48.Amchem Products Inc. v. British Columbia, [1993] 1 S.C.R. 897.

CHAPTER 6: RIGHT OF PRIVACY AND INTERNET

1. INTRODUCTION

Privacy is a fundamental human right. It protects human dignity and other values such as freedom of association and freedom of speech. It has become one of the most important human rights of the modern age [1].

Privacy is recognized around the world in different regions and cultures. It is protected in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and in many other international and regional human rights treaties. Nearly every country in the world includes a right of privacy in its constitution. At a minimum, these provisions include rights of inviolability of the home and secrecy of communications. In many of the countries where privacy is not specifically recognized in the constitution, the courts have found that right in other provisions. In the United States, the concept of privacy has evolved since it was first articulated by Justice Brandeis in 1898. His definition of privacy - "The right to be let alone" (Brandeis and Warren, 1890) - has been influential for nearly a century. In the 1960s, 1970s, and 1980s, the proliferation of information technology (and concurrent developments in the law of reproductive and sexual liberties) prompted further and more sophisticated legal inquiry into the meaning of privacy. Justice Brandeis's vision of being "let alone" no longer suffices to define the concept of privacy in today's digital environment, where personal information can be transported and distributed around the world in seconds.

With the growth and development of new technological advancements, society and government also recognized its importance. The surveillance potential of powerful computer systems prompted demands for specific rules governing the collection and handling of personal information.

The genesis of modern legislation in this area can be traced to the first data protection law enacted in Germany in 1970. This was followed by national laws in Sweden (1973), the United States (1974), Germany (1977), and France (1978). At the fragent end of 2000, ideas about privacy became more complex. It reflected, the rapid and remarkable advances in computers that have made storage, manipulation, and sharing of data. At unprecedented rate.

2. EVOLUTION AND GROWTH OF CONCEPT OF PRIVACY

Privacy is a concept that is often discussed but seldom defined. Raymond Wacks, Tom Gerety, and Stephan have expressed the view that the concept of privacy is vague, perhaps too vague for definition or description [2]. In general the concept of privacy is different from the 'right to privacy'. Our claims to the privacy will be protected only upto that extent which is determined by law. The term "privacy" is used frequently in ordinary language as well as in philosophical, political and legal discussions, yet there is no single definition or analysis or meaning of the term. The concept of privacy has broad historical roots in sociological and anthropological discussions about how extensively it is valued and preserved in various cultures. The recognition of privacy is deeply rooted in history.

The origin of the concept of privacy may be traced into the natural instincts of a man who seeks to preserve a private realm of his own. The observation of Justice Cobb appears to be the correct when he said in Pavsich case that the right to privacy is derived from Natural law. He observed: "The right to privacy has its foundations in the instincts of nature..." [3]. There is recognition of privacy in the *Qur'an* [4] and in the sayings of Mohammed [5]. The Bible has numerous references to privacy [6]. Jewish law has long recognized the concept of being free from being watched [7]. There were also protections in classical Greece and ancient China [8]. Legal protections have existed in Western

countries for hundreds of years. In 1361, the Justices of the Peace Act in England provided for the arrest of peeping toms and eavesdroppers [9]. In 1765, British Lord Camden, striking down a warrant to enter a house and seize papers wrote, "We can safely say there is no law in this country to justify the defendants in what they have done; if there was, it would destroy all the comforts of society, for papers are often the dearest property any man can have"[10]. Parliamentarian William Pitt wrote, "The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storms may enter; the rain may enter - but the King of England cannot enter; all his forces dare not cross the threshold of the ruined tenement"[11].

Various countries developed specific protections for privacy in the centuries that followed. In 1776, the Swedish Parliament enacted the Access to Public Records Act that required that all government-held information be used for legitimate purposes. France prohibited the publication of private facts and set stiff fines for violators in 1858 [12]. The Norwegian Criminal Code prohibited the publication of information relating to "personal or domestic affairs" in 1889 [13].

In 1890, American lawyers Samuel Warren and Louis Brandies wrote a seminal piece on the right to privacy as a tort action, describing privacy as "the right to be left alone. Following the publication, this concept of the privacy tort was gradually picked up across the United States as part of the common law. The modern privacy benchmark at an international level can be found in the 1948 Universal Declaration of Human Rights, which specifically protects territorial and communications privacy [14]. Article 12 states:

"No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks".

Numerous international human rights treaties specifically recognize privacy as a right [15]. The International Covenant on Civil and Political Rights (ICCPR), Article 17 [16], the United Nations Convention on Migrant Workers, Article 14 [17], and the UN Convention on Protection of the Child, Article 16 [18] adopt the same language [19].

Discussion of the concept is complicated by the fact that privacy appears to be something we value to provide a sphere within which we can be free from interference by others, and yet it also appears to function negatively, as the cloak under which one can hide domination, degradation, or physical harm to women and others.

Today, when we talk about privacy, we are often talking about personal autonomy as it relates to information about an individual. Privacy entails an individual's right to control the collection and use of his or her personal information, even after he discloses it to others. When individuals provide information to a doctor, a merchant, or a bank, they expect that those professionals or companies will collect the information they need to deliver a service and use it for that sole purpose. Individual expect that they have the right to object to any further use. Implementation of principles of fair information practices - notice, choice, access, security, and enforcement - is key to preserving this autonomy by ensuring that an individual's privacy interests in his or her personal information are protected.

