CHAPTER-I

INTRODUCTION

The recognition of 'Privacy' is deeply rooted in history and religion. Several religious Scriptures, texts, and classical write-ups recognize the importance of Privacy. There is recognition of Privacy in the Quran\(^1\) and in the sayings of Prophet Mohammed. The Bible has numerous references to Privacy and the Jewish law has long recognized the concept of 'freedom from being watched'. Fifty years ago, George Orwell, the English writer, whose fears for the loss of individual liberty dominated his novels, imagined a totalitarian state where advanced technologies would be used to monitor the people in all their endeavors. "Big Brother" would be watching us and privacy would be a thing of the past\(^2\). Orwell's fears have come true in this era of Information and Communication Revolution (ICR).\(^3\)

Privacy is a fundamental human right recognized in the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights and in many other international and regional treaties. Privacy underpins human dignity and other key values such as freedom of association and freedom of speech. It has become one of the most important human rights issues of the modern age.

Nearly every country in the world recognizes a right of privacy explicitly in their Constitution. At a minimum, these provisions include rights of inviolability of the home and secrecy of communications. Most recently-written Constitutions such as South Africa's and Hungary's include specific rights to access and control one's personal information.

In many of the countries where privacy is not explicitly recognized in the Constitution, such as the United States, Ireland and India, the courts have found that right

\(^1\) An-Noor 24:27: "O you who believed enter not houses other than your own until you have asked permission and greeted those in them, that is better for you, in order that you may remember". (Yusufali). An-Noor 24:28: "And if you find no one therein, still, enter not until permission has been given. And if you are asked to go back, go back, for it is purer for you, and Allah is All-Known of what you do." (Yusufali). Al-Hujrat 49:12: O you who believe! Avoid much suspicion, indeed some suspicions are sins. And spy not, neither back bite one another." (Yusufali).

\(^2\) Hereinafter ICR.

\(^3\) Hereinafter ICR.
in other provisions. In many countries, international agreements that recognize privacy rights such as the International Covenant on Civil and Political Rights or the European Convention on Human Rights have been adopted into law.

In the early 1970s, countries began adopting broad laws intended to protect individual privacy. Throughout the world, there is a general movement towards the adoption of comprehensive privacy laws that set a framework for protection. Most of these laws are based on the models introduced by the Organization for Economic Cooperation and Development and the Council of Europe.

The new technologies have enhanced the possibilities of invasion into the Privacy of individuals and provided new tools in the hands of eavesdroppers. Individual Privacy is at a greater stake than ever before. Computers and the Internet can be used to amass huge amount of data regarding people, profile it in various ways, commodify it and deal with it in a manner which could violate individual’s privacy.3

Modern technological innovations and developments in the field of computers and Internet have created an environment in which there is inexpensive and ready access to an ever growing pool of personal information about indefinable individuals anywhere in the cyber world. “Privacy in the technology driven world is a difficult proposition. Technology has become kind of double edged sword, on one hand it equips the person to safeguard his privacy and on the other it helps in blowing the privacy cover, one may had”.4

The Internet is a rich Source of personal information about online potential consumers. Some of the web site owners follow the consumer’s online activities and gather information about personal liking and disliking. The data so collected is valuable for a web enterprise because not only it is possible to target market produce and services but on the basis of such data they may also sell advertising space on their web sites. The personal information data may be recorded by government departments, various service providers and other organizations like insurance companies, banks, hospitals, schools, credit card companies, telephone service provider etc. This personal information may be

misused if fallen in a wrong hand. Mr. Bill Gates in his book "The Road Ahead" has expressed his concerns relating to privacy - "Loss of privacy is another major worry, where the network is concerned. The potential problem is not the mere existence of information. It is the above that make me worry".  

Privacy is a fundamental human right. It is recognized around the world in diverse regions and cultures. Though the whole world is yet to arrive at an agreed definition on privacy, the advocates of 'right to privacy' have agreed that the meaning of privacy is dependent on a nation's culture. If we look back at history, we find that a great amount of effort has been devoted to evolve paws on privacy.

