unless any pecuniary damage is there. Also on the same side, the existing mechanism for filing the suit for the same, the victim has to go to the adjudicator⁶, then to the cyber tribunal⁷ and as a last resort to the High Court of respective jurisdiction and then to the Apex Court of the country. And it becomes moreover evident from the fact that not a single case in India in the last several years got the compensation even of a single penny⁸.

Taking into the consideration the privacy of an individual mentioning the importance of section 66E of the same act becomes pertinent. It is one of the two sections which contain 'Privacy' in their main heading.

Section 66E of Information and Technology (Amendment) Act, 2008 reads as:

“Punishment for violation of privacy.-

⁵NCRB, Cyber Crimes, Crimes in India (Oct. 29, 2017, 3:31 PM)

<http://ncrb.nic.in/StatPublications/CII/CII2015/chapters/Chapter%2018-15.11.16.pdf>

⁶Information and Technology Act, Section 46(2000)

⁷ Information and Technology Act, Section 48(2000)

⁸ Pawan Duggal, Cyber Law. (2014)

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both”

Apparently the section seems to cover each and every possible aspect of privacy of a person. But if analyzed critically, this section can be regarded as a section without any scope. The ambit of this section is very limited to only body parts. Basically it is concerned about the privacy when talked with reference to body.

Basically none of the section of IT Act, 2000 deals with the issue of data protection and privacy of person in cyberspace.

Talking about data protection, it becomes pertinent to talk about the second section after section 66E of Information Technology Act, 2000 which contains the word ‘Privacy’ i.e. section 72 titled ‘Penalty for breach of confidentiality and privacy’ reads as

“Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.”

This section takes into consideration the acts done by the person authorized under this act which means that the scope of this section is limited.

Now the question arises that whether mere trespass to the data of an individual by a person authorized is an offence or not under this act. This section deals only with the situation when the person so authorized by the act is able to get the secured access i.e. if the said person gets access to above mentioned material in an unsecured manner. Instance of infringement of privacy of the general public can be taken from the privacy policy of companies like Uber and etc. Talking about Uber and the privacy it can be said that the privacy of data of Indians is at stake. Data controller in the case of Uber user living in United States is Uber Technologies, Inc., California. If the user lives outside United States, Uber B.V., Amsterdam, the Netherlands is the data controller. This means that the data controller in the case of Indian user is in the Netherlands.

Now the question arises that how can an Indian user ensure his data's privacy in such a situation where he is not even aware of the locality of his data. Privacy is also infringed when some applications are able to break down into one's phone and can make replicas of the data in the system of the person who wants to steal the same. Popular video of Mr. Saket Modi hacking a girl's mobile in just few seconds has gone viral on social media in recent times. This shows that how can an intruder may manage to enter into someone other's personal life and cause harm which can be unexpected.

RIGHT TO BE FORGOTTEN VIS-À-VIS RIGHT TO PRIVACY

Right to be forgotten is basically a European concept. It reflects the claim of an individual to have certain data deleted so that third person can no longer trace them. The landmark case in this regard is *Google Spain v. AEPD and Mario Costeja Gonzalez* (2014). However, there are more concerns about its relation and interaction with right to privacy. Experts say that, right to be forgotten would decrease the quality of the Internet through censorship and a rewriting of history.

For example: If one types the name of a person say Mr. A, search engine would definitely shows the most visited links about him. Now according to the above decision, if Mr. A wants to get those links deleted from the suggestion, he can do that. It is because that every person has the right to privacy and no one has the right to intrude in his/her personal life.

There is an on-going debate about its applicability in India. For example: If one political leader say Mr. ABC is contesting elections, each and every person of the respective constituency has the right to know about him. But Mr. ABC through the orders of the court, gets his information about his history, criminal records etc. deleted. He may put forward the ground of right to privacy. In this situation, unjust would be done with each and every person who has such right to know about his/her future representative. India till now, does not have any law regarding to the right to be forgotten and it can be understood that laws for each and every field is not possible, but India should be ready for some legal steps in the same field. Thus a balance has to be created and maintained so that right to be forgotten do not interfere with the right to information and right to know.