Privacy today also refers to protection from government surveillance. The Fourth Amendment of the US Constitution , originally intended to protect citizens from physical searches and seizures, establishes an expectation of privacy in communications as well. New technologies that enhance the ability of law enforcement to monitor communications and compile an array of information about an individual, test the limits of Fourth Amendment protections and require that we revisit and redefine our established ideas about this constitutional protection. (Similarly Fourth Amendment protection against search and seizure was also extended later in the twentieth century to cover telephone wiretaps and electronic surveillance).

The earliest arguments by Warren and Brandeis for explicit recognition of privacy protection in law were in large part motivated by expanding communication and technology. It is now clear that many people still view privacy is a valuable interest, and feel that it is now more at threat, than ever

due to technological advances. There are massive databases and Internet records of information about individual financial and credit history, medical records, purchases and telephone calls, for example, and most people do not know what information is stored about them or who has access to it.

3. DEFINING PRIVACY IN DIGITAL AGE

Privacy is a concept that is neither clearly understood nor easily defined. Of all the human rights in the international catalogue, privacy is perhaps the most difficult to define [20]. Definitions of privacy vary widely according to context and environment.

In many countries, the concept has been fused with data protection, which interprets privacy in terms of management of personal information. Outside this, in rather strict context, privacy protection is frequently seen as a way of drawing the line at how far society can intrude into a person's affairs [21]. The lack of a single definition should not imply that the issue lacks importance. Ability for others to access and link the databases, with few controls on how they use, share, or exploit the information, makes individual control over information about oneself more difficult than ever before.

4. VARIOUS ASPECTS OF PRIVACY [22]

Privacy can be divided into the following separate but related concepts:

- Information privacy, which involves the establishment of rules which governs the collection and handling of personal data such as credit information, and medical and government records. It is also known as "data protection";
- Bodily privacy, which concerns with the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches;
- Privacy of communications, which covers the security and privacy of mail, telephones, e-mail and other forms of communication; and

- Territorial privacy, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks.

The Internet is at once a new communications medium and a new locus for social organization on a global basis. Because of its decentralized, open, and interactive nature, the Internet is the first electronic medium to allow every user to "publish" and engage in commerce. Users can reach and create communities of interest despite geographic, social, and political barriers. The Internet is an unprecedented mechanism for providing invaluable information to government, social organizations, health care, and educational institutions. As the World Wide Web has grown fully support voice, data, and video, it has become a virtual "face-to-face" social and political medium.

However, it remains an open question whether the Internet's democratic potential will be achieved. The Internet exists within social, political, and technological contexts that can impede its democratic potential. Governments propagate the Internet, but worry about its threat to their traditional authority. The private sector sees the economic potential of the Internet, but anti-competitive impulses are also part of the scene. Users bring not only their social aspirations to the Internet, but also their potential for antisocial behavior. Adopting the frontier metaphor, we are now witnessing the struggle over governance of the Internet. After the revolution, what type of constitution do we want? Will it be truly democratic? Will it incorporate a bill of rights that protects individual liberty and equality? [23]

Protection of privacy is one of the critical issues that must be resolved. Will the "Digital Age" be one in which individuals maintain, lose, or gain control over information about themselves? In the midst of this uncertainty, there are reasons for hopefulness. Of course, Individuals operating on the Internet can use new tools for protecting their privacy. From anonymous mailers and web browsers that allow individuals to interact anonymously, to encryption programs that protect e-mail messages as they pass through the network; individuals can harness the technology to promote their privacy. Equally

important is the newfound voice of individuals. Using e-mail, Web sites, list servers, and newsgroups, individuals on the Internet are able to quickly respond to perceived threats to privacy.

But it is not just individuals' self-interest leading us toward increased privacy protection. Faced with numerous surveys documenting that the lack of privacy protections is a major barrier to consumer participation in electronic commerce, businesses are beginning to take privacy protection more seriously. Numerous efforts at self-regulation have emerged; such as TRUSTe [24]. A growing number of companies, under public and regulatory scrutiny, have begun incorporating privacy into their management process and actually marketing their "privacy sensitivity" to the public. The collective efforts pose difficult questions about how to ensure the adoption and enforcement of rules in this global, decentralized medium. Governments are also struggling to identify their appropriate role in this new environment.

While expectations of privacy are under serious challenge, the self-interest of the various constituencies that make up the Internet—i.e. users, advocates, industry, and government--are all pushing toward the adoption of technologies and rules that provide individuals with greater control over their information and their privacy.

5. HOW INTERNET IS DIFFERENT

Internet is an ocean of information. A person can collect information by clicking on the mouse from any nook and corner of the world. If we are to design system that protect privacy on the Internet--a globally, networked environment--we must understand the specific challenges to privacy posed by its functions and use. The Internet presents a series of new challenges for achieving public policy goals--be they protecting children from inappropriate material or protecting privacy.

Individuals give their personal information regarding their financial status to the Banks, patients give their personal information regarding the ailments from which they suffer to the doctors, individuals also give their personal information

to the insurance company while taking insurance. Further while subscribing for the new credit card one had to give his personal information. All this information, which was earlier, noted down on the papers, now stored in the hard drive of doctor, insurance company, or credit card company's computers. There are very fair chances that if this information is passed on to somebody else which an individual is not aware about, it would surely amount to breach of right of privacy. Modern technology had brought along with it its own dark side. Hackers are hacking the computers for such information. Cookies also provide such valuable information to the owner of the website.

