CHAPTER 7
INFORMATIONAL PRIVACY IN THE TECHNOLOGICAL WORLD

7.1 Introduction
Since the whole Universe preserves the huge sea of information, it is only an enlightened person who can fathom it. Even on our planet, every substance provides us the information about its content, form, structure, advantages or disadvantages. According to Aristotle’s Theory of Human nature, individual entities in the Universe are made out of matter and forms, and forms either are or at the very least contain information. So matter and information are significant components of every physical thing in the Universe. Aristotle’s account of perception assumes that all animals are information-processing beings whose bodily structures account for the ways in which information gets processed within them.¹

Aristotle said that Information processing within an animal’s body initiates and controls the animal’s behavior. Like other animals, humans are also information processing beings, but the ability of humans to choose their actions and control their behavior, using theoretical and practical reasoning, distinguishes humans from all other animals, and makes them ethically responsible for what they do and what they become.² It is submitted that human Beings have been transforming the information since past times. It would have been impossible for any civilized society to survive, if it could not gain the past records or information.

Obviously, in order to facilitate the management of society, the information systems- urban information systems, health information systems, business records systems, survey data banks- have been designed. Such information systems contain predominantly data about man and society.³ For a vast array of vital social and economic activities, personal data have become an indispensable ‘raw material’. For countless government and private organizations, crucial products, services, performances, and responsibilities require finely calculated use of data on the person concerned.⁴

² Ibid.
Throughout the world’s prosperous societies, it has become increasingly rare to deal with any governmental or private-sector organization without generating and relying upon a database of personal information. In recent years, the private sector has shown the greatest innovation in these respects. Medical care increasingly involves complex, multi-channel flows of information on matters ranging from the patient’s medical history and genetic inheritance to his insurance status. Credit and banking require constant accessing of account balances, recent transactions, credit history, and available credit. The sale and use of all forms of insurance are predicated on close assessment of risk and reward, cost and benefit—all requiring analysis of the experience of identifiable individuals. Marketing, in its many forms, involves analytical monitoring of consumers’ product choices and advertising susceptibilities.  

No doubt, the collection and use of personal information has become a predominant factor in the development of whole society. But at the same time, these developments have also endangered many privacy issues. In this Chapter, the privacy issues of the present information age have been explored.

7.2 Meaning of Informational Privacy

L. Floridi defines informational privacy as freedom from epistemic interference or intrusion, that is achieved when there is a restriction on facts about someone that are unknown or unknowable. Judith Wagner Decew further suggested that information about one’s daily activities, personal lifestyle, finances, medical history, and academic achievement, whether written or not, part of a public record or not, may be viewed by an individual as information he or she need not divulge and can expect others to guard as well.

Besides, Herman T. Tavani showed great concern about informational privacy in computer/informational technology. Tavani says that personal privacy can be analysed in terms of four factors— the amount of personal information that can be collected, the speed at which personal information can be exchanged, the duration of time that the information can be retained, and the kind of information that can be acquired.
7.3 Role of Technology in the Process of Data Collection

In 1973, a panel reported to the United States Secretary of Health, Education, and Welfare (HEW) on computers and privacy. The report could have been written today:

It is no wonder that people have come to distrust computer-based record-keeping operations. Even in non-governmental settings, an individual’s control over the personal information that he gives to an organization, or that an organization obtains about him, is lessening as the relationship between the giver and receiver of personal data grows more attenuated, impersonal, and diffused. There was a time when information about an individual tended to be elicited in face-to-face contacts involving personal trust and a certain symmetry, or balance, between giver and receiver. Nowadays an individual must increasingly give information about himself to large and relatively faceless institutions, for handling and use by strangers—unknown, unseen and, all too frequently, unresponsive. Sometimes the individual does not even know that an organization maintains a record about him. Often he may not see it, much less contest its accuracy, control its dissemination, or challenge its use by others.9

The report pinpointed troubles arising not simply from powerful computing technology that could be used both for good and ill, but also from its impersonal quality: the sterile computer processed one’s warm, three-dimensional life into data handled and maintained by faraway faceless institutions, viewed at will by strangers. The worries of that era are not obsolete. We are still concerned about databases with too much information that are too readily accessed; databases with inaccurate information; and having the data from databases built for reasonable purposes diverted to less noble if not outright immoral uses.10

The computer-born revolution in man’s capacity to process data is obviously an enormous boon. In business, government, medicine, science, and a dozen other fields, men are

---

now able to make more fact-based, more logical, and more predictable decisions than they could do before the age of electronic information storage and retrieval.\textsuperscript{11}

The traditional methods of gathering information have been replaced by the electronic digital computers. The recent technologies have the capacity to store more records and manipulate them more effectively and rapidly than was ever possible before.\textsuperscript{12} Every organization, by using giant computers, collects information about its employees, clients, members, taxpayers, or other persons in the interest of the organization.\textsuperscript{13}

Further advances in the computer field are rapidly accelerating the sharing of data among those who use the machines. Standardization of computer languages and the perfection of machines that translate one machine system into another have made it possible for computers to communicate directly with one another, so that data can flow in and out of separate systems. This innovation has led to information exchanges among units within the same large organization, such as police and health agencies in a state or among independent organizations with common interests, such as life-insurance companies. A more significant aspect of this trend is the growth of central data pools in many important fields, from education and health to banking, civil defense, and social-science analysis.\textsuperscript{14}

In the present era, the automatic data processing has also replaced almost every kind of cash transactions of the past. Such data processing provides the trail of records about significant transactions of the individual’s life. More and more types of transactions are being put on such credit cards- plane travel, auto rentals, hotel accommodation, dining, purchases of goods, and the like, all potential records for income-tax subpoena or criminal investigation.\textsuperscript{15} For planning, efficiency, and social control, the government data centers, computerized transaction systems, and control record files of the future could bring enormous benefits to society.\textsuperscript{16}

Meanwhile, it is pertinent to mention about Data-mining, which is being considered as the revolution in the information technology. Data mining has attracted a great deal of attention in the information industry and in society as a whole in recent years, due to the wide availability of huge amounts of data and the imminent need for turning such data into useful information and

\textsuperscript{12}\textsuperscript{12}\textsuperscript{12}\textsuperscript{12} Id., at 160.
\textsuperscript{13}\textsuperscript{13}\textsuperscript{13}\textsuperscript{13} Id., at 161.
\textsuperscript{14}\textsuperscript{14}\textsuperscript{14}\textsuperscript{14} Id., at 162.
\textsuperscript{15}\textsuperscript{15}\textsuperscript{15}\textsuperscript{15} Ibid.
\textsuperscript{16}\textsuperscript{16}\textsuperscript{16}\textsuperscript{16} Id., at 168.
knowledge. The information and knowledge gained can be used for applications ranging from market analysis, fraud detection, and customer retention, to production control and science exploration.\textsuperscript{17} Data mining is the process of discovering interesting knowledge from large amounts of data stored in databases, data warehouses, or other information repositories.\textsuperscript{18} In the world of information technology, the term “database system”, also called a Database management system (DBMS), has its own distinctive characteristics. A Database system consists of a collection of interrelated data, known as database, and a set of software programs to manage and access the data. The software programs involve mechanisms for the definition of data base structures, for data storage, for concurrent shared or distributed data access, and for ensuring the consistency and security of the information stored, despite system crashes or attempts at unauthorized access.\textsuperscript{19}

In simple words, Data mining can be defined as the use of statistical techniques to unearth previously undiscovered relationships from large volumes of data. The goal of data mining may be classification, such as trying to identify whether an individual belongs to a particular group, or it may be prediction, such as trying to identify those who will spend the most at a website.\textsuperscript{20} It means that the dossiers about one’s private lives are being strategically studied and analyzed to make judgments about the person’s tastes, preferences, behavior, and attitude.

A wide range of commercial, governmental, charitable, educational, and medical organizations make use of data mining applications. Objectives of data mining include Security, Customer relations management, Political and charitable fundraising, Credit scoring, Fraud detection, and Medical.\textsuperscript{21} Hospitals use data mining results to design emergency room protocols to deliver more effective patient care. Businesses have employed data mining to target advertising campaigns and to improve customer service.\textsuperscript{22}

Therefore, no one deliberately designs computer-based systems with the intention of creating inefficiency, hurting people, or damaging the organizational and social structures within which the system operates. The disadvantages, the dangers, and the damages that accompany

\textsuperscript{17} Jiawei Han and Micheline Kamber, \textit{Data Mining: Concepts and Techniques}, 1 (2010).
\textsuperscript{18} \textit{Id.}, at 7.
\textsuperscript{19} \textit{Id.}, at 10.
\textsuperscript{21} \textit{Ibid.}
\textsuperscript{22} \textit{Id.}, at 161.
computerization are all by-products.\textsuperscript{23} In the context of modern society and its use of computer, privacy has become the name of many problems like criminal records unfairly causing more punishment than the law provides, welfare recipients being exposed to degrading inquiries, and insurance, loans and credit being denied because of errors in semi-relevant data gathered for other purposes.\textsuperscript{24}

Indeed, the elaborate repercussions are hidden in the whole process of Data mining. It is so because of the fact that data mining involves an integration of techniques from multiple disciplines such as database and data warehouse technology, statistics, machine learning, high-performance computing, pattern recognition, neural networks, data visualization, information retrieval, image and signal processing, and spatial or temporal data analysis.\textsuperscript{25} By performing data mining, interesting knowledge, regularities, or high-level information can be extracted from databases and viewed or browsed from different angles. The discovered knowledge can be applied to decision making, process control, information management, and query processing.\textsuperscript{26}

With more and more information accessible in electronic forms and available on the web, and with increasingly powerful data mining tools being developed and put into use, there are increasing concerns that data mining may pose a threat to individual privacy and data security.\textsuperscript{27} Therefore, it is possible that the data of an individual’s personal information may be misclassified. A larger concern is the misapplication of data mining techniques. Data may also be used for unauthorized purposes.\textsuperscript{28}

The United States Government began using “watch lists” to prescreen passengers in the early 1990s. These lists contain information about people known or thought to pose a risk to aviation security. An individual whose name appears on the “no fly” list is not permitted to board an airplane. People on the “selectee” list must undergo additional screening before they are permitted to fly. Some people with names similar to those on watch lists have experienced delays and extensive screening during air travel.\textsuperscript{29} Therefore, if government computers misclassify and

\textsuperscript{24} \textit{Id.}, at 296.
\textsuperscript{25} Jiawei Han and Micheline Kamber, \textit{Data Mining: Concepts and Techniques}, 9 (2010).
\textsuperscript{26} \textit{Ibid.}
\textsuperscript{27} \textit{Id.}, at 679.
misapply the data of personal information, then it is possible that one might find himself in the “watch list” and might face difficulty at Airports.

Considering the above said problems, the European Union has identified three main trends, which pose a challenge for the protection of personal data in the future. The first threat is about the astounding capabilities of modern technologies. Secondly, the privacy concern is regarding the increased globalization of data flows. Thirdly, the access to personal data by law enforcement authorities, that is greater than ever, has put an individual’s liberty at stake.\(^{30}\)

However, the technology by itself doesn’t violate an individual’s privacy rather it’s the people using this technology and the policies they carry out that create violations. Many people are in favour of relinquishing some degree of privacy in order to enjoy the benefits of modern society. According to them, it has to be accepted that credit card transactions inevitably store the routine collection of our purchases and driving habits in a large database over which we have no control. It’s a simple bargain, albeit a Faustian one.\(^{31}\) But Simson Garfinkel does not support this tradeoff. Garfinkel said:

> I think this tradeoff is both unnecessary and wrong. It reminds me of another crisis our society faced back in the 1950s and 1960s—the environmental crisis. Then, advocates of big business said that poisoned rivers and lakes were the necessary costs of economic development, jobs, and an improved standard of living. Poison was progress: anybody who argued otherwise simply didn't understand the facts.\(^{32}\)

The author continued to say:

> Today we know better. Today we know that sustainable economic development depends on preserving the environment. Indeed, preserving the environment is a prerequisite to the survivability of the human race. Without clean air to breathe and clean water to drink, we will all surely die. Similarly, in order to reap the benefits of technology, it is more important than ever for us to use technology to protect personal freedom.\(^{33}\)


\(^{32}\) Ibid.