Legal protection for privacy existed in western countries for hundreds of years. In 1361, the Justices of Peace Act in England provided for the arrest of peeping toms and eavesdroppers. In 1765, Lord Camden, Striking down a warrant to enter a house and seize papers wrote, "We can safely say there is no law in this country to justify the comforts of society, for papers are often the dearest property any man can have". In 1763, in his speech on the Excise Bill, British Parliamentarian William Pitt Wrote, "The poorest man may in his cottage bid defiance to all the force of the crown. It may be frail; its roof may shake; the wind may blow through it; the storms may enter; the rain may enter - but the king of England Cannot enters; all his forces dare not cross the threshold of the ruined tenements".

In 1776 the Swedish Parliament – enacted the Access to Public Records Act that required all government held information be used for legitimate purposes. Trance prohibited the publication of private facts and set stiff fines for violators in 1858. The Norwegian criminal code prohibited the publication of information relating to "Personal or domestic affairs" in 1889.

---

5 Bill Gates, the Road Ahead, 302 quoted in Yatindra Singh, Cyber Laws, 2003, p.47.
6 Justices of Peace Act, 1361 (Eng.) 34 Edw. 3, C.1; supra note 3 p.199.
7 Eutick V. Carrington, 1558-1774 AIER Rep. 45. supra note 3 p.199.
The cyber world and its related crimes have no territorial barriers, and this makes everything complex because evidence is very hard to come by. As global companies and government join e-market place and business becomes borderless, their vulnerability multiply. Privacy in these e-markets would be a major area of concern in the coming days, with greater degree of 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. And damages can take place in a matter of few seconds. Along with these damages there is harassment in several forms to an individual or a group of people online, breaking all barriers of privacy. With the privacy issue as centre stage not only at the national and international level but also about the legal Protection of Right to Privacy in the Information Technology era are important areas of discussion where in security from the technological front arises.10

1.1 The Problem

Even with the adoption of legal and other protections, violations of privacy remain a concern. In many countries, laws have not kept up with the technology, leaving significant gaps in protections. In other countries, law enforcement and intelligence agencies have been given significant exemptions. Finally, in the absence of adequate oversight and enforcement, the mere presence of a law may not provide adequate protection.

There are widespread violations of laws relating to surveillance of communications, even in the most democratic of countries. The U.S. State Department's annual review of human rights violations finds that over 90 countries engage in illegally monitoring the communications of political opponents, human rights workers, journalists and labor organizers. In France, a government commission estimated in 1996 that there were over 100,000 wiretaps conducted by private parties, many on behalf of government agencies. In Japan, police were recently fined 2.5 million yen for illegally wiretapping members of the Communist party.

10 Supra note 3, p.214.
Police services, even in countries with strong privacy laws, still maintain extensive files on citizens not accused or even suspected of any crime. There are currently investigations in Sweden and Norway, two countries with the longest history of privacy protection for police files.

Companies regularly flaunt the laws, collecting and disseminating personal information. In the United States, even with the long-standing existence of a law on consumer credit information, companies still make extensive use of such information for marketing purposes.

The increasing sophistication of information technology with its capacity to collect, analyze and disseminate information on individuals has introduced a sense of urgency to the demand for legislation. Furthermore, new developments in medical research and care, telecommunications, advanced transportation systems and financial transfers have dramatically increased the level of information generated by each individual. Computers linked together by high speed networks with advanced processing systems can create comprehensive dossiers on any person without the need for a single central computer system. New technologies developed by the defense industry are spreading into law enforcement, civilian agencies, and private companies.

According to opinion polls, concern over privacy violations is now greater than at any time in recent history\(^\text{11}\). Uniformly, populations throughout the world express fears about encroachment on privacy, prompting an unprecedented number of nations to pass laws which specifically protect the privacy of their citizens. Human rights groups are concerned that much of this technology is being exported to developing countries which lack adequate protections. Currently, there are few barriers to the trade in surveillance technologies.