In following ways Internet is differing as compared to other means of communications:

A. Large amount of Data Creation and Collection

Data collection is one of the most important feature of Internet. The Internet accelerates the trend toward increased information collection, which is already evident in our offline world. The massive flow of data trail, known as transactional data, which the individual leaves behind him while surfing on the web provides rich source of information about their habits of association, speech, and commerce.

This information also includes, the Internet protocol address ("IP address") of the individual's computer, the computer type, and what the individual did on previous visits to the Web site. This data, which may or may not be enough to identify a specific individual, is captured at various points in the network and available for reuse and disclosure. Along with information intentionally revealed through purchasing or registration activities (like on-line purchase, subscribing for new credit card etc), this transactional data can provide a "profile" of an individual's activities. When aggregated, these digital fingerprints reveal the blueprint of an individual's life. This increasingly detailed information is bought and sold as a commodity by a growing assortment of players.

B. Globalization of Information

Another important feature of Internet is, the information and communications flow uninterruptedly across national borders. The individual by clicking to the mouse can, reach to the information stored at the very distance place. Just as the flow of personal information across national borders poses a risk to individual privacy, citizens' ability to transact with entities in other countries places individual privacy at risk in countries that lack privacy protections. At times, if National laws are insufficient, it may fail to provide necessary privacy protections, across the borders.

C. No Centralized Control

Earlier, before the Internet was developed, it was possible for the government to control the flow of information about the individual because the transactions were taking place in the paper-based world. Also, there was there was centralization of the control mechanism. However, when the transactions are done through Internet, things changes. As Internet is decentralized mechanism, information in a networked environment flows effortless from country to country, organization to organization, and policy regime to policy regime. Effective monitoring of the generation, collection, and flow of information on this vast scale is a difficult task.

In addition to the difficulty of enforcing rules, governments around the world are struggling with how to develop appropriate and effective rules. Efforts to use legal and regulatory instruments developed to address issues in other media—broadcast or telephone may not be effective in this digital world [25].

Along with this, the characteristics of the new medium pose challenges to our traditional methods of implementing policy and controlling behavior. If we want to provide full privacy to the information that flows through this uncharted territory, we have to use all of the tools at our disposal, like, --international agreements, legislation, self-regulation, public education, and the technology itself. We must begin by reaching consensus on what we mean by protecting privacy, but we must also keep the characteristics of the online environment in focus. Concentrating in this manner is essential for the nature of the Internet and may alter the manner through which we achieve our goals.

6. WHAT DO WE MEAN BY PRIVACY AND HOW IT IS VIOLATED ON INTERNET

Privacy is a concept that is difficult to define. It means many things to many people and different things in different contexts. For the purpose of our discussion, we will examine some important "privacy expectations" that individuals have long held, and which should carry over to their interactions on the Internet that are under threat.

A. The Expectation of secrecy

Imagine that you are walking through a shopping mall, and you are unaware about a sign on your back which tells everyone which store you visited, where you have been, what you looked at, and what you purchased. Something very close to this is possible—when you are on the Internet. When individuals surf the World Wide Web, they have a general expectation of secrecy, more so than in the physical world where an individual may be observed by others. If an individual has not actively disclosed information about herself, she believes that no one knows who she is or what she is doing. But Internet generates an elaborate trail of data detailing every stop a person makes on the Web. This data trail may be captured by the individual's employer if he/she logged on at work, and is captured by the Web sites the individual visits [26]. Transactional data can provide a "profile" of an individual's online life.

Technologies such as "cookies [27] written directly onto your hard drive, enable Web sites to secretly collect information about your online activities and store it for future use. The secret collection of information about individual's activities, across multiple Web sites enabled through some "cookie" implementations, has gained the attention of Internet users, technicians, and policy makers. It is through these cookies, that your personal information is disclosed to websites. (It is through these cookies that we get Junk mail/spams in our mailbox). Evidence of the growing market for detailed "personal profiles" of individuals has became rampant on the Internet. Whether one surfs through search

engines or through portals, the pervasive use of "cookies" to collect your personal information on the net has become rampant in the cyberspace.
The business community's appetite for information is also getting worst. Last August, some of the largest commercial sites on the World Wide Web announced that they would provide all information about their customers' reading, shopping, and entertainment habits into a system developed by a Massachusetts company that was already tracking the moves of more than thirty million Internet users, recording where they go on the Internet and what they read, often without the users' knowledge [28]. In a sense, the system does what direct mail companies have done for years. But Internet based systems can be more precise, determining not only which magazines you subscribe to, but also which articles you read.

While the public and the press have scrutinized the private sector uses of personal information generated by use of the Internet, the government's interest in and use of it has received less attention. But governments are also interested in this data too. In this world of competition information is the power. Both government and the private sector have their eye on this location information. While the government seeks to build added surveillance features into the network and ensure their access to the increasingly detailed data it captures, the private sector is considering how to use this new form of information for making money out of it.

In the physical world, individuals can choose to purchase goods and services with a variety of payment mechanisms, the most common being cash, check, bank card, credit card, and a prepaid stored value mechanism, such as a travelers check or smart- card. Individuals can, and often do, pay by cash. This individual's choice of payment mechanism impacts a lot on her privacy. The amount of personal information generated and collected through the use of Internet varies from, transaction to identity, item or service purchased, merchant, and date and time in a credit transaction. In the same way, the list of parties who have access to personal data can range from - the individual and the merchant in a cash transaction, to the merchant, affiliated issuer, transaction processor, credit card company, and individual in a credit card

transaction. In general, cash provides the most privacy protection during financial transactions in the offline world. It is largely untraceable, and because its value is inherent and irrefutable, it requires no additional assurance of authenticity, which often drives the collection of identity information.