\(^{33}\) Ibid., at 5-6.
Therefore, it is necessary to regulate the technology. At the same time, the government should play prominent role in stopping technology and the free market from killing our privacy. Furthermore, the problem can also be diluted by way of making careful and informed consumers.34

7.4 Aggregation of Public Records and Privacy Issues

Today, every government is in dire need of data about individuals for a wide variety of important public purposes.35 Many of the government’s data-based programs involve the delivery of social services, which would be impossible without detailed information on the citizen as client, customer, or simply person to be controlled.36

The earliest mode of gathering information from every household by the government is the Census. The counting of citizens can be traced back to the Biblical recordings of Moses. In the Book of Numbers, Moses counted people in areas surrounding his kingdom in order to strengthen the count of the population under his control.37

The census provides much information to the policy makers. If the government is possessed with sufficient information about its population only then it can adopt effective measures for the promotion of welfare schemes. Therefore, it is very necessary for the people to participate in the surveys conducted by the government. However, with the passage of time, the governments have increased the questions in the questionnaires. These questions seek more personal information about people. Obviously, people would hesitate to answer such personal questions and definitely, ask stricter laws to protect the confidentiality of census data.

Meanwhile, the mobility of persons and the standardization of life in mass society have led to the development of large private and governmental investigative systems whose function is the amassing of personal dossiers of every individual. This has become the method by which a large organization makes judgments about people when it wants to hire or fire them, lend them money, or give them passports to travel abroad.38

In the present inevitable information age, the governments collect as well as maintain panoply of records about individuals, many available to the public. These records contain

34 Id., at 6.
37 http://epic.org/privacy/census/ accessed on April 13, 2012, at 3:50 p.m. IST.
38 Supra note 11 at 159.
varying kinds of information. Birth records often disclose one’s name, date of birth, place of birth, name and ages of one’s parents, and mother’s maiden name. The government also maintains driver’s license records as well as accident reports. Similarly, voting records, which can disclose one’s political party affiliation, date of birth, email address, home address, and telephone number, are publicly available. Several types of professions require state licensing, such as doctors, attorneys, engineers, nurses, police, and teachers. Property ownership records contain a physical description of one’s property, including the number and size of rooms as well as the value of the property. Police records, such as records of arrests, are also frequently made publicly available.39

Again, court records are potentially the most revealing records about individuals. Whenever a person comes into contact with the judicial system, information is released into a public record.40 For claiming compensation in the civil suits, the plaintiff usually submits his medical and psychological information. While determining the amount of compensation, the court also seeks more personal details about plaintiff’s life style, activities, and employment.41

As far as criminal cases are concerned, there is even less privacy. The personal details of an accused convicted or acquitted at trial, become public records. The court files also contain the personal details about victims of crime. Many governments maintain the database of information about prior sex offenders and usually, such information is being disclosed to public for the sake of public interest. Sometimes governments put such information about sex-offenders on their websites.42

However, for information in court records, privacy is protected by way of protective orders, which are issued at the discretion of trial court judges. Courts also have discretion to seal certain court proceedings from the public as well as court proceedings from the public as well as permit parties to proceed anonymously under special circumstances.43

In the process of such collection, the government makes dossiers on each individual’s personal information. The dangerous aspect of these dossiers lies in the fact that the individuals

41 Ibid.
42 Id., at 1147.
43 Supra note 39 at 134.
hardly know about the existence of such dossiers. They also unaware regarding the content in those dossiers.\(^{44}\)

With the advancement in the Information and Communication Technologies, the information gathered in these digital dossiers flows in between different government departments. Data also flows from government public record systems to a variety of businesses in the private sector. Indeed, many companies construct their databases by culling personal data from public records. Simultaneously, the information flows from the private sector to government agencies and law enforcement officials.\(^{45}\) The data in digital dossiers increasingly flows from the private sector to the government, particularly for law enforcement use. Law enforcement agencies have long sought personal information about individuals from various companies and financial institutions to investigate fraud, white-collar crime, drug trafficking, computer crime, child pornography, and other types of criminal activity.\(^{46}\)

Public records can help verify individual identity, investigate fraud, and locate lost friends and classmates. Public records enable law enforcement officials to locate criminals and investigate crimes, and can assist in tracking down deadbeat parents. Public records can permit people to investigate babysitters or child care professionals. Employers can use public record information to screen potential employees, such as examining the past driving records of prospective truck drivers or taxicab drivers. Criminal history information might be relevant when hiring a worker in a child care facility or a kindergarten teacher.\(^{47}\)

While providing more fuel to the repository of public records, the government also taps the personal data possessed by libraries. However, libraries have a long tradition of protecting people’s privacy, and librarians have fought efforts by the government to gather more data. An individual’s library details can reflect his personality as well as ideas or thoughts he’s possessed with. In the same fashion, the law enforcement agencies determine whether a person is likely to engage in criminal or terrorist activity in the future based on patterns of behavior, purchases and interests.\(^{48}\)

It has been seen that public libraries are committed as well as bound by laws relating to the confidentiality of the personal data. Even the government cannot access these public libraries

\(^{44}\) Supra note 11 at 160.


\(^{46}\) Id., at 5.

\(^{47}\) Supra note 45 at 142.

records. But with the increase in private libraries, the governments are easily accessing the personal data. Increasingly, the information resources provided by libraries to their users, including electronic journals, citation databases, and online reference software, are hosted not on the library’s own computer servers but on computers owned by the publisher or vendor. This may result in information being collected about library patrons without their knowledge and outside the control of the library that pays for the services.\textsuperscript{49}

However, at the same time, freedom to access public information is essential for the betterment of every democratic society. Open access to public documents serves public good. It makes the government more accountable and transparent. Public access is a check on abuse and corruption in government departments. Similarly open access to court records and police records ensures the fairness in justice. Information about a politician’s criminal history, property records, and some other personal details helps voters in casting their votes.\textsuperscript{50}

Therefore, in order to execute the objectives of transparency, almost every democratic country has adopted the laws relating to freedom of information. However, at the same point of time, such Freedom of Information laws also contains exemptions including an exemption to protect individual privacy.

The problem with information collection and use today is not merely that individuals are no longer able to exercise control over their information; it is that their information is subjected to a bureaucratic process that is itself out of control. Without this process being subject to regulation and control and without individuals having rights to exercise some dominion over their information, individuals will be routinely subjected to the ills of bureaucracy.\textsuperscript{51}

Public records contribute to this privacy problem because they are often a principal source of information for businesses in the construction of their databases. Marketers stock their databases with public record information, and the uses to which these databases are put are manifold and potentially limitless. The personal information in public records is often supplied involuntarily and typically for a purpose linked to the reason why particular records are kept. The

\textsuperscript{50} Supra note 40 at 1171.
\textsuperscript{51} Supra note 45 at 149.
problem is that, often without the individual’s knowledge or consent, the information is then used for a host of different purposes by both the government and businesses.\footnote{Ibid.}

Therefore, the privacy problem caused by public records concerns the structure of information flow—the way that information circulates throughout our society. The problem is not necessarily the disclosure of secrets or the injury of reputations, but is one created by increased access and aggregation of data.\footnote{Ibid.}

It is, therefore, interesting to mention here the public concerns regarding their privacy issues. Alan F. Westin, aptly, observed that in the period of limited information technology, public had full trust in government, business, and the non-profit sectors. People supported and participated in the information collecting processes.\footnote{Alan F. Westin, “Social and Political Dimensions of Privacy”, Journal of Social Sciences, Vol. 59, No. 2, 431-453 at 435 (2003). Available at http://onlinelibrary.wiley.eom/doi/10.1111/1540-1560.00072/pdf accessed on July 19, 2011, at 1:30 p.m. IST.} However, the advancement in physical, psychological, and data surveillance technologies alarmed the society and struggle for privacy rights was accelerated.\footnote{Id., at 436.} Initially people won the decisional privacy and thereafter, they started battle against data surveillance. This battle still continues.

In United States, after 9/11 attacks, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) was passed. Under this shield, the law enforcement agencies have received wide discretionary powers and can access any kind of records whether possessed by public entities or private entities. In granting such powers, the Fourth Amendment of the United States Constitution has also been diluted.

The most significant features of the Act of 2001 are as follows:\footnote{William C. Banks, “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)”, in William G. Staples (ed.), Encyclopedia of Privacy,. 583-588 at 584, (2007).}

- Law enforcement and intelligence agents can conduct secret searches of private homes and businesses without prior notice.
- Intelligence investigators can easily access to personal records held by libraries, health insurance companies, bookstores, schools, businesses, and civil or nonprofit organizations.
• Expanded wiretapping authorities, which permit law enforcement agents
to monitor personal Internet usage, including inbound and outbound
electronic mail traffic and sites visited on the Internet. Court orders may
be implemented nationwide ("roving wiretaps").
• Eased restrictions on foreign intelligence gathering in the United States
and greater access for intelligence investigators to information obtained
during criminal investigations.
• Greater authority to bypass court approval and obtain personal records
from financial institutions, telephone companies, and Internet service
providers.

It is submitted here that the above mentioned features clearly show the need to bring balance
between security and right to privacy.

7.5 Collection of Personal Records by Private Entities
Daniel J. Solove wrote:

[B]usinesses are collecting an unprecedented amount of personal data,
recording the items we buy at the supermarket, the books we buy
online, our web surfing activity, our financial transactions, the movies
we watch, the videos we rent, much more. Nearly every organization
and company we interact with now has tons of personal data about us.
Companies we’ve never heard of also possess profiles of us.57

Firms and other organizations generate a lot of data. Almost every private sector is using
technologies and softwares, and the firms have turned to mining their own proprietary databases.
It is because of the fact that the price of such technologies is being continuously decreased. If a
database has information for many variables on many people, it is possible to look for useful
correlations.58 Most public attention has been focused on the retention of data about customers,
but companies also collect data about their own products, their employees, or the companies they
do business with.59

The interesting aspect is that the information itself has become a valued property. A
mailing list is nothing more than a mailing list. The value is in the information it contains like

57 Supra note 48 at 56.
58 Renee Marlin-Bennett, Knowledge Power, 151 (2004).
59 Id., at 163.
potential customers’ names and their addresses. There is nothing new about selling mailing lists
or about keeping careful records. But today computers are able to combine large datasets into a
single database that can be mined to extract commercially useful information. Therefore, the
commodification of information and the ability of computers to manipulate informational data
has become potential threat to individual privacy.

Every social system, from ancient to modern, has its public sphere of personal
information. But repositories of personal information that are created and maintained strictly to
provide bases for the dealings of organizations with specific individuals are a distinctive feature
of the modern world. Over roughly the last century, such transactional systems have taken on
vast social and economic importance. They are basic to the workings of all sorts of public and
private organizations.61

Earlier, only the government was interested in collecting the personal data of social and
economic importance. But since the early 1990s, private sector has vastly been engaged in such
transactional data systems. Sophisticated strategists in the industries like consumer credit, direct
marketing, insurance, and publishing, enhanced profit by tailoring the consumers’ personal
data.62

In the cyber age, everybody inevitably leaves trails of his personal information and
hence, such personal data provides the infinite opportunities to organizations to make calculated
appeals to specific individual for commercial transactions. Therefore, commercially motivated
organizations exhaust every resource for Target Marketing and Target-Pricing. In Target-Pricing,
sellers adjust their prices by watching the consumers’ previous purchase history.63

To support this scenario, Helen Nissenbaum rightly observed:

At the heart of contemporary data harvesting is the activity known
variously as “profiling,” “matching,” “data aggregation,” and “data
mining” in which disparate records, diverse sources of information
about people, are aggregated to produce databases with complex
patterns of information….For example, A.T.&T. creating specialty
directories for customers based on the aggregated record of their 800

---

60 Id., at 164.
61 Supra note 4 at 195.
62 Ibid.
63 Id., at 196.
calls; Citicorp's analyzing the credit card purchases of customers in order to sell profiles to others; banks ... creating an expert system to categorize individuals into profile groups by pooling information about them ...; super-bureaus collecting “information available in many places—from regular credit bureaus ..., drivers’ license and motor vehicle records, voter registration lists, Social Security number lists, birth records, court records, etc.,' in order to devise comprehensive profiles about individuals that would indicate such things as: purchasing power (credit card activity index, estimated income, fixed payments, etc.), purchasing activity (active accounts, bank debits, etc.), shopping data, and demographic data (job, marriage status, dwelling type, gender, market segment, etc.).