It is now common wisdom that the power, capacity and speed of information technology are accelerating rapidly. The extent of privacy invasion -- or certainly the potential to invade privacy -- increases correspondingly.

\(^{11}\) Simon Davies "Re-engineering the right to privacy : how privacy has been transformed from a right to a commodity", in Agre and Rotenberg (ed) "Technology and Privacy : the New Landscape", MIT Press, 1997 p.143.
Beyond these obvious aspects of capacity and cost, there are a number of important trends that contribute to privacy invasion:

GLOBALISATION removes geographical limitations to the flow of data. The development of the Internet is perhaps the best known example of a global technology.

CONVERGENCE is leading to the elimination of technological barriers between systems. Modern information systems are increasingly interoperable with other systems, and can mutually exchange and process different forms of data.

MULTI-MEDIA fuse many forms of transmission and expression of data and images so that information gathered in a certain form can be easily translated into other forms.

The macro-trends outlined above have had particular effect on surveillance in developing nations. In the field of information and communications technology, the speed of policy convergence is compressed. Across the surveillance spectrum -- wiretapping, personal ID systems, data mining, censorship or encryption controls -- it is the West which invariably sets a proscriptive pace.\(^{12}\)

Governments of developing nations rely on first world countries to supply them with technologies of surveillance such as digital wiretapping equipment, deciphering equipment, scanners, bugs, tracking equipment and computer intercept systems. The transfer of surveillance technology from first to third world is now a lucrative sideline for the arms industry.\(^{13}\)

According to a 1997 report "Assessing the Technologies of Political Control" commissioned by the European Parliament's Civil Liberties Committee and undertaken by the European Commission's Science and Technology Options Assessment office (STOA), much of this technology is used to track the activities of dissidents, human rights activists, journalists, student leaders, minorities, trade union leaders, and political

---


\(^{13}\) Big Brother Incorporated, Privacy International site: <http://www.privacy.org/pi/reports/>. 
opponents. The report concludes that such technologies (which it describes as "new surveillance technology") can exert a powerful 'chill effect' on those who "might wish to take a dissenting view and few will risk exercising their right to democratic protest". Large scale ID systems are also useful for monitoring larger sectors of the population. As Privacy International observed, "In the absence of meaningful legal or constitutional protections, such technology is inimical to democratic reform. It can certainly prove fatal to anyone 'of interest' to a regime."

The United States Security Agency has broken privacy rules and overstepped its legal authority thousands of times each year since 2008, according to documents leaked by the whistleblower Edward Snowden, the Washington Post reported citing an internal audit and other top-secret documents. According to the report, the largest amount of intelligence was gathered from Iran, with more than 14 billion reports, followed by 13.5 billion from Pakistan. Jordan came third with 12.7 billion, Egypt fourth with 7.6 billion and India fifth with 6.3 billion.

Former CIA worker Edward Snowden revealed to the Washington Post and the Guardian that the US agency has been using tech giants Microsoft, Google, Apple, Yahoo, Face book, Skype and YouTube to spy on private information of users around the world. The PRISM programme, which has been in operation since 2007, is aimed to monitor foreign communications that take place on US servers.14

Government and citizen alike may benefit from the plethora of IT schemes being implemented by the private and public sectors. New "smart card" projects in which client information is placed on a chip in a card may streamline complex transactions. The Internet will revolutionize access to basic information on government services. Encryption can provide security and privacy for all parties.

However, these initiatives will require a bold, forward looking legislative framework. Whether governments can deliver this framework will depend on their willingness to listen to the pulse of the emerging global digital economy and to recognize the need for strong protection of privacy.

1.2 Objectives of the Study

The primary objective of the study is to analyze the serious threat to right to privacy of individual by the Information Technology and the effectiveness of the present legal mechanism to deal with it.