In the online environment, the digital equivalent of cash has not yet achieved widespread use. Most online purchases are made with credit cards, which identify the individual and facilitate the collection of purchasing data. The lack of cash equivalent in the online world, and its reduced use in the physical world, will seriously alter the privacy of individual's financial dealings [30]. For example, consider the differences between an auction sale in the physical world and auction sale done via Internet. Attendees at a traditional auction while physically present do not reveal who they are prior to participation. While, in an auction sale via net, individual must provide a name, home address, phone number and e-mail address. The differences between the information collected to support a similar activity in these two environments to some degree reveals the increased emphasis placed on knowing the identity of the individual with whom you are interacting where the payment mechanism is less secure than what cash affords.

B. The anticipation of Control Over Personal Information

When individuals provide information to a doctor, a merchant, insurance company or a bank, they anticipate that those professionals/companies will base the information collected on the service and use it for the sole purpose of providing the service requested. The doctor will use it to tend to their health, the merchant will use it to process the bill and ship the product, and the bank will use it to manage their account--end of story.

Unfortunately, current practices, both offline and online, frustrate this expectation of privacy. Whether it is medical information, or a record of a book purchased at the bookstore, information generated in the course of a business transaction is routinely used for a variety of other purposes without the individual's knowledge or consent. Some entities go so far as to declare the

information individuals provide them as company "property." There are multiple examples of companies using and disclosing personal information for purposes well beyond what the individual intended:

For example, recent news stories have focused the public on misuses of personal health information by the private sector--particularly when it is digitized, stored and manipulated. Recently, the Washington Post reported that CVS drug stores and Giant Food were disclosing patient prescription records to a direct mail and pharmaceutical company [31]. The company was using the information to track customers who failed to refill prescriptions, and then sending them notices encouraging them to refill and to consider other treatments [32]. Due to public outrage and perhaps the concern expressed by senators crafting legislation on the issue of health privacy, CVS and Giant Food agreed to halt the marketing disclosures. But the sale and disclosure of personal health information is big business.

In a recent advertisement Patient Direct Metromail advertised that it had 7.6 million names of people suffering from allergies, 945,000 suffering from bladder-control problems, and 558,000 suffering from yeast infections [33].

While many expect strong concern for privacy to surround sensitive information such as health and financial records, several recent incidents involving the sale and disclosure of what many perceive as less sensitive information indicate a rising of privacy concerns among the public. In recent years, a number of corporations, as well as government entities, have learned the hard way that consumers are prepared to protest against services that appear to infringe on their privacy.

In 1996, public criticism forced Lexis-Nexis to withdraw a service known as P-Trak, which granted easy access to a database of millions of individuals' Social Security numbers.

During August of 1997, American Online ("AOL") announced plans to disclose its subscribers' telephone numbers to business partners for telemarketing [34].

AOL heard loud objections from subscribers and advocates opposed to this unilateral change in the "terms of service agreement" covering the use and disclosure of personal information. In response, AOL decided not to follow through with its proposal.

The surveillance capacity of the technology to collect, aggregate, analyze and distribute personal information coupled with current business practices have left individual privacy unprotected. While recent surveys [35] and public pressure have raised the privacy consciousness of companies, information is frequently used and disclosed for purposes well beyond what the individual provided it for.

C. Anticipation of Confidentiality

When individuals send an e-mail message, they expect that only the intended recipient will read it. Unfortunately, this expectation too is in danger. For starters, if an individual is using an office computer, it is possible, and legal, for her boss to monitor her messages. If she is using her home computer, her privacy is still not fully assured.

While, law provides e-mail the same legal protection as a first class letter, the technology leaves unencrypted e-mail as vulnerable as a postcard. Compared to a letter, an e-mail message travels in a relatively unpredictable and unregulated environment. As it travels through the network, e-mail is handled by many independent entities: in comparison, a letter is handled only by the Postal Department of particular country. To further complicate matters, the e-mail message may be routed, depending upon traffic patterns, overseas and back, even if it is a purely domestic communication. While the message may effortlessly flow from nation to nation, the statutory privacy protections stop at the border. In addition, unlike the phone or postal systems, the Internet does not have central points of control. While the decentralized nature of the Internet allows it to cope with problems and failures in any given computer network, by simply routing in another direction, it also provides ample opportunities for those seeking to capture confidential communications [36]. The policy of a single computer network can compromise the confidentiality of

information. But e-mail is just one example; today our diaries, our medical records, our communications, and confidential documents are more likely to be out in the network than under our bed. This has drastic consequences for our privacy--as information moves further out onto the network our existing statutory framework provide less and less protection.

It's useful to look at the weak state of privacy protections for other personal papers and records. Individuals traditionally kept their diaries under their mattress, in the bottom drawer of their dresser, or at their writing table. Situated within the four walls of the home, these private papers are protected by the Fourth Amendment of the US Constitution (it guarantees the American people immunity from unreasonable search and seizure). With the advent of home computers, individual diaries moved to the desktop and the hard drive. Writers, poets, and average citizens quickly took advantage of computers to manage and transcribe their important records and thoughts. Similarly, pictures moved from the photo album to the CD-ROM.