Eventually, Consumers are obvious stakeholders in the whole process of behavioral target marketing. Consumers do have the respect for their privacy. Their unwanted dissemination of information decreases lessens their sense of autonomy. Such intrusive selling disturbs their household peace. Paradoxically consumers don’t even know about the information they gave to the marketers.

No doubt, European Union Privacy Directive and many other nations’ private-sector privacy laws required individual consent for collection or use of such data. But J.B. Rule argued, [I]Indeed, in many settings where privacy is at stake, one has to ask whether prevailing market architecture actually encourages meaningful consent.

Although it is not explicit, an individual always supplies information under this understanding that it will be used for particular purpose. If such information is being exhibited for any other purpose without his consent then it is a breach of the privacy one is entitled to expect, and an infringement of his right to choose.

---


66 Supra note 4 at 200.

Further, as soon as an individual subscribes himself with any Communications providers, like the telephone companies and Internet Service Providers, the latter collects the personal details of the former. The Internet Service Providers have access to certain kinds of transactional data. Whenever the individual downloads any software, calls anyone, sends or receives e-mail, upload videos, etc., the Internet Service Providers may make dossiers of such transactions.68

In the present world, however, all public and private entities have the same source for accessing personal data. Common source is known as Data brokers who gathers, organizes and sells the data about individuals. Employers, lenders, marketers, insurance vendors, law enforcement agencies, and others buy such data from Data brokers as per according to their needs. While Data brokers have their own multi-dimensional sources in collecting personal data which are as follows:69

- Credit-granting consortiums (banks, department stores, credit card issuers, etc.)
- Insurance or insurance applications
- Real estate transactions
- Tax records and property appraisals
- Product registrations
- Rebate forms
- Sweepstakes forms
- Store discount cards
- Telephone directories
- Billable telephone addresses
- Legal or criminal justice records
- Licensing (driver’s and other)
- Vehicle registrations
- News organizations
- Post office deliverable address counts

Some of information is voluntarily uploaded by the individual at websites or through blogging and hence made it public. Other information may also be given voluntarily but without

the realization that the information might be put to more generally use than the provider intended.\textsuperscript{70}

Certainly such practice aggravates the problem when the data is inaccurate. Data may be incorrectly entered into a database. An innocent person can be falsely arrested if law enforcement database recorded wrong information about him.\textsuperscript{71}

7.5.1 Employees’ Privacy at Workplaces

In recent times, the employers act in the capacity of communication providers when they provide sophisticated equipments to their employees. By using such equipments, the employees access cyberspace. In exchange for providing that access, employers collect every personal detail of their employees. With the help of various software and network management tools, the employers read employees’ e-mail and track employees’ every cyber activity.\textsuperscript{72} Many employers usually ask very personal questions before and during employment. They install miniature hidden cameras in the offices to prevent crime by, and to improve efficiency among their employees.\textsuperscript{73}

The right of the employer to conduct workplace surveillance as a means to protect the employer’s interest to organize work, select technology, set production standards, manage the use of facilities and other resources, is recognized by the law. However, it should be done in a fair and reasonable manner.\textsuperscript{74} Unfortunately, employers’ greed has been increased. Resultantly, with the intention to increase their profit, productivity and employees’ efficiency, they have enhanced the surveillance of their employees. It is for this reason that they are using more sophisticated surveillance techniques like Deoxyribonucleic Acid (DNA) profiling, hidden cameras, global positioning system (GPS) devices, etc. It has been seen that the employers are

\textsuperscript{70} Id., at 158.
\textsuperscript{71} Id., at 159.
\textsuperscript{72} Supra note 68.
\textsuperscript{73} Supra note 67.
\textsuperscript{74} Lucas D. Introna, “Workplace Surveillance, Privacy and Distributive Justice”, Computers and Society, December, 33-39 at 34, (2000). Available at https://cb7088bd-a-62cb3a1a-s-sites.googlegroups.com/site/lucasintrona/home/journal-publications/publication-archive-1/WorkplaceSurveillance%2CPrivacyComputersandSociety.pdf?attachauth=ANoY7cr5BiuSc3eRjapp3KsTK-1P1hiQzpJijdVAVZufPcye3A8faosBnagewiSJDAvKhcUKJuexi50c-Exr6iyYDFRCoCieP52nFe7G3S-h95FSySpcySHuJUiXM6oPbdkaWqj4l10PfHlz7EklVyWfOou8oxy4u0be3J5ibZ917Q0NQ6Pb5m2YW-7wiACNP23CvehVdaCe4QjfxKZgC4P2js326c99gb3zaDVZ30auLA4Crv6guwuRxwDwhrdT4N99c5ld88B)\textsuperscript{75} accessed on June 17, 2012, at 1:00 pm IST.
always anxious to know the results of their employees' Deoxyribonucleic Acid (DNA) sample. Deoxyribonucleic Acid (DNA) sample may provide the information about an employee’s future efficiency level, which is of great concern for the employers. Thus, by using Deoxyribonucleic Acid (DNA) report the employers may draft the contract of service as per according their own wishes. Such contract of service may result to be discriminatory in nature. If Deoxyribonucleic Acid (DNA) report discloses an employee’s future incurable disease or any other disease which could affect his services, then the employer would make contract for limited period only. After utilizing the employee’s energy, the employer may terminate his services, hence, would be violative of one’s fundamental right to livelihood.

Moreover, the use of Radio Frequency Identification (RFID) and VeriChip at the workplaces has increased the privacy concern. Radio Frequency Identification (RFID) is a generic term used to describe technologies that involve the use of data stored on small chips or tags which can be communicated to a reader from a distance by means of radio transmission. It means that the huge amount of people’s personal information can be stored on a small chip. Moreover, such information can be read from distance. Initially, the Radio Frequency Identification (RFID) devices were being used to prevent shop lifting. However, these technologies are now being used at the workplaces to monitor the employees. For the purpose of monitoring, the employers may compel their employees to wear Radio Frequency Identification (RFID) small devices on their uniforms, wrists, fingers or arms.

Indeed, Jennifer Stoddart, Privacy Commissioner of Canada, said that the ‘workplace privacy’ is a significant part of one’s personal autonomy. If the employees do not enjoy privacy at work places, then it would have bad impact on employees’ sense of dignity, their sense of freedom, and their sense of autonomy. The Commissioner said that the continual surveillance is a very dehumanizing process. Obviously, it affects the enthusiastic workforce.

Therefore, employees do expect privacy at work places, even if the place belongs to their employer. Obviously, employers need basic information about their employees for many lawful

things. However, the collection of information through illegal means, and without the consent or knowledge, is the violation of employees' privacy.

Office of the Privacy Commissioner of Canada provides certain Good Practices for Radio Frequency Identification (RFID) in the workplace, which are as follows:77

- Organization must appoint a person who will be accountable for the use of Radio Frequency Identification (RFID) systems.
- Organizations must notify the lawful purposes for which personal information is collected.
- Before collecting the personal information through Radio Frequency Identification (RFID) technology, the organizations must obtain the consent of the employees.
- The personal information can be collected and utilized for the notified purposes only.
- Organizations must retain the accurate and up-to-date information of its employees.
- Organizations must be responsible for the protection of the personal information.
- Organizations should provide adequate information and training to the employees about the functioning of Radio Frequency Identification (RFID) technology.
- Employees should have the right to access to their personal information, which has been collected by their employers.

Organizations must investigate the employees’ complaints against abuses of Radio Frequency Identification (RFID) technology.

Increasingly, developments in Human Genome Research, and its use by employers, and insurance companies have increased the danger of violation of an individual privacy.

Genetic testing can be defined as any technique that can be used to gain information about aspects of an individual that are influenced, caused by, or controlled by genes. In health care, genetic testing is used to identify predispositions to rare genetic diseases (e.g., Huntington’s

77 Supra note 75 at 18-24.
disease), to predict response to drugs, to estimate risks for developing common illnesses (e.g., some cancers), and to determine carrier status for reproductive purposes.\textsuperscript{78}

Genomic information serves public good by identifying and understanding etiology and pathophysiology of disease. With the help of Genetic testing, medicine and science have expanded the abilities to prevent and ameliorate human malady. However, such Genetic information can be used to invade a person's private lives, and family life.\textsuperscript{79}

Genomic data has the capacity to identify an individual and his family members, and can make present and future health profiles with more scientific accuracy than any other health data. Therefore, any breach of such informational privacy results into economic harms, such as loss of employment, insurance, or housing. Ultimately, it results into social stigmatization, embarrassment, loss of self-esteem, and much more psychological harm. Although genomic information cannot be fully trusted, public perception aggravates the stigma and discrimination.\textsuperscript{80}

At workplaces, the employers are easily accessing the clinical records of employees. By doing such testing, they can determine an employee's current and future capacity to perform a job. Such records can also be used for pension and health care benefit plans. Despite the existence of legal restrictions under disability discrimination, such testing is still in practice.\textsuperscript{81}

The lack of clear connection between genetic make-up and disease has raised concerns about discrimination in health insurance. Health insurers claim that good business practices require them to charge higher rates or limit available insurance to people at higher risk of developing diseases, and that all known risk factors should be considered in the risk rating. Life insurance applications generally require individuals to disclose information about themselves, their health and their lifestyles as a condition of obtaining coverage. Some life insurers have asked individuals to take genetic tests in order to determine whether they are predisposed to diseases that could make them greater risks.\textsuperscript{82}

To cope with above said problems, Lawrence O. Gostin suggested:

Maintaining reasonable levels of privacy is essential to the effective functioning of the health and public health systems. Patients are less


\textsuperscript{80} Id., at 324.

\textsuperscript{81} Id., at 321.

\textsuperscript{82} \texttt{http://epic.org/privacy/genetic/} accessed on April 15, 2012, at 9:00 p.m. IST.
likely to divulge sensitive information to health professionals, such as family histories, if they are not assured that their confidences will be respected. The consequence of incomplete information is that patients may not receive adequate diagnosis and treatment. Persons at risk of genetic disease may not come forward for the testing, counseling, or treatment. Informational privacy, therefore, not only protects patients' social and economic interests, but also their health and the health of their families and discrete populations.83

7.6 Consumers’ Privacy

7.6.1 Online Consumers’ Privacy

Many online consumers may not realize that when interacting with Web sites they are subject to privacy-related threats posed by cookies. Cookies technology enables Website owners to collect information about users’ online browsing preferences when users interact with their sites.84

Cookies are pieces of information sent by a Web server to a user's browser. Cookies may include information such as login or registration identification, user preferences, online "shopping cart" information, and so on. The browser saves the information, and sends it back to the Web server whenever the browser returns to the Web site. The Web server may use the cookie to customize the display it sends to the user, or it may keep track of the different pages within the site that the user accesses. Legitimate Web sites use cookies to make special offers to returning users and to track the results of their advertising.85

In the Behavioral marketing or targeting, the companies collect and compile the internet users’ online records. Therefore, companies monitor individual’s web browsing history, their interactions on social networking sites, the content of their emails, and the products and services they purchase. By doing this, they decipher the taste, preferences, behavior or interests of the users and accordingly, advertise their products.86

83 Supra note 79 at 321.
84 Supra note 8 at 151.
85 http://www.privacyrights.orgjis18-cyb.htm accessed on April 17, 2012, at 11:25 a.m. IST.
86 Ibid.
7.6.2 Access to Mobile Phones' Personal Information

In the history of the collection of personal information, the first revolution took place in the form of computer technology which actually replaced traditional modes of collection. Usage of Mobile phones during past decade also strengthens the bridge between communication and information. Obviously, people do have strong expectation of privacy while communicating and transacting information with each other.