More specifically the objectives of the study were:

1) To make a conceptual analysis of Right to Privacy;
2) To analyze the legal protection of right to privacy at national and International level;
3) To evaluate various provisions relating to Right to Privacy under International Conventions on Human Rights, European Directives and UNCITRAL Model Laws;
4) To evaluate the provisions of Information Technology Law via-a-via Right to Privacy;
5) To determine the liability of Internet Service Providers at national and International Level;
6) To examine the Cloud Computing implications on the Right to Privacy;
7) To examine the National and International Standards on Data Protection;
8) To focus on remedies against violation of Right to Privacy;
9) Lastly, to present the major findings of the study and to offer pertinent suggestions to strengthen the legal system.

1.3 Significance of the Study

Although modern telecommunications technologies, such as computers, the Internet, and wireless communications provide tremendous convenience and tools for productivity they also raise numerous concerns and legal issues. These concerns and issues generate new responsibilities for system managers, new challenges for law enforcement, and new questions for individuals. One of the most critical of these legal issues is privacy.
Nearly everyone willingly provides very detailed private information about them on loan applications; on medical, dental, and insurance forms; and two friends, clergy, and counselors. In doing so, however, they expect control over (1) what information is collected, (2) how it is collected, (3) how it is used, (4) for what purpose it is used, (5) to whom the information is revealed or shared, (6) what information is retained in files, (7) how long the information is kept, (8) the security of the information while it is being stored to porter against the theft of the information in the system, (9) continued accuracy of the information in the file, and (10) our right to review the information and to correct errors in it. In short, everyone is willing to share private information under certain circumstances, but they do not want that information to be widely publicized without their permission. People expect their communications, whether by phone, email, the Internet, or other means, to be as safe as messages in a sealed envelope.

However with computerized databases, technology provides for the first time in history the capability to collect, organize, and store massive amounts of personal information in databases over which individuals have little or no control. Modern telecommunications networks allow that information to be accessed analyzed, and transported across the country or around the world at speeds never before possible. Information that people once believed was private and confidential is now being compiled and used without their knowledge or control. These issues affect both customers and providers of the systems.

The term privacy, used in telecommunications law today, encompasses these expectations by individuals to control the confidentiality, accuracy, and application of their personal information. Currently, however, U.S. law allows the extensive collection and use of such information without the permission of the individual. This is because U.S. law tends to view personal data as a resource to help companies identify potential customers and to serve existing customers. Other countries, such as the member states of the European Union, however, view Privacy as more of a human rights issue. U.S. Privacy law operator mainly a privacy statements offered by companies to their customers and industry codes of conducted rather than a concerted, directed body of law. This is an acceptable to other countries, and as the Internet and electronic commerce,
expend, other countries, including the European Union, have placed embargoes on personal data flows to the United States until the United States increases its protections for personal data.

In order to protect the Right to Privacy in the Information Technology Era it is necessary to make an objective assessment of the laws and policies both national and international, to ascertain whether they are efficient to protect the Right to Privacy. The present study will be highly useful to the Law makers and administrators as it seeks to strengthen the legal mechanism to prevent the misuse of technology to affect the right to privacy of individuals.

1.4 Methodology

The methodology adopted for the study is purely doctrinal. Various books, journals, magazines, International materials, treaties and conventions etc., have been studied for the collection of the data. Materials from various websites have been visited & used to get the latest information in analyzing the problem. Secondary data available from various sources have been used to support some conclusions and findings.

1.5 Limitations

The study confines itself in examining the Legal Protection of Right to Privacy from national and international perspective. Protection of Right to Privacy is investigated with reference to different national and international laws, European Directives and UNCITRAL Model Laws. The empirical study has not been undertaken in relation to the Right to Privacy in India.

The study has been confined only to the doctrinal research involving books, articles, International Documents and relevant statutory material.

Due to lack of literature in print form in this new area, the investigator has made extensive reference to the material available on the Internet.

1.6 Scheme of the study and its presentation

The Whole Study is presented in ten chapters.
Chapter I: Introduction

This chapter deals with introduction, elucidation of the objectives of the study, its significance and the methodology adopted for the study.