Today, network computing allows individuals to rent space outside their home to store personal files and personal World Wide Web pages. The information has remained the same. But storing those personal thoughts and reflections on a remote server eliminates many of the privacy protections they were afforded when they were under the bed or on the hard drive. Rather than the Fourth Amendment protections--including a warrant based on probable cause, judicial oversight, and notice--the individual's recorded thoughts may be obtained from the service provider through a mere court order with no notice to the individual at all. The weak state of privacy protection is evident in the business setting too. Let's look at medical records. Hospitals, their affiliated clinics, and physicians are using intranets to enable the sharing of patient, clinical, financial, and administrative data. Built on Internet technologies, the private networks link the hospital's information system, to pharmacy and laboratory systems, transcription systems, doctor and clinic offices and others.

As computing comes to medicine, the detailed records of individuals health continue to move not just out of our homes, but out of our doctor's offices.

While the use of network technology promises to bring information to the fingertips of medical providers when they need it most, and greatly ease billing, prescription refills, and insurance pre-authorization's, it raises privacy concerns.

In the absence of comprehensive legislation to protect patient privacy, the legal protections afforded medical records may vary greatly depending upon how the network is structured, where data is stored, and how long it is kept. If records are housed on the computer of an individual doctor then access to that data will be governed by the Fourth Amendment [37]. Law enforcement would be required to serve the doctor with a warrant and the doctor would receive notice and have the chance to halt an inappropriate search. Under the US federal law, the patient however, would receive no notice and have no opportunity to contest the production of the records.

The confidentiality of our sensitive information is challenged by a legal framework that hinges protections on who maintains the information, how the network is structured, where data is stored, and how long it is kept. As our wallets become "e-wallets" housed somewhere out on the Internet rather than in our back-pockets, and as our public institutions, businesses, and even cultural institutions find homes online, the confidentiality of our communications, papers, and information is at risk of compromise.

7. HOW TO PROTECT RIGHT OF PRIVACY IN DIGITAL AGE?

It is clear that our existing legal framework did not foresee the persistent role; the information technology would play in our daily lives. Hackers, Phreakers can easily break into your computer and collect your valuable information. Nor did it envision a world where the private sector would collect and use information at the level it does today. Our legal framework for protecting individual privacy in electronic communications while built upon constitutional principles and statutory protections reflects the technical and social "givens" of specific moments in history. A belief, that the government's collection and use of

information about individuals activities and communications was the only threat to individual privacy and that a solid wall separated the data held by the private and public sector; has now began to stress our existing privacy framework.

Crafting proper privacy protections in the electronic realm has always been a complex endeavor. It requires a keen awareness of not only changes in technology, but also changes in how citizens use the technology, and how those changes are pushing at the edges of existing laws. From time to time these changes require us to reexamine our fabric of privacy protections. The Internet has changed the quantity and quality of data available about individuals' lives, but unfortunately our business practices, norms, and laws have not progressed to ensure individuals' privacy.

At the outset, there are five areas where we must put our efforts to strengthen privacy protections:

A). Maintaining a reliable Level of Privacy Protection for Communications

Increasingly, our most important records are not "papers" in our "houses" but "bytes" stored electronically at distant "virtual" locations for indefinite periods of time and held by third parties. In the US, there are now essentially four legal regimes for access to electronic data:

- the traditional Fourth Amendment [38] standard for records stored on an individual's hard drive or floppy disks;
- the Title III-Electronic Communications Privacy Act [39] standard for records in transmission;
- the standard for business records held by third parties, available on a mere subpoena to the third party with no notice to the individual subject of the record and
- for records stored on a remote server such as the research paper, or the diary, of a student stored on a university server, or the records, including the

personal correspondence, of an employee stored on the server of the employer, the scope of which is probably unclear.

As the third and fourth categories of records expand because the wealth of transactional data collected in the private sector grows and people find it more convenient to store records remotely, the legal ambiguity and lack of strong protection grows more significant and poses grave threats to privacy in the digital environment.

Advocate Starr's investigation into books purchased by Monica Lewinsky highlights the potential sensitivity of records routinely collected by businesses and the intersection of privacy and First Amendment concerns [40]. During his investigation into President Clinton's relationship with White House intern Monica Lewinsky, Starr sought information confirming the purchase of a specific book by Miss Lewinsky. Starr served a subpoena upon Kramer Books, a local DC bookstore, demanding the production of records reflecting purchasing activities. While the bookstore valiantly objected to the subpoena on First Amendment and privacy grounds, and Starr eventually obtained Miss Lewinsky's records through other channels, this incident raised concern among the book-buying public. To search Miss Lewinsky's residence for information about her reading habits Starr would have needed a warrant, but in the hands of the bookstore the records were available under a less stringent standard.

Sometimes the equation is flipped--the government has collected the data and the private sector seeks access to it.

During the lawsuit brought by several states, including Massachusetts, against the tobacco industry for repayment of state health care costs for smoking related illnesses, lawyers for the tobacco industry sought access to a Massachusetts database containing records on every hospital visit by every person in the entire state population [41]. While the State's purpose for collecting the data was to compare what it paid for health care to private insurers, it failed to enact privacy protections to limit access to the database. Because the State's argument for repayment was premised on its ability to prove damage to

state residents from tobacco products, the tobacco companies wanted to see the data supporting it. Massachusetts acted responsibly, hiring a team of cryptographers to ensure that the data released wouldn't identify individuals, however the fact remains that law did not protect the data.