However, such mobile phones have evolved from simple headsets to Smartphones which are equipped with sophisticated applications. Once installed by the user, these applications can interact with, and retrieve information from, various functions on the phone such as its camera or address book. Such “applications”, in short term, are known as “apps”. The “apps” are in the form of games, utility or any other type of program including basic torch on phones, weight-loss guide, wallpapers and Global Positioning System (GPS) softwares. Usually the app developers tag some unclear “terms and conditions” with the applications and seek users’ consent. No doubt users get fascinated with new softwares and applications, and hence, install the applications by agreeing their unclear terms and conditions. By agreeing, the users grant license to apps agreed that App developers and their advertisers now have access to their phone. With this they can now read users’ text messages, harvest e-mail addresses, take images from the camera at any time, dial any number from users’ phone and intercept the calls, and access users’ web browsing history. Unfortunately, every multi-national internet giants like Facebook, Yahoo!, Flickr, etc. are engaged in such malpractice. The apps of Facebook, twitter, or others are being downloaded to Google Android phones, Apple’s iPhone, etc. and hence. accessing the private information of users.  

For mobile apps, the Wall Street Journal reported on a study of 100 apps for the iPhone and Android, finding that more than half of them sent phone identification (IMEI) without users’ awareness or consent, while others sent age, gender and more.

Therefore, equipped with relatively powerful processors and fairly large memory and storage capabilities, smartphones can accommodate increasingly complex interactive applications. As a result, the growing amount of sensitive information shared by smartphone

---

users raises serious privacy concerns and motivates the need for appropriate privacy-preserving mechanisms.\textsuperscript{89}

Besides, among the variety of phones, smartphones in particular received incredible adoption. This trend is further propelled with the wide availability of feature-rich applications that can be downloaded and run on smartphones. For example, Google provides Android Market that contains a large collection of Android applications (or apps for short). It is important to note that these app stores or marketplaces contain not only vendor-provided programs, but also third-party apps. For example, Android Market had an increase from about 15,000 third-party apps in November 2009 to about 150,000 in November 2010. Unfortunately, recent studies reveal that there are malicious apps that can be uploaded to the app stores and successfully advertised to users for installation on their smartphones. These malicious apps will leak private information without user authorization.\textsuperscript{90}

Even if apps developers ask users’ permission before installing application, the permission mechanism is too coarse-grained for two main reasons. First, the Android permission mechanism requires that a user has to grant all the requested permissions of the app if he wants to use it. Otherwise the app cannot be installed. Second, if a user has granted the requested permissions to an app, there is no mechanism in place to later re-adjust the permission(s) or constrain the runtime app behavior.\textsuperscript{91}

To effectively protect user private information from malicious smartphone apps, there is need of a new privacy mode in smartphones. The privacy mode can be used to lock down (or fine tune) an app’s access to various private information stored in the phone. More specifically, if a user wants to install an untrusted third-party app, he can control the app’s access in a fine-grained manner to specify what types of private information (e.g., device ID, contacts, call log, and locations) are accessible to the app. Further, the user can flexibly (re)adjust at runtime the previously granted access (e.g., at install time).\textsuperscript{92}

\textsuperscript{90}Yajin Zhou et. al., “Taming Information-Stealing Smartphone Applications (on Android)”, in J.M. McCune et. al. (Eds.), \textit{Lecture Notes in Computer Science}, Volume 6740, 93-107 at 93, (2011).
\textsuperscript{91}Id., at 94.
\textsuperscript{92}Ibid.
7.6.3 Digitization of Cable Television

After the Cable Television Networks (Regulation) Amendment Act 2011, The Central Government has made it obligatory for every cable operator to transmit or re-transmit programmes of any channels in an encrypted form through a digital addressable system.93 The addressable system is an electronic device put in an integrated system through which signals of cable television network can be sent in encrypted form, which can be decoded by the device or devices, having an activated Conditional Access System at the premises of the subscriber within the limits of authorisation made, through the Conditional Access System and the subscriber management system, on the explicit choice and request of such subscriber, by the cable operator to the subscriber.94 And for this purpose ‘subscriber management system’ means a system or device which stores the subscriber records and details with respect to name, address and other information regarding channels subscribed to by the subscriber, etc.95

As per according to the Amendment Act of 2011, it is also obligatory on the part of cable operators to provide information relating to its cable services and networks to the government.96

It is very obvious that by installing set top boxes, the cable service providers can access and store the list of channels, which the subscriber watch daily. By doing this, it would become very easy for them to determine subscriber’s tastes, choices and preferences.

Furthermore, the Central Government has the right to inspect the cable network and services.97 And for this the government does not require any prior permission.98 Increasingly, the cable operator should help the Central Government for lawful interception or continuous monitoring of the cable service.99

Besides, in order to provide efficient and error-free service to the subscribers, every multi-system operator i.e. cable operator will have to set up and operationalize subscriber management system by recording and providing individualized preferences for pay channels, billing cycles, refunds etc.100 Therefore, it is possible that cable service providers may share subscribers’ information with private companies for giving better service to the subscribers.

93 The Cable Television Networks (Regulation) Amendment Act, 2011, s. 4A.
94 Id., s.4A, explanation (a).
95 Id., s.4A, explanation (f).
96 Id., s.4A (7).
97 Id., s.10A (1).
98 Id., s.10A (2).
99 Id., s.10A (4).
100 The Cable Television Networks Rules, 1994, s. 13(4).
Consequently, the private companies may use such information for telemarketing and target marketing.

So far as India is concerned, consumers’ grievances are remedied under the Consumer Protection Act 1986. Under this legislation, the National Consumer Disputes Redressal Commission has been established for protecting the consumer rights. The Commission also aims at providing less expensive redressal mechanism. Indeed, the definition of ‘unfair trade practice’ under the Act of 1986 is very wide and, hence, includes the complaints about misuse of personal data.

In Cellular Operators Ass. O.I. & Ors v. Nivedita Sharma, the Delhi High Court directed Cellular Operators Association of India to inform all its Members to immediately withdraw the list of subscribers and their mobiles telephone numbers provided by them to banks, finance companies or any other agencies or persons and give them directions in writing that they shall not use this information for any purpose whatsoever and also by way of telemarketing. It was further directed that all those agencies, banks, financial institutions or persons who are having their own directories for this purpose who are neither their subscribers nor their clients, shall disband those directories forthwith. The court also awarded compensation to the aggrieved subscribers. The court intended to bring competition among service providers. For Telecom Regulatory Authority of India (TRAI) is directed to bring in ‘number portability’. Telecom Regulatory Authority of India (TRAI) shall establish a National ‘Do Not Call Registry’ to prohibit commercial telemarketers from calling a subscriber, whose number is on the Registry. Furthermore, publicity of such Registry was also directed.

In order to curb Unsolicited Commercial Communications, therefore, the Telecom Regulatory Authority of India (TRAI) notified the Telecom Unsolicited Commercial Communications Regulations, 2007 dated 5th June, 2007, which put in place a framework for controlling unsolicited commercial communications. It envisaged establishment of a National Do Not Call (NDNC) Registry to facilitate registration of requests from customers who do not wish to receive UCC.

To implement the said regulation, Telecom Regulatory Authority of India (TRAI) decided to setup National Do Not Call (NDNC) Registry Portal. Thereafter the Telecom

---


102 http://www.nccptrai.gov.in/nccpregistiy/regulation1diccndiv.pdf accessed on June 26, 2012 at 11:00 a.m. IST.
Regulatory Authority of India (TRAI) issued “The Telecom Commercial Communications Customer Preference Regulations, 2010” which govern different aspects of the provision of telecommunications service to customers. For example, Do Not Call Registry, partially blocked category, restriction to unsolicited commercial communications, regulations on standards for quality of service, and regulation on a code of practice for metering and billing accuracy etc.

7.7 Users’ Personal Information on Social Networking Sites and Privacy Issues

Social networking sites have become a new medium of expression. It is axiomatic principle that freedom of speech and expression is a pre-condition for the betterment of democracy. For every democratic nation, it is necessary that informed citizens should participate in the making of any public policy. Obviously, the social networking sites have provided much better platform for such participation than real world ever possessed with. In recent times, everybody is admitting that Jasmine Revolution, Anna Hazare movement, etc. could become possible only because of social networking sites.

According to Barnes, Social networking sites are a group of Web sites that provide people with the opportunity to create an online profile and to share that profile with others. Social network websites are designed around the concept of social networks. A social network is a web of connections, such as a group of people who associate together. All persons are connected in some way to each other. In 1967 a psychologist named Stanley Milgram proved, in his experiment, that everybody is bound to everyone on this planet by a trail of six people. Social network sites attempt to embody these concepts. Through them, networks of friends and acquaintances can interlink their profiles, share personal information, and communicate with each other.

Indeed, social networking tools are gaining recognition in educational institutions to engage the students in creative and thought provoking ideas. Similarly, academic libraries, corporations including hospitals, etc. are very interested in such networking tools and applications because sharing knowledge and finding experts is critical to the success of the

---

105 Id., at 26.
Musicians in particular are using social networking sites to promote themselves. For example, in India, a song named “why this kolaveri, kolaveri, kolaveri dee?” skyrocketed just because of uploading it at the sites like YouTube.

The social networking sites require every user to sign up first. At the time of registration, the users at least submit their names or usernames. Later, in the site, the users make a profile which consists of detailed personal information and preferences. All users voluntarily upload their pictures, family pictures, videos, etc. on the sites like YouTube, Facebook and MySpace. Similarly, the users express their feelings, ideas, comments, etc. by way of blogging at the sites like Twitter.

Despite its social benefits, the usage of social networking sites has also raised many privacy issues. People are using these sites without any sense of responsibility and hence, infringing each other’s privacy rights. No doubt, blogging and uploading pictures or videos come within the ambit of freedom of speech and expression. But at the same time, the freedom is not absolute. Legislature is empowered to put reasonable restrictions on the freedom of speech and expression. People are aware about such restrictions in the real world, but have forgotten them in the virtual world. If there is no public interest involved, a person cannot publish someone’s picture or video without latter’s consent.

Further, due to the wide accessibility of virtual world, the privacy violations at such social networking sites have harmed the victims in both manner ways physically as well psychologically. Daniel J. Solove proved the psychological harm by discussing the story of “Dog poop girl”. This name was given to a girl when she refused to clean up her dog’s excrement on train. The fellow passenger captured her image along with dog’s excrement on the floor of train. The image, then, was disseminated in the internet world. Due to the widespread of image, the girl felt humiliation and embarrassment. It seems that she was punished disproportionately and unreasonably in the virtual world.