Chapter II: Right to Privacy as a Human Right – A Conceptual Analysis

Chapter two provides a conceptual analysis of the notion of Right to Privacy along with its different dimensions, scope and significance as a human right. The chapter reviews the literature on the difficulties of defining a right to privacy. The chapter argues in favour of an approach in accordance with which the right to privacy is justified as a necessary element of a system which adequately values and protects human autonomy. Privacy is argued, in this regard, to go beyond the simple protection of the secret or confidential so as to include the social dimension of human existence. Protecting privacy encourages the individual to fully engage in this social sphere by facilitating experimentation, intimacy and the development of a sense of individual and social identity.

The chapter then proceeds to consider the differences between privacy as an autonomy value and privacy as a legally enforceable right. It would not be workable for the law to define privacy as anything which engages individual or social identity.

The chapter then considers the extent to which a right to privacy may be regarded as a claim of control over these dimensions. It concludes that control should not be understood in this context as an all-or-nothing entitlement to prevent all access to the area in question. Privacy is a more complex and context-sensitive concept. Thus a right to privacy operates as an entitlement to exercise control over who may access a particular dimension and/or of the use that may legitimately be made of such access. Just what the right involves will depend upon the particular circumstances of the claim.

Chapter III: International Dimensions of Right to Privacy

Privacy is a fundamental right recognized in the United Nations Universal Declaration of Human Rights, the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the International
Covenant on Civil and Political Rights, and many other international and regional treaties. Privacy has been defined as the 'right of individuals to control the collection and use of personal information about themselves.' Privacy underpins human dignity and other key values such as freedom of association and freedom of speech. The right to privacy has become one of the most important human rights and ethical issues of the information age. This chapter reflects the growing importance, diversity and complexity of this fundamental right.

Nearly every country in the world recognizes the right to privacy in their constitutions or laws. While some only provide provisions for such rights as inviolability of the home and secrecy of communications, many recently written constitutions, such as South Africa and Hungary, include specific rights to access and control one's personal information. In many countries such as the United States, Ireland, and India where privacy is not explicitly recognized in the constitution, the courts or new laws have identified the right to privacy. In addition, international agreements that extol the right to privacy, such as the International Covenant on Civil and Political Rights or the European Convention on Human Rights, have been adopted into law by many countries.

Chapter three evaluates the provisions relating to the Right of Privacy in USA, the Right of Privacy in the European Union, the Right of Privacy in the Great Britain, the Right of Privacy in France, the Right of Privacy in Germany, the Right of Privacy in Italy, the Right of Privacy in the Netherlands, the Right of Privacy in Sweden.

Chapter IV: Law Relating to Right of Privacy in India – An Analysis

Privacy is the ability of an individual or group to seclude either themselves or information about themselves and thereby reveal themselves selectively. Privacy as a concept involves what privacy entails and how it is to be valued. Privacy as a right involves the extent to which privacy is (and should be legally protected). “The law does not determine what privacy is, but only what situations of privacy will be afforded legal protection.” It is interesting to note that the common law does not know a general right of privacy and the Indian Parliament has so far been reluctant to enact one.
As of now there is no enactment on Privacy in India but the Constitution of India has embodied many Rights in Part III, which are called Fundamental Rights. These are enumerated in Article 14-30 of the Constitution. But judicial activism has brought the Right to Privacy within the sphere of Fundamental Rights. Article 141 of the Constitution states “the law declared by the Supreme Court shall be binding on all courts within the territory of India.” Therefore, the decisions of The Supreme Court of India become the Law of the Land. The Supreme Court of India has come to the rescue of common citizen, time and again by construing “right to privacy” as a part of the Fundamental Right to “protection of life and personal liberty” under Article 21 of the Constitution, which states “no person shall be deprived of his life or personal liberty except according to procedures established by law”. In the context of personal liberty, the Supreme Court has observed “those who feel called upon to deprive other persons of their personal liberty in the discharge of what they conceive to be their duty must strictly and scrupulously observe the forms and rules of the law”.