B). Raise the Legal Protections Afforded to Transactional Data when it is collected

Where information is needed, we must make sure that it is protected from misuse and unregulated government access. The US Congress acted by legislation to establish a right of privacy in bank records in the wake of a Supreme Court decision finding they were without constitutional protection [42]. Institutions all across the economy are quickly becoming storehouses of information about individuals' marketplace behaviors, --unlike records held by banks, these new databases are unprotected.

The possibilities of computer analysis have given value to tidbits previously considered meaningless: the little digital footprints individuals leave showing who they called, where they used their credit cards, what websites they visited, what products they purchased, and when they entered the "intelligent" highway using the automatic toll booth. While a certain website or product registration card may only ask for a few minor pieces of personal information, together they constitute a fairly complete profile of one's associations, habits, health condition and personal interests, combining credit card transactions with magazine subscriptions, telephone numbers, real estate records, car registrations and fishing licenses.

The digital storage of these transactional details are so deep that the practice of exploiting their commercial value is called "data-mining," evoking the intensive, and highly lucrative labors of an earlier age. It's time to ensure that the records of our reading habits, our online browsing, and all the details of our lives left behind, online and in electronic commerce, are not treated as mere "business records" available, without our knowledge or permission, at the government's request. For even the most mundane of records can harbor risks to privacy.

C). Developing Software's that prevents the Collection of Personally Identifiable Data

Law is only one tool for protecting privacy. In this global, decentralized medium, we must promote applications of technology that limit the collection of transactional information that can be tied to individuals. Some tools developed to protect privacy by limiting the disclosure, or cloaking it, of information likely to reveal identity, or decoupling this identity information from the individual's actions and communications, exploit the decentralized and open nature of the Internet [43].

D). Enacting Legislations and developing technologies that gives an individual to have control over personal information during Commercial Interactions

We must adopt enforceable standards, both self-regulatory and regulatory, to ensure that information provided for one purpose is not used or redisclosed for other purposes. At the same time, we must recognize that in this freewheeling, open marketplace, there will be limits to the effectiveness of regulation and self-regulation. Therefore, we must look to technological tools (like software's) that will empower individuals to control their personal information.

Lastly, in the decentralized and global environment of the Internet, the impact of law will be limited. In an area such as privacy, where the government's actions have often been detrimental rather than supportive, we must ask if other options--such as technology. We must encourage the development and implementation of technologies that support privacy. They are critically important on the Internet and other global medium. Strong encryption is the backbone of technological protections for privacy. But as we ward off the bad, we must move for the development of the good--seeking to foster technologies, --both standards and specific products, --that protect privacy.

Future technical developments have the capacity to provide an underlying framework for privacy, providing greater anonymity, confidentiality, and a platform for fair information practices. Technologies must be a central part of our privacy protection framework, for they can provide protection across the global and decentralized Internet where law or self-regulation may fail us.

8. DIFFERENT POSSIBLE MODES OF PROTECTING THE RIGHT OF PRIVACY IN DIGITAL ERA

We may start with four different modes for privacy protection.

a). Comprehensive Laws

b). Sectoral laws

c). Self regulation

d. Technologies of privacy

Depending on their application, these modes can be complementary or contradictory. In most countries, more then one modes are used simultaneously. In the countries that protect privacy most effectively, all of the models are used together to ensure privacy protection.

a). Comprehensive laws

In many countries around the world, there is a general law that governs the collection, use and dissemination of personal information by both the public and private sectors.

Indian position:

The Constitution of 1950 does not expressly recognize the right to privacy. However, the Supreme Court first recognized in 1964 that there is a right of privacy implicit in the Constitution under Article 21 of the Constitution, which states, "No person shall be deprived of his life or personal liberty except according to procedure established by law." (Kharak Singh v. State of UP AIR 1963 SC 1285). In this cast SC held that the domiciliary visits of the policeman were an invasion on the petitioners right of personal liberty. It was held that

unauthorized intrusion into a person's home and the disturbance caused to him is the violation of the personal liberty of the individual.

After Maneka Gandhi's landmark decision, the right to privacy has taken a meaning full turn. In the landmark case of Peoples Union of Civil Liberties v. UOI AIR 1997 SC 568 popularly known as "Telephone Tapping case", the supreme court held that, the telephone tapping is a serious invasion of an individuals right to privacy which is part of the right to "life and personal liberty" enshrined in A.21 of the Constitution, and it should not be resorted to by the state unless there is public emergency or interest of public safety requires. Wiretapping is regulated under the Telegraph Act of 1885. There have been numerous phone tap scandals in India, resulting in a 1996 decision (above mentioned) by the Supreme Court, which ruled that wiretaps are a "serious invasion of an individual's privacy"

Again in case of R.Rajagopal v. St. of T.N. 1994 SCC 632 popularly knows as "Auto Shanker case" the Supreme Court has expressly held that the "right to privacy", or the right to be let alone is guaranteed by A.21 of the Constitution. A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, childbearing, and education among other matters. No one can publish anything concerning the above matters without his consent.

This judgment of the Supreme Court will go a long way in protecting the right to privacy of the individual. It can be applied to the information stored in the computer by way of data. No institutions or organizations (like insurance company, hospitals, credit card companies) can use such information for the commercial purpose or any other purpose.