Similarly, David J. Houghton and Adam N. Joinson interviewed many victims of privacy violations online. Participants were asked about emotional responses to a violation of their privacy at social networking sites. A person who recently broken up with her partner, suffered a
privacy violation because this partner put details of the relationships demise onto a mutual friend’s Facebook wall. The participant felt painful experience because break up news was broadcasted everywhere on the internet. Her partner did this just after two days of break up. Therefore, due to timing and the widespread dissemination, the victim suffered emotional distress.109

Unfortunately, majority of users don’t even aware about their own privacy issues in the virtual world. The information posted to social media may be detrimental to users’ privacy and reputation. Surprisingly, such personal information is being used by companies, employers, anonymous cyber-stalkers, and the governments. It has been revealed that the social networking sites are selling the personal data of its users to third parties, in consideration of huge amount of money. The companies, who bought personal details, can easily decipher the taste and preferences of the users. Hence, they use it for behavior target marketing. Increasingly, numerous media stories report the loss of jobs, college admissions, or relationships due to the posting of photos taken in different states of intoxication.110

The employers are well equipped with sophisticated techniques through which they can have continuous surveillance on their employees. In addition to this, the employees’ personal information and status update records on the social networking sites have again increased the surveillance power of their employers. In England, an employee was fired by her employer because she wrote on her Facebook status that her job is totally boring.111

Moreover, certain information posted on social networking sites is publicly available to users and non-users alike, and is even searchable by search engines such as Google.112 But it does not mean that users don’t value privacy. They still have reasonable expectation of privacy. The problem is the lack of knowledge regarding the new softwares, applications, and technologies. The users often hurrriedly adopt new social media tools without considering service providers’ capacity and potentiality to collect the personal data of its users. Therefore, it has become necessary on the part of the social networking sites to inform the users about the

111 Supra note 109 at 75.
112 Supra note 110 at 24.
consequences of the choices, and clarify the tradeoff between publicity and privacy. Such kind of awareness may enable the users to make free and informed choices.\textsuperscript{113}

Gross and Acquisti explained that the people exchange the vast amount of personal information with strangers on social networking sites because people are unaware about wider accessibility of such networking system. Furthermore, they don’t even know the repercussions of stranger viewings. The authors reasoned that due to such lack of privacy concern, a very less number of users change their privacy settings.\textsuperscript{114} Consequently, users’ profile becomes accessible by third parties who can create digital dossiers of users’ behavior.\textsuperscript{115} Real and accurate information make it easy for stalkers to target and victimize the users.\textsuperscript{116}

With the increase in the use of social networking sites, the users are being victimized by the anonymous cyber-stalkers. When the users upload their personal details on the internet, the cyber-stalkers watch users’ every update and determine the taste, choices, behavior of preferences of the users. It was reported that, by using details, the cyber-stalkers set up the sex profile in user’s name. This led to harassment for the victims. Police and criminal justice system is still weak in dealing with such matters. However, Facebook and other social networking sites are working with police and trying to capture the malicious people. Facebook claimed that whenever an abuse is reported, they react swiftly to review the malicious content and disable the fake accounts.\textsuperscript{117}

Increasingly, what would happen if the government starts prosecuting and convicting dissenters for posting content online? This frightening story is of Shi Tao. In 2005, he composed an email from his office in China using a Yahoo account, which he then sent to a pro-democracy website in New York City. He attached to the email an article, which he wished to publish anonymously, on China’s new policies regarding crackdowns on potential pro-democracy dissidents in China. When Chinese authorities became aware of the article they considered it a breach of state secrets and sought to find out the author. They eventually received

\textsuperscript{113} Id., at 25.
\textsuperscript{115} Id., at 79.
\textsuperscript{116} Id., at 78.
\textsuperscript{117} Alexi Mostrous, “Harassment soars as Stalkers go online,” The Times, February 21, 2012.
crucial information about Shi Tao’s identity from Yahoo’s Asian business partners in Hong Kong. This evidence was then used to convict him in a Chinese court.118

7.8 Medical Privacy

Since the creation of the Hippocratic oath about 400 B.C., protecting the privacy of patients has been an important part of physicians’ code of conduct. Over time, health information has come into use by many organizations and individuals who are not subject to medical ethics codes, including employers, insurers, government program administrators, attorneys and others. As uses of medical information multiplied, so have regulatory protections for this highly sensitive and deeply personal information.119

Since the relationship between doctor and patient is fiduciary one, it becomes necessary on doctor’s part to keep the confidentiality and privacy of its patient’s health records. Over the period of time, the healthcare has become the huge source of one’s sensitive information. Health care providers, companies providing medical services, medical health organizations, etc., collect and collate the huge amount of patients’ health information. Privacy advocates have raised concerns about the ways in which a person’s medical and healthcare data can be manipulated and abused with the aid of information/computing technologies.120 Obviously, disclosure of one’s personal health report could cause an embarrassment to him. Moreover, such personal health information can be exploited discriminatorily by life insurance companies, employers, or by any person in many avenues of life.

So far as India is concerned, the legislations regarding health care system are scattered. Therefore, one has to find out the medical privacy in different statutes. The Medical Council of India’s Code of Ethics Regulations, 2002 provides the professional standards for medical practice. Under the regulations, it is the duty of physicians to protect the confidentiality of patients including their personal and domestic lives. However, the exception is that the health information will be revealed if it is required by law or if there is a serious and identified risk to a specific person and/or community. Moreover, Physicians must maintain the medical records of

119 “Medical Record Privacy” available at http://epic.org/privacy/medical/ accessed on May 29, 2013, at 5:30 p.m. IST.
120 Supra note 8 at 152.
their patients for a period of three years. Publication of photographs or case studies without 
consent by patients is prohibited.

In \textit{Mr. X v. Hospital Z},\textsuperscript{121} the Supreme Court dealt with the issue of confidentiality 
between doctor and patient. The Court admitted that ‘right to privacy’ is a basic human right, and 
may be aroused out of contract, or out of a particular specific relationship which may be 
commercial, matrimonial, or even political. It was observed that in the Doctor-patient doctors are 
morally and ethically bound to maintain confidentiality. Therefore, public disclosure of even true 
private facts may amount to an invasion of the Right of Privacy which may sometimes lead to 
the clash of person's 'right to be let alone' with another person's right to be informed. The court 
continued and observed that disclosure of even true private facts has the tendency to disturb a 
person’s tranquility. It may generate many complexes in him and may even lead to psychological 
problems. He may, thereafter, have a disturbed life all through. In the face of these potentialities, 
the Right of Privacy is an essential component of right to life envisaged by Article 21. But the 
Supreme Court held that the right to privacy is not an absolute right. It can be lawfully restricted 
for the prevention of crime, disorder or protection of health or morals or protection of rights and 
freedom of others. The court held that where the appellant was found to be HIV(+), its disclosure 
would not be violative of either the rule of confidentiality or the appellant's Right of Privacy as 
Ms. Akali with whom the appellant was likely to be married was saved in time by such 
disclosure, or else, she too would have been infected with the dreadful disease if marriage had 
taken place and consummated.\textsuperscript{122}

In the case of \textit{Neera Mathur v. LIC}\textsuperscript{123}, LIC Corporation asked its employee Neera Mathur 
to disclose the information about her menstrual cycles, conceptions and pregnancies and 
abortions. But the Supreme Court of India required the LIC Corporation to delete such questions 
as such information sought by Life Insurance Corporation of India is embarrassing and 
humiliating. In \textit{X v. Hospital Z},\textsuperscript{124} the court held that a healthy person can contract a valid 
marriage even after knowing the fact of ailment.\textsuperscript{125}

\textsuperscript{121} AIR 1999 SC 495. \hfill \textsuperscript{122} \textit{Id.}, at 501. 
\textsuperscript{123} AIR 1992 SC 392. \hfill \textsuperscript{124} AIR 2003 SC 664. 
\textsuperscript{124} \textit{Id.}, at 666. 

339
In *Sharda v. Dharmpal*, it was held that in divorce proceedings an order to undergo medical examination on strong grounds of necessity to establish a contention was held not invasive of right to privacy. Public policy requirements was permitted to prevail over private interests.

However, the Punjab and Haryana High Court in the case of *Surjit Singh Thind v. Kawaljit Kaur*, held that allowing a medical examination of a women for her virginity amounts to violation of her right to privacy and personal liberty enshrined under Article 21 of the Constitution. In this case, the wife filed a petition for divorce before lower court on the ground that the marriage has never been consummated. Whereas, the husband contended that he is not impotent and the marriage was consummated. In order to prove his contention, he filed the petition before the Hon'ble High Court and prayed that her wife’s virginity test should be conducted. But the High Court rejected the contention on the ground that such a medical examination even if it does not prove her virginity would not necessarily lead to the conclusion that the marriage with the husband-petitioner has been consummated.

In *Ms. X v. Mr. Z & Anr.*, the respondent alleged that his wife i.e. the appellant had adulterous affairs with one Jose Thomas. He also denied being the father of aborted foetus, which was discharged by his wife. In order to prove his contention, he sought directions from the court that the Deoxyribonucleic Acid (DNA) test of aborted foetus should be conducted. The Delhi High Court held that an aborted foetus was not a part of a body of women and therefore, she was not being compelled to be a witness against herself. The court held that aborted foetus was discharged by herself with her own consent, and therefore, subjected to Deoxyribonucleic Acid (DNA) test. While considering the whole facts of the case, the court held that it would not be a violation of right to privacy.

*Dr. Tokugha Yepthomi v. Appollo Hospital Enterprises Ltd & Anr. III case*, the Supreme Court held that the “Right to life” would positively include the right to be told that a person, with whom she was proposed to be married, was a victim of deadly disease, which was
sexually communicable, since right of life includes right to lead a healthy life. Moreover where there is a clash of two fundamental rights, the Right which would advance the public morality or public interest, would alone be enforced through the process of Court.  

In G.R. Rawal v. Director General of Income Tax (Investigation), the judge barred the appellant’s request for information and said that the payment of tax by a person was his personal matter, disclosure whereof had no relationship to any public activity or interest. The disclosure would also cause unwarranted invasion of privacy. The Public Information Officer (PIO) deduced that it is necessary to analyze the ambit and scope of both the expressions “personal information” (name, address, occupation, physical and mental and medical status, financial status of the person, one’s hobbies, etc.) and “invasion of privacy” when deciding if disclosure of information satisfies the larger public interest. However, an invasion of privacy and disclosure of personal information may also be justified if the larger public interest so warrants. Therefore, one’s medical and mental status or other reports like whether a person is suffering from disease like diabetes, blood pressure, asthma, Tuberculosis, cancer, etc., may be disclosed in the larger public interest. The Delhi High Court in the case of Secretary General, Supreme Court of India v. Subhash Chandra Agarwal held that “personal information including tax returns, medical records, etc. cannot be disclosed in view of Section 8(1)(j) of the Right to Information Act.” The Court, however, maintained that if it can be shown that sufficient public interest is involved in disclosure, the bar (preventing disclosure) would be lifted and after duly notifying the third party (i.e. the individual concerned with the information or whose records are sought) and after considering his views, the authority can disclose it. The Court also stated that in the case of private individuals, the degree of protection afforded (to their privacy) is greater; in the case of public servants, the degree of protection can be lower, depending on what is at stake. This is so because a public servant is expected to act for the public good in the discharge of his duties and is accountable for them.

---

134 Id., at 666.
136 Ibid.
137 Ibid.
138 AIR 2010 Del. 159.
139 Ibid.
7.9 Right to Information vis-à-vis Right to Privacy

In India, the right of the citizens to obtain information on matters relating to public acts flows from the fundamental freedom of speech and expression mentioned under Article 19(1)(a) of the Indian Constitution. Equitable, fair, transparent and justice ridden administration presupposes that persons be made aware of the law, rules, regulations and administrative guidelines by which their affairs will be governed. Moreover, the voters must have a right to know about the antecedents of their candidate. In this sense, it is clear that right to get information from public authorities is very important for every democratic set up. However, it raises the question that whether an individual has full access to all public documents? Obviously, privacy advocates want justified answer.

Right to information is not an absolute right. The Parliament has power to impose reasonable restrictions on the ‘right to information’ in the interests of sovereignty, integrity, and security of India, foreign relations, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence. It means that one’s right to information can also be curtailed for protecting an individual’s right to privacy.

Although ‘right to privacy’ has not been mentioned anywhere in the Indian Constitution, the judiciary brought it within the ambit of ‘right to life and personal liberty under Article 21 of the Indian Constitution. In Kharak Singh v. State of UP, the appellant was being harassed by the police under Regulation 236(b) of UP Police Regulation, which permits domiciliary visits at night. The Supreme Court held that the Regulation 236 is unconstitutional and violative of Article 21. It concluded that the Article 21 of the Constitution includes “right to privacy” as a part of the right to life and personal liberty.