CYBER SOVEREIGNTY

Here now arises the need of concept of cyber sovereignty. Cyber sovereignty implies the desire of the government to exercise control over internet within the domestic boundaries, including political, cultural, economic and technological activities. Cyber Sovereignty is generally used in the context of the internet governance. States have sovereign power over their cyber infrastructure and that with that sovereign power come corresponding responsibility to control that infrastructure and prevent it from being knowingly used to harm other States. Despite the hesitance of States to accept responsibility for the attacks crossing their cyber infrastructure, there is a fundamental assumption in international law that authority and obligations strive to stay in balance with each other which is quite right. This balance between responsibility and authority continues to underlie the modern law of armed conflict. As a matter of sovereignty, States have the right to develop their cyber capabilities according to their own desires and resources. The State may choose to develop its cyber capabilities extensively and make them available to its citizens broadly, or it can choose to close its cyber borders to avoid outside influence and outside interference in any way.⁹ Talking about the same concept in India, it is quite difficult for the government of the largest democracy to close its cyber borders in order to avoid outside influence and outside interference by mean. But if Indian government chooses to develop its cyber borders and make them available to its citizen as a case of now, then privacy of individual citizen may get threatened. As per report published in Times of India one cybercrime took place in every 10 minutes.¹⁰ In India concept of cyber sovereignty is not so developed. However experts say that the cyber sovereignty principles need to be quickly defined so as to address not just national sovereignty and security but also to balance the state of conflict of interests in cyberspace. The cyber environment, being a worldwide worldview, should be seen from a comprehensive point of view and not from a western driven vision as it were¹¹.

⁹ Eric Talbot Jensen, *Cyber Sovereignty : The Way Ahead* TILJ 3, (2014).

¹⁰ Chethan Kumar, One cybercrime in India every 10 minutes, The Times of India , July 22,2017 at P1

¹¹ IANS, Cyber sovereignty principles need to be quickly defined, The Indian Express, February 24, 2017

CONCLUSION

Privacy is one of those values which underpin human dignity and other key values such as freedom of speech. The meaning of privacy has been evolved over the years and with its widening scope it covers more areas under its ambit.

Though no justification is required to protect privacy, its meaning is however dependent on the culture of nation. Even when privacy is recognized as a fundamental right, there is a long way to go as far as the protection of rights and data is concerned. India needs better laws and regulations to protect privacy of an individual especially when it comes to privacy in cyberspace which also includes data protection. Privacy needs to be defined in the context of cyberspace. What it means in a general context, may not mean in context of cyberspace.

One cannot deny the fact that the applicability of IT has seen a substantial rise in the present decade. However, one has to strike a balance between the two i.e. IT and privacy because privacy is quite vulnerable in cyberspace. Bill Gates gives us a good picture of the same in the chapter 'Critical Issues' of his book "The Road Ahead". He says, 'Loss of privacy is another major worry where the network is concerned'¹². Existing laws and regulations are not suffice enough to tackle the same issue. A lot has been done but a lot more has to be done in this regard. Though in 2008, IT Act has witnessed several amendments but with the changing time a few changes are required. Data forming a crucial part of the privacy of an individual needs to be protected. Cybercrime is a branch of crime which is comparatively less explored. Most of the cybercrimes committed with the intent to steal data and to cause loss to the other party whether in terms of reputation or monetary terms. In every such situation, one thing that ends up coming at the stake is privacy. Gap areas of existing laws and regulations are needed to be fulfilled. Though the fact of requirement of active role of the state in protecting privacy whether in general world or in cyberspace cannot be denied but awareness has to be bought in general public. Even today a person cannot easily identify unless any evident damage whether his data has been stolen or not. This approach of the general public has to be changed.

States have to be directed by the Supreme Court to take some effective and efficient steps to handle the problems concerning privacy in cyberspace. All the times we cannot blame the government, nor we can leave everything on the government, we should understand our responsibility and then respond to the situation. A citizen must have options to undertake basic

¹² Bill Gates, Nathan Myhrvold, Peter Rinearson, The Road Ahead 302 (1995).

digital functions like emailing, information search, social networking, etc. without sacrificing her privacy rights.