A prominent expose of government corruption by the web portal Tehelka sparked a growing debate on the appropriate balance between the press and personal privacy. Telehka's investigative journalists covertly filmed high-level officials accepting bribes and army officers groping call girls as part of their expose on how official corruption operates in India [44]. While some critics admit that the journalists did shed much needed light on a murky subject, they argue that there should be some restrictions on the press' behavior [45]. India authorizes the use of illegally obtained evidence that would therefore allow

journalists to present such evidence in court. Similar questions arose in relation to the transcripts of tapped phone calls released to the press in a match fixing scandal surrounding the national sport of cricket in April 2000 [46].

There is no general data protection law in India. In June 2000 the National Association of Software and Service Companies (NASSCOM) urged the government to pass a data protection law to ensure the privacy of information supplied over computer networks and to meet European data protection standards [47]. The National Task Force on IT and Software Development had submitted an "IT Action Plan" to Prime Minister Vajpayee in July 1998 calling for the creation of a "National Policy on Information Security, Privacy and Data Protection Act for handling of computerized data." It examined the United Kingdom Data Protection Act as a model and recommended several cyber laws including ones on privacy and encryption [48]. No legislative measures, however, has been considered to date. In May of 2000, the government passed the Information Technology Act; a set of laws intended to provide a comprehensive regulatory environment for electronic commerce. The Act also addresses computer crime, hacking, damage to computer source code, breach of confidentiality and viewing of pornography.

Section 72 of the IT Act specifically deals with - Penalty for breach of confidentially and privacy. The section says -

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

Thus by the virtue of this section any person who has secured access to any electronic record, book etc. without the consent of the person concerned is deemed to have committed the offence of breach of privacy.

Again the act of interrupting with the personal data of the person without his consent will also fall under the offence of Hacking which is widely defined under - Section 66 of the IT Act. It says -

"Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any other person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.... The section also lays down punishment by way of imprisonment upto 3 yeas and fine which may extend upto 2 lakh rupees, or with both".

In February 2003, India convicted its first cyber-criminal when a Delhi High Court sentenced Arif Azim on the charges of online cheating. In the said case, Arif Azim, while working for a call center near Delhi stole the credit card information that belonged to an American citizen and used it to order a color television and a cordless hand phone. This case has highlighted the security and privacy risks for companies to outsource some of their processing operations in India where there is a lack of a clear privacy legal framework. The Indian government is currently considering the idea of enacting a detailed law on data protection under the initiative of the Ministry of Communication and Information Technology. (See: www.hindustantimes.com/news/181_156334,0008.htm)

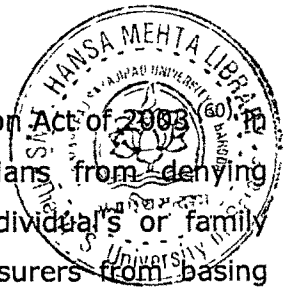
Position in USA:

There is no explicit right to privacy in the United States Constitution. The Supreme Court has ruled that there is a limited constitutional right of privacy based on several provisions in the Bill of Rights. This includes a right to privacy from government surveillance into an area where a person has a "reasonable expectation of privacy" [49] and also in matters relating to marriage, procreation, contraception, family relationships, child rearing and education [50]. Some states within the country have incorporated explicit privacy protections into their state constitutions [51]. However, the United States has taken a sectoral approach to privacy regulation so that records held by third parties, such as consumer marketing profiles or telephone calling records, are generally not protected unless a legislature has enacted a specific law [52]. The Court has

also recognized a right of anonymity and the right of political groups to prevent disclosure of their members' names to government agencies [53]. The United States Supreme Court has considered several important privacy cases over the last few years. In January 2000, the Supreme Court heard *Reno v. Condon*, a case addressing the constitutionality of the Drivers Privacy Protection Act (DPPA), a 1994 law that protects drivers' records held by state motor vehicle agencies. In a unanimous decision, the Court found that the information was "an article of commerce" and can be regulated by the federal government ([54]). In June 2001, the Supreme Court ruled in the case of *Kyllo v. United States* that the use of a thermal imaging device, without a warrant, to detect heat emanating from a person's residence constituted an illegal search under the Fourth Amendment. The Fourth Amendment protects individuals from intrusions into areas where there is a "reasonable expectation of privacy"[55]. In November 2000, the Supreme Court ruled held that suspicion less vehicle checkpoints, used to discover and interdict illegal narcotics, violate the Fourth Amendment [56]. Also, in March 2001, the Supreme Court held that a state hospital couldn't perform diagnostic tests to obtain evidence of criminal conduct without the patient's consent; such a test is unreasonable and violates the Fourth Amendment [57].

In a far-reaching opinion, the Supreme Court ruled in *Lawrence v. Texas* that a state law that prohibited homosexual sodomy violated the due process rights of the Constitution [58]. The Court reversed an earlier opinion in which it had upheld sodomy statutes. Justice Kennedy writing for the Court said, "The petitioners are entitled to respect for their private lives. The state cannot demean their existence or control their destiny by making their private sexual conduct a crime." Significantly, Justice Kennedy also cited with approval the European Court of Human Rights and other foreign courts that have affirmed the "rights of homosexual adults to engage in intimate, consensual conduct." The decisions were brought to the attention of the high court in an amicus brief filed by the former UN High Commissioner for Human Rights [59].

As the mapping of the human genome has been completed, the use of genetic testing information became an area of particular concern. In response to this



concern, the Senate is considering Genetics Nondiscrimination Act of 2003 [60]. In May 2003. The bill would prohibit health insurance plans from denying enrollment or charging premiums on the basis of an individual's or family members' genetic information. It also prohibits health insurers from basing premiums of a group health plan on the basis of genetic information of plan members or their families. The bill prohibits disclosures or collection (requesting, requiring or purchasing) of genetic information for underwriting purposes. In addition, it prohibits the use of genetic information in employment decisions and applies the same procedures and remedies as apply to other forms of employment discrimination [61].