In a very significant decision, People’s Union for Civil Liberties v. Union of India, the Supreme Court held that wiretapping invades an individual’s privacy. The Supreme Court held that the telephone tapping by Government under S. 5(2) of Telegraph Act, 1885 amounts infraction of Article 21 of the Constitution of India. The said right cannot be curtailed “except according to procedure established by law”. And the procedure should be just, fair and
reasonable. But again, right to privacy is also subject to certain restrictions. In the case Mr. X v. Hospital 'Z'\textsuperscript{146}, Supreme Court held that the right is not an absolute right. It can be lawfully restricted for the prevention of crime, disorder or protection of health or morals or protection of rights and freedom of others. The court held that where the appellant was found to be HIV(+), its disclosure would not be violative of either the rule of confidentiality or the appellant's Right of Privacy as Ms. Akali with whom the appellant was likely to be married was saved in time by such disclosure, or else, she too would have been infected with the dreadful disease if marriage had taken place and consummated.\textsuperscript{147}

Furthermore, in Peoples' Union for Civil Liberties (PUCL) v. Union of India,\textsuperscript{148} Right to privacy of an electoral candidate was held not violated by publications of details of his criminal antecedents and/or his assets and liabilities. The right to be informed of the electorate was held superior to candidate's desire for secrecy.\textsuperscript{149}

7.9.1 Publication of Judicial Proceedings

What is an information to others, according to a journalist, could be personal and sensitive information to an individual in a litigation relating to a matrimonial dispute.\textsuperscript{150} So far as court records are concerned, they are not accessible every time. It means that every court record is not accessible, and subject to certain exceptions. Many times, a statute or an enactment itself prohibits the publication of the proceedings which is being regulated under that statute or enactment. Moreover, it is upon the court to decide whether any of its judgment is reportable or not. The Madras High Court in the case of R. Sukanya v. R. Sridhar,\textsuperscript{151} held that Section 22 of the Hindu Marriage Act, 1955 recognizes the right to privacy between the parties in proceedings conducted under the Hindu Marriage Act. The court emphasized on the mandatory requirement of the section 22 which clearly demands that the proceedings under the Act should be conducted in camera. The provision continues to say that it shall not be lawful for any person to print or publish any matter relating to such proceedings and if any one contravenes such bar he is liable for punishment with a fine which may extend to one thousand rupees. Undoubtedly, the matrimonial matters which are very sensitive and personal matters, have no relation with the

\textsuperscript{146} Supra note 121.
\textsuperscript{147} Id., at 501.
\textsuperscript{148} AIR 2003 SC 2363.
\textsuperscript{149} Id., at 2364.
\textsuperscript{150} Dewan, Exhaustive Commentary on the Right to Information Act, 2005, 44 (2010).
\textsuperscript{151} AIR 2008 Mad. 244
public interest and public affairs. Therefore, the press is lawfully prohibited to publish or telecast such personal matters.152

In the case of M.P. Lohia v. State of West Bengal,153 the investigation with regard to the death of young wife was pending in the courts of law. In a magazine called “Saga” an article titled “Doomed by Dowry” was printed based on an interview of the family of the deceased. Giving version of the tragedy and extensively quoting the father of the deceased as to his version of the case and the facts narrated were all materials which could be used in the forthcoming trial in the case. The Supreme Court observed that such type of articles appearing in the media would certainly interfere with the administration of justice. The Apex court deprecated such practice and cautioned the publisher, editor and the journalist concerned responsible for such article, against such trial by media when the issue was subjudiced. The journalist concerned was asked to take note of such displeasure expressed by the Apex Court.154

Furthermore, another question arises as to whether the identity of the victim of rape or sexual offences should be disclosed in the public. The answer must be in negative. The Supreme Court of India considers sexual violence as dehumanizing act and a violation of female’s right to privacy.155 A victim of rape passes through agony and traumatic crisis.156 In such situation, the publication of the victim’s or her family member’s name, identity, or photograph may subject her to secondary victimization. Moreover, disclosure of the identity of victim of certain offences is punishable under Indian Penal Code, 1860.157 However, the prohibition of publication does not applicable in case of High Court or Supreme Court judgments. But while realizing the social victimization of victim in the offence of rape or any other sexual violence, the Supreme Court held that all lower courts, High Courts and the Supreme Court itself should not use the name of the victim in their judgments.158

Despite the persistent and prevailing friction between ‘right to know’ and ‘right to privacy’, the Supreme Court’s judgment of R. Rajagopal v. State of T.N159 is somehow a guide for every advocate. In this case, the Supreme Court showed its great concern to balance between

152 Id., at 248.
153 AIR 2005 SC 790.
154 Id., at 798.
157 Indian Penal Code, 1860, s. 228-A.
159 (1994) 6 SCC 632.
these two countervailing rights. The court mentioned that the right to privacy has two aspects i.e. privacy as a ‘Tort’ and ‘constitutional right to privacy’. The privacy as a tort provides damages, and can also be enforced against the private individuals. And the constitutional right to privacy prohibits the ‘State’ from taking any action which invades an individual’s privacy. The first aspect of privacy gets violated when a person’s name or likeness is used for advertising or non-advertising purposes without his consent. Similarly, it is not authorized for anyone to publish anything about one’s personal matters whether truthful or otherwise and whether laudatory or critical. While recognizing the fundamental freedom of press under Article 19(1) of the Indian Constitution, the court also emphasized on the reasonable restrictions in the form of law of torts providing for damage for the invasion of privacy, and sections 499/500 Indian Penal Code, 1860. However, right to privacy is not an absolute right. It is also subject to certain exceptions. Considering major legal issues, the court clearly said that neither the government nor the public officials, who apprehend that they may be defamed, have any right to impose a prior restraint on any publication (in this case, publication of the alleged autobiography of Auto Shankar). And the remedy for public officials and public figures, if any, will arise only after the publication and not before. Similarly, any publication concerning one’s personal matters or private details becomes unobjectionable if such publication is based upon public records including court records. The court reasoned that once a matter becomes public record, the right to privacy no longer subsists and it becomes legitimate for press to comment upon. However, the court restricted the press and media from publishing the name of female victims of sexual assault, kidnap, abduction or a like offence.

7.9.2 Public Officials’ Right to Privacy

Another issue is regarding right to privacy of public officials. In case of ‘public officials’ right to privacy, or for that matter, the remedy of action for damages is simply not available with respect to their acts and conduct relevant to the discharge of their official duties. This is so even where the publication is based upon facts and statements which are not true, unless the official establishes that the publication was made (by the defendant) with reckless disregard for truth. In

---

160 Id., at 640.
161 Id., at 649.
162 Id., at 650.
163 Id., at 651.
164 Ibid.
165 Ibid.
such circumstances, it is not necessary for the press or media persons to prove the truth of their writings. It would be enough for them to prove that they acted after a reasonable verification of the facts. But where the plaintiff succeeds to prove the publication false and actuated by malice or personal animosity, the defendant is liable for damages. Apart from his official duty, the public official enjoys the right to privacy for his personal matters.

While the Right to Information Act, 2005 gives the public right to access public documents, it also restricts disclosure of certain kinds of information. Sub-sections 8(1)(a) to 8(1)(j) of Section 8(1) of the Act contain a list of categories of information which are exempted from any kind of disclosure. However, under Section 8(2), all these exemptions can be waived if a public authority decides that public interest in disclosure outweighs the harm to the protected interests.

Indeed, there are two specific provisions under Right to Information Act 2005 i.e. section 8(1)(j) and section 11, which protect ‘right to privacy’ of both private individual as well as of public official.

---

166 Ibid.
167 The Right to Information Act 2005, s. 8(2).
Section 8(2) of the Right to Information Act, 2005 provides as follows:
Notwithstanding anything to the contrary in the Official Secrets Act, 1923 (19 of 1923) or any of the exemptions permissible in accordance with sub-section (1), a public authority may allow access to information, if public interest in disclosure outweighs the harm to the protected interests.
168 The Right to Information Act, 2005, s. 8(1)(j).
It provides as follows:
(1) Notwithstanding anything contained in this Act, there shall be no obligation to give any citizen—
(j) information which relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information: Provided that the information which cannot be denied to the Parliament or a State Legislature shall not be denied to any person.
169 The Right to Information Act, 2005, s. 11.
It provides as follows:
Third party information—
(1) Where a Central Public Information Officer or a State Public Information Officer, as the case may be, intends to disclose any information or record, or part thereof on a request made under this Act, which relates to or has been supplied by a third party and has been treated as confidential by that third party, the Central Public Information Officer or State Public Information Officer, as the case may be, shall, within five days from the receipt of the request, give a written notice to such third party of the request and of the fact that the Central Public Information Officer or State Public Information Officer, as the case may be, intends to disclose the information or record, or part thereof, and invite the third party to make a submission in writing or orally, regarding whether the information should be disclosed, and such submission of the third party shall be kept in view while taking a decision about disclosure of information: Provided that except in the case of trade or commercial secrets protected by law, disclosure may be allowed if the public interest in disclosure outweighs in importance any possible harm or injury to the interests of such third party.
Under section 8(1)(j) of Right to Information Act, the ‘personal information’ does not mean information relating to the information seeker, but about a third party. This is the reason why the Section states "unwarranted invasion of the privacy of the individual". If one were to seek information about himself or his own case, the question of invasion of privacy of his own self does not arise. If one were to ask information about a third party and if it were to invade the privacy of the individual, the information seeker can be denied the information on the ground that disclosure would invade the privacy of a third party. Therefore, when a citizen seeks information about his own case and as long as the information sought is not exempt in terms of other provisions of Section 8 of Right to Information Act, this Section cannot be applied to deny the information.\footnote{Shri Rakesh Kumar Singh v. Lok Sabha Secretariat, Complaint No. CIC\_WB/C2006/00223; Appeal Nos. CIC/WB/A/2006/00469; & 00394; Appeal Nos. CIC/OK/A/2006/00266, 00058/00066/00315. Available at http://www.rti.india.gov.in/cic\_decisions/CIC\_WB\_C\_2006\_00223,CIC\_WB\_A\_2006\_00469,00394,CIC\_OK\_A\_2006\_00266,00058,00066,000066,000215_M_33430.pdf accessed on May 9, 2013 at 7:30 p.m. IST.}

Section 8(1)(j) of the Right to Information Act was exhaustively analysed by the full Bench of the Central Information Commission in \textit{G.R. Rawal v. Director General of Income Tax (Investigation)}\footnote{Supra note 135.}. In this case, the judge barred the appellant’s request for information and said that the payment of tax by a person was his personal matter, disclosure whereof had no relationship to any public activity or interest. The disclosure would also cause unwarranted invasion of privacy. The Public Information Officer (PIO) deduced that it is necessary to analyze the ambit and scope of both the expressions “personal information” (name, address, occupation, physical and mental and medical status, financial status of the person, one’s hobbies, etc.) and “invasion of privacy” when deciding if disclosure of information satisfies the larger public interest.\footnote{Ibid.} However, an invasion of privacy and disclosure of personal information may also be

\begin{itemize}
\item \textbf{(2)} Where a notice is served by the Central Public Information Officer or State Public Information Officer, as the case may be, under sub- section (1) to a third party in respect of any information or record or part thereof, the third party shall, within ten days from the date of receipt of such notice, be given the opportunity to make representation against the proposed disclosure.
\item \textbf{(3)} Notwithstanding anything contained in section 7, the Central Public Information Officer or State Public Information Officer, as the case may be, shall, within forty days after receipt of the request under section 6, if the third party has been given an opportunity to make representation under sub-section (2), make a decision as to whether or not to disclose the information or record or part thereof and give in writing the notice of his decision to the third party.
\item \textbf{(4)} A notice given under sub-section (3) shall include a statement that the third party to whom the notice is given is entitled to prefer an appeal under section 19 against the decision.
\end{itemize}
justified if the larger public interest so warrants.\textsuperscript{173} The Commission said that Section 8(1)(j) excludes from disclosure an information which relates to personal information, the disclosure of which

\begin{itemize}
  \item[a)] has no relationship to any public activity or interest; or
  \item[b)] would cause unwarranted invasion of the privacy of the individual.
\end{itemize}

Moreover, Indian courts are being guided by Section 2 of the United Kingdom Data Protection Act 1998 for protecting individuals’ right to privacy in India. According to the provision, Sensitive Personal Data read means personal data consisting of information as to:

\begin{itemize}
  \item[a)] The racial or ethnic origin of the data subject
  \item[b)] His political opinions
  \item[c)] His religious beliefs or other beliefs of a similar nature
  \item[d)] Whether he is a member of a Trade Union
  \item[e)] His physical or mental health or condition
  \item[f)] His sexual life
  \item[g)] The commission or alleged commission by him of any offence
  \item[h)] Any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.
\end{itemize}

Therefore, such provision of ‘sensitive personal information’ is also helpful for protecting public officials’ right to privacy.