Chapter four evaluates the Vedic approach to the development of Right to privacy in India, Constitutional protection with Judicial Interpretations, Privacy of Communications, Privacy of Home, Privacy of the Body, Privacy of Records, Grey areas of Right to Privacy, Emergence of the issue of Data protection and alternatives to current enforcement regimes in India.

Chapter V: An Overview of Law relating to Information Technology in the International Sphere

Information technology continues to have an ever-growing impact upon society and the way that society conducts its affairs. Information and communications technologies have permeated almost every professional, commercial and industrial activity and most organizations would find it difficult, if not impossible, to function without relying heavily on these technologies. As far as the law is concerned, computers and electronic communications networks have been a mixed blessing. They have become indispensable tools, allowing the use of massive information storage, processing, dissemination, searching and retrieval. On the other hand, information and communications technologies have posed and continue to pose novel and complex social
and legal problems. Frequently, the law has been found wanting when dealing with the issues raised by these constantly evolving technologies, and legislators and the courts have often struggled to come to terms with the challenges raised by them.

An understanding of the legal issues involved remains of key importance to persons and organizations concerned with information and communications technology, and it is only armed with such understanding that they can satisfactorily address and cater for the problems raised by the development and use of these technologies.

This chapter analyses the Evolution, Nature and concept of Information Technology and an overview of law relating to Information Technology in the International sphere.

Chapter VI: Information Technology and Threat to Privacy – An Analysis

Privacy undoubtedly connotes a very important personal right, and thus if one’s privacy is to be disturbed it ought to be done with good reason and constraint. With the advent of telecommunication and now the internet, e-commerce and e-governance, privacy has attracted much attention.

Although Information and Communications Technologies (ICTs) have greatly enhanced our capacities to collect, store, process and communicate information, it is ironically these very capacities of technology which make us vulnerable to intrusions of our privacy on a previously impossible scale. Firstly, data on our own personal computers can compromise us in unpleasant ways — with consequences ranging from personal embarrassment to financial loss. Secondly, transmission of data over the Internet and mobile networks is equally fraught with the risk of interception — both lawful and unlawful — which could compromise our privacy. Thirdly, in this age of cloud computing when much of “our” data — our e-mails, chat logs, personal profiles, bank statements, etc., reside on distant servers of the companies whose services we use, our privacy becomes only as strong as these companies’ internal electronic security systems. Fourthly, the privacy of children, women and minorities tend to be especially fragile in this digital age and they have become frequent targets of exploitation. Fifthly, Internet
has spawned new kinds of annoyances from electronic voyeurism to spam or offensive e-mail to ‘phishing’ — impersonating someone else’s identity for financial gain — each of which have the effect of impinging on one’s privacy.

Although there are a number of technological measures through which these risks can be reduced, it is equally important to have a robust legal regime in place which lays emphasis on the maintenance of privacy. This chapter looks at whether and how the Information Technology Act that we currently have in India measures up to these challenges of electronic privacy.

This chapter delves into an analysis of the present legal regime in relation to privacy as a right and a tool to protect human dignity and esteem; especially in the light of the new developments in Information Communication Technology (ICT). Modes by which one’s privacy can be encroached upon through the use of modern technology will also come into focus in this paper. Privacy has often been looked upon as an individual right, which fails to consider the broader aspect of privacy as a social right. The failure to do so generates difficulty in striking a fine balance with competing social interests such as, for example, national security. Hence, in this paper, the social implications of the right to privacy will be considered with a view to building a stronger case for providing constitutional protection for privacy — especially in the context of the modern evolution towards e-governance.

This chapter deals with threats to Right to Privacy through Technological means and tools to protect the Right to Privacy.

Chapter VII: Cloud Computing, Right to Privacy and Legal Implications

Cloud computing is the long dreamt vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud
Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public audit ability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed.