In the case of \textit{Vijay Prakash v. Union of India},\textsuperscript{174} the writ petitioner wanted an access to his wife’s service information. His contention was that being a public official, his wife is under an obligation to make proper and truthful disclosure. However, the Central Information Commission rejected his plea on the ground that it lacks any public interest, as the petitioner wanted his wife’s information for the divorce proceedings only. The Delhi High Court stated that the Section 8(1)(j) of the Right to Information Act embodies the exception of information in the possession of the public authority which relates to a third party. In simple words, this exception is that if the information concerns a third party (i.e. a party other than the information seeker and the information provider) unless a public interest in disclosure is shown, information would not

\textsuperscript{173} Ibid.
\textsuperscript{174} AIR 2010 Del. 7
be given. Information may also be refused on the ground that disclosure may result in unwarranted intrusion of the individual. Significantly, the enactment of 2005 makes no distinction between a private individual third party and a public servant or public official third party.\textsuperscript{175}

In this case, the court also outlined two types of information which cannot be accessed. The court observed that the first category of inaccessible information refers to the matters of the general public good, such as security of State, matters relating to investigation, sensitive cabinet deliberations, etc. However, in such cases the relevant authorities will have to prove the damage. The second class of information with public agencies is the personal data of both citizens and artificial or juristic entities, like corporations. Individuals’ personal data is protected by the laws of access to confidentiality and by privacy rights.\textsuperscript{176}

In this case, the court also felt the practical difficulties in differentiating public and private details of the public servants. For this, the Delhi High Court said that a distinction must be made between ‘official’ information inherent to the position and those that are not, and therefore affect only public official’s private life. If public access to the personal details such as identity particulars of public servants, i.e. details such as their dates of birth, personal identification numbers, or other personal information furnished to public agencies, is requested, following considerations will be taken into account:

i) whether the information is deemed to comprise the individual’s private details, unrelated to his position in the organization, and,

ii) whether the disclosure of the personal information is with the aim of providing knowledge of the proper performance of the duties and tasks assigned to the public servant in any specific case;

iii) whether the disclosure will furnish any information required to establish accountability or transparency in the use of public resources.\textsuperscript{177}

Finally, the court acknowledged that the degree of protection of right to privacy is greater in case of private individuals. And it can be lower in case of public servants depending on what is at stake.\textsuperscript{178}

\textsuperscript{175} \textit{Id.}, para 17.
\textsuperscript{176} \textit{Id.}, para 15
\textsuperscript{177} \textit{Id.}, para 20.
\textsuperscript{178} \textit{Id.}, para 22.
The Delhi High Court in the case of Secretary General, Supreme Court of India v. Subhash Chandra Agarwal, 2009 held that “personal information including tax returns, medical records, etc. cannot be disclosed in view of Section 8(1)(j) of the Right to Information Act.” The Court, however, maintained that if it can be shown that sufficient public interest is involved in disclosure, the bar (preventing disclosure) would be lifted and after duly notifying the third party (i.e. the individual concerned with the information or whose records are sought) and after considering his views, the authority can disclose it. The Court also stated that in the case of private individuals, the degree of protection afforded (to their privacy) is greater; in the case of public servants, the degree of protection can be lower, depending on what is at stake. This is so because a public servant is expected to act for the public good in the discharge of his duties and is accountable for them.

Considering the accountability of a public post, the Central Information Commission in its number of decisions has declared that Section 8(1)(j) of the Right to Information Act is unavailable to the public servants in the following situations:

- Public authorities cannot deny the access to the information relating to Appointments, promotions and upgradations.
- Documents regarding the transfer of two of his colleagues, vis-à-vis whom he felt that he had been discriminated against, have to be disclosed.
- Details of leave taken by the public servant have to be disclosed. However, the purpose for which the leave was taken need not be given because it is exempted under section 8(1)(j) of the Right to Information Act.
- Rules governing salary, service matters, study leave records, Posting and transfer information of public servant can’t be called ‘personal information’.
- Public officers’ tour programme is not personal information.
- Personal Information sought by legal heir of the deceased employee is not exempted to him.

In the similar fashion, the Kerala High Court in the case of Canara Bank v. Central Information Commission, held that the information relating to posting, transfer and promotion of clerical staff of a bank do not pertain to any fiduciary relationship of the bank with the its

---

179 Supra note 138.
180 AIR 2007 Ker. 225.
employees within the meaning of expression ‘fiduciary’ under section 8(1)(e). The court reasoned that without knowing this information, one employee cannot know his rights vis-à-vis other employees. The court further held that the disclosure of such information would not cause unwarranted invasion of privacy of the other employees in any manner insofar as that information is not one which those employees can keep to themselves.\(^{181}\)

At the same time, it has also been recognized that privacy will not be violated unless there are good and sufficient reasons to disclose, as the concerned party may suffer incalculable and irretrievable harm by unjustified disclosures. The Central Information Commission, in many other decisions has not allowed disclosure of income tax returns, Permanent Account numbers, details filed for tax determination, bank accounts, sources of funds, partnership details, plan to run dealership etc.\(^{182}\)

From above, it has been observed that the private individual third party enjoys greater degree of protection. Moreover, the information in respect of details of customers, and private individuals, etc., falls under the exceptions of right to information given under section 8 of the Right to Information Act. The Punjab and High Court said that the competitive position of the third party including an information relating to commercial confidence, trade secrets or intellectual property cannot be sought as the same is barred under Section 8(1)(d) of the Right to Information Act. It has been further observed that personal information and the information between the person in fiduciary relationship, is exempted from disclosure under the Right to Information Act.\(^{183}\) In order to give reasonable protection to third party’s (including both public servant as well as private individual) personal information, Section 11\(^{184}\) of the Right to Information Act requires the concerned Public Information Officer to provide proper hearing to the third party before disclosing his or her personal information. The Gujarat High Court in \textit{Reliance Industries Ltd. v. Gujarat State Information Commission},\(^{185}\) held that it is duty vested in the Public Information Officer to give an opportunity of personal hearing to the third party, to get his submissions, whether he treats the information should be disclosed, if the information is relating to or is supplied by the third party. In one of the case, an employee was reinstated with back wages subject to the condition that the employee was not gainfully employed anywhere.

\(^{181}\) \textit{Id.}, at 230.
\(^{182}\) \textit{Id.}, at 232.
\(^{183}\) \textit{Rajan Verma v. Union of India, Ministry of Finance, Banking Division, New Delhi, 2008 (2) CCC 335 (P&H)}.
\(^{184}\) \textit{Supra} note 168.
\(^{185}\) AIR 2007 Gujar 203.
However, the employer came to know about his employment in a foreign country and, remittances made by him to the bank. When the employer requested the bank to provide details of the remittances, the bank refused to provide any of his details on the ground of secrecy and confidentiality. But the Division Bench of Kerala High Court favoured the disclosure of financial details for protecting the bank, or persons interested, or the public, against fraud or crime.  

7.9.3 Awareness among Public Information Officers (PIOs) about the Exemptions under Right to Information Act

It is mandatory for the Public Information officers to know provisions of section 8(1) of the Right to Information Act 2005 and to develop a clear understanding of it, so that any denial of requested information clearly falls within its scope. The Public Information Officer must also know that mere quoting of a clause of section 8(1) is not sufficient and it should be backed by reasonable justification. It will also be useful for public authorities, researchers, activists, and citizens to be aware of these provisions and judgements relating to these aspects.

In this context, it is worth noting that the Report of the National Sub-Committee of Chief Information Commissioners of nine states and a Central Information Commissioner (July 2008) stated that in fulfilling their role as adjudicators and regulators, they face considerable handicap. Firstly, the suppliers of information, public authorities, and PIOs are not properly trained and secondly the seeker of information, the common citizen is not yet fully aware of his empowerment and the procedure for securing access of information. The sub-committee concluded that many matters need not have been brought up for adjudication at all, if well informed Public Information Officers and information seekers had resolved the issue at the outset. The sub-committee recommended the need for the appropriate mechanism to bring uniformity and clarity in interpretation of the Right to Information Act by exchange of information on case law interpretation.

---

188 Ibid.
7.9.4 Whether a Bank or financial institution has any right to publish the photograph of the defaulting borrower in newspapers

In another case of Mr. K.J. Doraisamy v. The Assistant General Manager, State Bank of India, the Madras High Court dealt with the question as to whether a Bank or financial institution has any right to publish the photograph of the defaulting borrower in newspapers, and if such whether it violates one’s right to privacy. In this case, the Bank issued a notice to defaulter under Section 13(2) of the Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act (SARFAESI Act). The provision also empowers the Banks to publish the photograph of defaulters and sureties in the newspapers. Therefore, the Bank threatened the defaulter to recover the loan by enforcing the security and bringing it to sale by publishing his photograph in the newspaper. The Madras High Court observed that the Act was enacted with a view to protect the interests of Banks and financial institutions. Considering the overriding effect of ‘public interest’ on an individual’s ‘right to privacy’ and Banks’ duty to maintain secrecy, the Madras High Court held that if borrowers could find newer and newer methods to avoid repayment of the loans, the Banks are also entitled to invent novel methods to recover their dues.190

7.9.5 Is Prisoner’s Detail Subject to Right to Information Act

So far as prisoner’s detail is concerned, it is being considered as a public document. In the case of A.S. Lall v. AA & Dir. Gen. (Prisons), Prison HQs. Central Jail, Tihar and another,191 details about the lodgment of an accused in Delhi jails was sought under Right to Information Act. But the Public Information Officer refused to give details. He contended that the disclosure of such information would amount to unwarranted invasion of individual’s privacy because it has no relationship with any public interest. However, Central Information Commission did not agree that the information was barred by the provision under Section 8 (j) of the Act. The lodgment in jail of an accused, whether on conviction by a court of law, or as an under trial, cannot be classified as “personal information” or “invasion of privacy”. The

189 Writ Petition No.17761 of2006. Available at http://indiankanoon.org/doc/251249 accessed on May 31, 2012 at 12:00 p.m. IST.
190 Id., para 32.