Accountability for security and privacy in public cloud deployments cannot be delegated to a cloud provider and remains an obligation for the organization to fulfill. Federal agencies must ensure that any selected public cloud computing solution is configured, deployed, and managed to meet the security, privacy, and other requirements of the organization. Organizational data must be protected in a manner consistent with policies, whether in the organization's computing center or the cloud. The organization must ensure that security and privacy controls are implemented correctly and operate as intended, throughout the system lifecycle.

Cloud computing is a new computing paradigm that is still emerging. Technology advances are expected to improve performance and other qualities of services from public clouds, including privacy and security. Many agency systems are long lived and, if transitioned to a public cloud, will likely experience technology and other changes over the course of their lifetime. Cloud providers may decide to sell or merge their offerings with other companies; service offerings may be eclipsed by those of another cloud provider or fall into disfavor; and organizations may be required to recompete an existing contract for cloud services, when all option years have been exhausted. Eventually having to displace some systems to another public cloud is a distinct possibility that federal agencies and other organizations must not overlook.

In this chapter the research investigator examines the notion of privacy, types of information that might need to be protected in cloud computing and the nature of the privacy challenge in cloud computing.

Chapter VIII: Liability of Internet Service Providers – An International perspective

Today in India, privacy is challenged perhaps the most by the internet and telecommunications. On one level the increased use of these technologies allows individuals to become more visible, accessible, and interconnected. On another level, these same forces allow governments, corporations, and other entities unrestricted access
into the lives of the public. For example, individuals are plagued with spam messages and unsolicited marketing calls/text messages; risk fraud and phishing attacks as they transact online, have personal information gathered, used, and sold without permission or knowledge, risk having ISPs retain user data and history, and risk having governments monitor online behavior and communications. Furthermore, online privacy is threatened as the user often does not have control over the information that they generate and the line between what is personal information, what is private information, and what is public information is often fuzzy. This has created a situation where information displayed on social networking sites can be used as evidence against an individual. For example, employees can look into an individual's Face book profile as part of the process for deciding whether to hire or promote a person. Information that is private, but perhaps not personal (does not identify the individual) is afforded no protection.

This chapter explores the Countries around the world have taken steps to address privacy issues that arise from the internet, including adopting legislation implementing do not track, the right to be forgotten, breach notification and data retention policies and how these policies and legislation are being implemented, and what the international best practices are.

Chapter IX: International Data Protection and Privacy Law

This chapter provides a cross-jurisdictional review of the development of regulatory instruments to protect privacy and related interests with regard to the processing of personal data. All of the instruments constituting the focus of this chapter are specifically aimed at regulating the processing of data relating to, and facilitating identification of, persons (i.e., personal data) in order to safeguard, at least partly, the privacy and related interests of those persons.

This chapter provides an overview of the main legal instruments at both international and national levels which deal directly with data privacy. Some account is also taken of instruments which formally are not legally binding but are, nevertheless, highly influential in development of regulatory policy in the field.

The legal systems of many, if not most, countries contain a variety of rules which embody elements of the basic principles typically found in data privacy instruments or which can otherwise promote these principles’ realization albeit in
incidental, ad hoc ways. However, what is primarily of interest in the following overview is the degree to which countries have adopted rule-sets that are directly concerned with promoting data privacy.

Taken together, these instruments form a field of law and policy that has attained considerable maturity, spread and normative importance over the last four decades. Well over forty countries have now enacted relatively comprehensive data protection laws. These national initiatives are augmented and often inspired by a large number of international agreements. Enveloping the regulatory field is an immense body of academic commentary analyzing privacy and data protection issues from a variety of perspectives.

This chapter examines these existing protections for personal data at the international and regional level. Section 1 focuses on the legally binding instruments of the Council of Europe and European Union. Section 2 examines the non-binding, yet influential, measures adopted by the United Nations General Assembly and Organization for Economic Cooperation and Development. Section 3 examines the Privacy law and Data Protection under the Indian Legal system.

Chapter X: Conclusion

In the last chapter an attempt is made to present the major findings of the study and to offer pertinent suggestions.