353
lodgment in jail of an accused or a convict is information which properly belongs to the public domain and every citizen has a right to access it.\textsuperscript{192}

In the case of \textit{Surup Singh Hrya Naik v. State of Maharashtra},\textsuperscript{193} the facts were like that a Member of Legislative Assembly was sentenced to one month imprisonment by the Supreme Court of India for the contempt of court. However, he remained in the hospital, where his medical treatment was conducted for 21 days. An application under Right to Information Act was moved, and sought from the hospital the medical reports of the MLA. It was contended by the applicant that it is in the public interest to know why a convict is allowed to stay in an air conditioned comfort of the hospital. The court held that the confidentiality of a convict’s medical records under the Regulations framed by the Medical Council of India cannot override the provisions of the Right to Information Act. Therefore, if there is any inconsistency occurs in between the Medical Council’s Regulations and the Right to Information Act, the provisions of the Act would prevail.\textsuperscript{194} Moreover, the court held that the Parliament/Legislature and/or its Committees are entitled to the records even if they be confidential or personal records of a patient.\textsuperscript{195} The court continued to say:

\begin{quote}
Once a patient admits himself to a hospital the records must be available to Parliament/Legislature, provided there is no legal bar. We find no legal bar, except the provisions of the Regulations framed under the Indian Medical Council Act. Those provisions, however, would be inconsistent with the proviso to Section 8(1)(j) of the Right to Information Act. The Right to Information Act would, therefore, prevail over the said Regulations.\textsuperscript{196}
\end{quote}

However, the juvenile’s right to privacy must be protected from undue publicity. In order to protect him or her from stigmatization, it is necessary on the part of the authorities not to disclose any name or information which may lead to the identification of the juvenile offender. In principle, the juvenile's or child's right to privacy and confidentiality shall be protected by all

\textsuperscript{192} \textit{Ibid}.
\textsuperscript{193} \textit{AIR 2007 Bom. 121}. Available at \url{http://indiankanoon.org/doc/570038} accessed on May 31, 2012 at 12:00 p.m.
\textsuperscript{194} \textit{Ibid.}, at 856.
\textsuperscript{195} \textit{Ibid.}, at 857.
\textsuperscript{196} \textit{Ibid}.
means and through all the stages of the proceedings and care and protection processes. Therefore, the whole inquiry of juvenile in conflict with law is required to be conducted in camera proceedings. Only few individuals like parents or guardian, lawyer, probation officer are authorized to attend the whole proceedings. It has to be done for keeping the juvenile’s information confidential.

7.9.6 Cyber Crimes Invade Informational Privacy

Computer crime can be broadly defined as a criminal act either aimed at a computer or carried out with its assistance. This includes the unauthorized use of, or access to, information systems, or the modification of programs either for profit or for malicious intent.

The most public manifestation of computer crime is the practice known as hacking, which basically entails use of the telephone system to gain unauthorized access to computer systems and their data. Hacking is defined as a search for access codes. This search can be random or can use highly sophisticated techniques to avoid detection. Manual hacking, using only a telephone is also known as finger hacking and is the technique of trying number after number until a valid access code is detected. Computer hacking uses computers programmed to dial target numbers and to search for access codes either sequentially, randomly or algorithmically.

In the case of computer crime, criminals have devised a variety of means of gaining illegal entry, sometimes from the same site and frequently from a remote location. Prominent among methods employed for remote intrusion into systems are virus, worms and Trojan horses.

Computer viruses are programs that modify other programs and reproduce endlessly, infecting other programs. Much as happens in the case of biological viruses, the virus invades the computer system by means of an infected program, which then replicates by instructing the host program to insert fragments of code into other programs. The infected programs proceed to pass on the virus until the point is reached at which with the infection sufficiently spread, the viruses become active and destroy all software on the system.
A worm is a program that replicates itself and spreads from one computer to another. A worm is a standalone program. It is suited to ‘sneaking’ from one computer site to another computer site. Once the work has sneaked into the target computer system, it may leak information to the outside world, destroy the system, or simply become a nuisance and slow the computer down to a sluggish pace. A worm is the most technically sophisticated form of attack on a system. It is the least likely to be detected and is superb at leaking sensitive information.\footnote{\textit{ibid.}}

A Trojan horse is a set of program procedures that will sometimes perform unauthorized functions but will usually allow the program to perform its intended purpose. For example, someone who wants to destroy a database might send its owners a file which, when run, can be silently destroy the database.\footnote{\textit{Id., at 108.}}

No doubt, Internet has improved the mode of communication and advanced the level of education, but it is still largely unregulated. Laws relating to online privacy are under development. In the virtual world, various malpractices are violating an individual’s informational privacy.

Another problem is of identity fraud or theft, one of cyber crime in which a person’s personal data (e.g., Identification numbers, address, or financial information) is used by someone else who assumes the identity of that person in order to obtain credit or money or to commit a crime in that person’s name. The victims of such crime obviously face serious repercussions. They will have to spend much time and money to restore their status.\footnote{\textit{Id., at 108.}}

Similarly, Phishing is the crime of sending fraudulent e-mails, presumably in the name of banks or e-commerce websites such as eBay or PayPal, to trick e-mail recipients into entering their personal information (including passwords, user names, address information, and credit card numbers) to a fraudulent website. It becomes very difficult for victims to detect fraud because these fraudulent websites are usually designed in such a manner that it appears authentic. Phishers use such the stolen personal data in many ways like use it directly to obtain credit, make purchases, or pursue criminal activities in the victim’s name.\footnote{Doreen Starke-Meyerring and Laura Gurak, “Internet”, in William G. Staples (ed.), \textit{Encyclopedia of Privacy}, (2007), 297-310, at 300.\footnote{Id., at 309.}}

Cybercrime like identity theft has countless repercussions. It is not only confined to financial harm but victim’s everyday life will be affected. The dossiers of personal information,
once polluted by thief, will continue to harm the victim if police fails to arrest the culprit. Further, such crime is a social problem. The terrorists’ engagement in identity theft is serious threat to the security of people. The identity theft also results into the losses to creditors, financial institutions and companies.  

7.10 Digital Right to be Forgotten

In the digital age, it has become very hard to delete the personal information from the internet because internet records everything and forgets nothing. People are feeling repentance on voluntary uploading of their photos, blogs, status update or any other personal information, on internet. European regulators felt users’ difficulty and proposed an alternative to such problem. In January 2012, the European Commissioner for Justice, Fundamental Rights, and Citizenship, Viviane Reding, announced “right to be forgotten” as a new privacy right. Therefore, most debated privacy right has now got codification in the proposed data proposed regulation. While announcing the privacy right, she emphasized that the personal data should be removed from the system if there is no legitimate reason to keep it. 

The basis of the “right to be forgotten” is French law, which recognizes “right of oblivion”. By exercising right of oblivion, a convicted criminal, who has served his time and been rehabilitated, can object the publication of the facts of his conviction and incarceration. However, in America, First Amendment protects such publication. 

The rationale behind restrictions on the publication of criminal’s history is that once a convict has served his sentence he should be free from having past criminality taints their reputation. Similarly, in the United States some states allow for sealing and expunging records of juvenile offenders. Obviously youthful offenders are first time offenders and should be rehabilitated. By considering the traditional rationality, in addition to rehabilitated criminals the European Commission in 2010 proposed to extend the right to be forgotten to the personal data of all persons.

207 Id., at 1246.  
209 Ibid.  
In the European Commission’s Communication of 4th November 2010, the right to be forgotten was defined as:

[T]he right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes.\(^{211}\)

Interestingly, the responsibility of search engines was the main issue at the heart of court proceedings in Spain which have become known as the ‘Spanish Google’ case. In this case, the Spanish data protection authority ordered Google to remove links and to stop indexing information about citizens who filed formal complaints with the data protection authority. Google criticized this, claiming that it would amount to censorship and has contested the order in some cases. Google received some sympathy for its arguments from the media and press.\(^{212}\)

However, the law on the right to be forgotten is not yet clear. Even Viviane Reding noted that such right is not absolute and favored the balance between right to be forgotten and freedom of speech and expression.

\textbf{7.11 Privacy Enhancing Techniques}

Privacy-Enhancing techniques have been devised for internet users so that they can have control over their personal data. Furthermore, it allows users to log, archive and look up past transfers of their personal data, including what data has been transferred, when, to whom and under what conditions. It also aware users about their legal rights regarding data inspection, correction and deletion.\(^{213}\)

Herbert Burkert defined Privacy Enhancing Technologies (“PETs”) as:

[T]echnical devices organizationally embedded in order to protect personal identity by minimizing or eliminating the collection of data that would identify an individual or, if so desired, a legal person.\(^{214}\)

---


\(^{213}\) [http://en.wikipedia.org/wiki/Privacy-enhancing_technologies](http://en.wikipedia.org/wiki/Privacy-enhancing_technologies) accessed on April 20, 2012, at 4:00 p.m. IST.

A. Michael Froomkin argued that although use of privacy-destroying technologies by
governments and businesses has threatened an individual’s informational privacy, everything is
not lost yet.\textsuperscript{215} Advancement in science and technology has decreased the costs of data collection
and increased the quantity and quality of data.\textsuperscript{216} He said that privacy-destroying technologies
can be responded by deploying privacy-enhancing techniques and other privacy protection
technologies in a system design. In addition to privacy-enhancing techniques, some other
techniques can also be used by people for self-help. Such technologies may either hardware or
software. Among hardware there are devices like masks or thick curtains. Similarly some
softwares like Platform for Privacy Preferences (“P3P”).\textsuperscript{217}

The World Wide Web Consortium (W3C), an international nonprofit consortium
devoted to the development of technology standards for the World Wide Web, has developed a
standard called Platform for Privacy Preferences (P3P) that provides Internet users with more
transparency and control regarding the data collection processes of websites. Using Platform for
Privacy Preferences (P3P)-enabled browsers, users can compare their privacy preferences with
those of the websites they are visiting and forgo visiting websites whose privacy standards do not
meet their expectations.\textsuperscript{218}

Many data security-enhancing techniques have been developed to protect data. Databases
can employ a multilevel security model to classify and restrict data according to various security
levels, with users permitted access to only their authorized level. Encryption is another technique
in which individual data items may be encoded. This may involve blind signatures (which build
on public key encryption), biometric encryption (e.g., where the image of a person’s iris or finger
print is used to encode his or her personal information), and anonymous databases (which permit
the consolidation of various databases but limit access to personal information to only those who
need to know; personal information is encrypted and stored at different locations). Intrusion
deletion is another active area of research that helps protect the privacy of personal data.\textsuperscript{219}

Privacy-preserving data mining is a new area of data mining research that is emerging in
response to privacy protection during mining. It is also known as privacy-enhanced or privacy-

\textsuperscript{215} A. Michael Froomkin, “The Death of Privacy?,” Stanford Law Review, Vol. 52, No. 5, 1461-1543 at 1540 (May,
2000).
\textsuperscript{216} Id., at 1464.
\textsuperscript{217} Id., at 1529.
\textsuperscript{218} Doreen Starke-Meyerring and Laura Gurak, “Internet,” in William G. Staples (ed.), Encyclopedia of Privacy,
\textsuperscript{219} Jiawei Han and Micheline Kamber, Data Mining: Concepts and Techniques, 680 (2010).
sensitive data mining. It deals with obtaining valid data mining results without learning the underlying data values. There are two common approaches i.e. secure multi-party computation and data obscuration. In secure multiparty computation, data values are encoded using simulation and cryptographic techniques so that no party can learn another’s data values. This approach can be impractical when mining large databases. In data obscuration, the actual data are distorted by aggregation or by adding random noise. The original distribution of a collection of distorted data values can be approximated using a reconstructions algorithm. Mining can be performed using these approximated values, rather than the actual ones.220

It is submitted that both public and private agencies have widened their processes of collecting individuals’ personal information for multiple purposes. However, the information processors have failed to provide adequate security to the collected personal data. Similarly, law is either inefficient or insufficient to regulate the collection, collation, storage, or disclosure of personal information. Therefore, answer to the problem lies in both technological and legal solutions.

Scott McNealy, head of the computer company Sun Microsystems, famously commented in 1999, “You already have zero privacy. Get over it.” McNealy has been quoted so often that it appears he touched a nerve.221

Privacy is in danger from private businesses that exploit data for marketing purposes, and from information sharing between public and private institutions. Overzealous investigators’ use of privately compiled data is of special concern, as is the danger that official lists made for one purpose will be used for another. There are too many possible exceptions to laws that supposedly protect records from disclosure in areas such as health and education.222

220 Id., at 681.
222 Ibid.