Internet privacy has remained the hottest issue of the past few years. Several profitable companies, including eBay.com, Amazon.com, drkoop.com, and Yahoo.com have either changed users' privacy settings or have changed privacy policies to the detriment of users [62]. A series of companies, including Intel and Microsoft, were discovered to have released products that secretly track the activities of Internet users [63]. Users have filed several lawsuits under the wiretap and computer crime laws. In several cases, TRUSTe, an industry-sponsored self-regulation watchdog group ruled that the practices did not violate its privacy seal program. Significant controversy arose around online profiling, the practice of advertising companies to track Internet users and compile dossiers on them in order to target banner advertisements. The largest of these advertisers, DoubleClick, ignited widespread public outrage when it began attaching personal information from a marketing firm it purchased to the estimated 100 million previously anonymous profiles it had collected [64]. The company backed down due to public opposition, a dramatic fall in its stock price and investigations from the FTC and several state attorneys general. In July 2000 the Federal Trade Commission reached an agreement with the Network Advertisers Initiative, a group consisting of the largest online advertisers including DoubleClick, which will allow for online profiling and any future merger of such databases to occur with only the opt-out consent [65]. In January 2001, the FTC dropped its investigation of DoubleClick. However, several private lawsuits were filed against DoubleClick. In January 2001, DoubleClick closed its online profiling division, and in May 2002, privacy class actions suits against the

company were settled that resulted in little or no benefit to Internet users. Intel announced in May 2000 that it was dropping the incorporation of unique identifiers in its next-generation computer processors following a consumer boycott.

Position in Canada:

There is no explicit right to privacy in Canada's Constitution and Charter of Rights and Freedoms [66]. However, in interpreting Section 8 of the Charter, which grants the right to be secure against unreasonable search or seizure, Canada's courts have recognized an individual's right to a reasonable expectation of privacy [67].

Privacy is regulated at both the federal and provincial level. At the federal level, privacy is protected by two acts: the 1982 federal Privacy Act and the 2001 Personal Information and Electronic Documents Act (PIPEDA). The Federal Privacy Act of 1982 regulates the collection, use and disclosure of personal information held by federal public agencies and provides individuals a right of access to personal information held by those agencies, subject to some exceptions, including an exemption for court records. Individuals can appeal to a federal court for review if access to their records is denied by an agency, but are not authorized to challenge the collection, use, or disclosure of information. In 1999, in order to tighten exemptions and loopholes, the Privacy Commissioner finished an extensive review of the Act and recommended over one hundred changes to the law to improve and update it. Some of the changes included giving the Commission primary authority over all information collected by the federal government, extending its coverage beyond "recorded" information, increasing notice of disclosures, expanding court reviews, creating rules on data matching, controlling "publicly available" information and expanding the mandate of the Privacy Commissioner [68].

There have been several highly public privacy blunders in Canada in 2003. In February 2003, copies of a patient's medical records were found on the back of a real estate newsletter. Reportedly the records were disclosed to a law firm who then recycled them. The law firm was chastised by the Ontario Privacy

Commissioner who commented on the need for proper record handling and destruction. Also in February, a computer hard drive was stolen which allegedly contained personal information of a medical, financial and tax nature on hundreds of thousands of customers of an insurance company, prompting significant privacy and identity theft concerns [69]. The hard drive was recovered after a week and a class action was launched, but it was uncertain how this personal information was used and whether it was disclosed. In June 2003, public computers terminals at courthouses in British Columbia were shut down for several weeks because a visitor was able to access information about court cases that was not supposed to be released to the public. The public information system was shut down as a precaution against any further access. Although the privacy law framework in Canada has received much media attention, a recent study from the Alberta Information and Privacy Commission found that there is a low level of awareness of current privacy laws: sixty percent of respondents were unaware of Canadian laws that protected their personal information. There was also a low level of awareness about Alberta's Health Information Act - only fifty-three percent of Albertans had heard of it.

b. Sectoral Laws

Some countries, such as the United States, have avoided enacting general data protection rules in favor of specific sectoral laws governing, for example, video rental records and financial privacy. In such cases, enforcement is achieved through a range of mechanisms. A major drawback with this approach is that it requires that new legislation be introduced with each new technology so protections frequently lag behind. The lack of legal protections for individual's privacy on the Internet in the United States is a striking example of its limitations. There is also the problem of a lack of an oversight agency. In many countries, sectoral laws are used to complement comprehensive legislation by providing more detailed protections for certain categories of information, such as telecommunications, police files or consumer credit records.

c. Self-Regulation

Data protection can also be achieved, at least in theory, through various forms of self-regulation, in which companies and industry bodies establish codes of practice and engage in self-policing. However, in many countries, especially the United States, these efforts have been disappointing, with little evidence that the aims of the codes are regularly fulfilled. Adequacy and enforcement are the major problem with these approaches. Industry codes in many countries have tended to provide only weak protections and lack enforcement.

d. Technologies of Privacy

With the recent development of commercially available technology-based systems, privacy protection has also moved into the hands of individual users. Users of the Internet and of some physical applications can employ a range of programs that provide varying degrees of privacy and security of communications. These include encryption, anonymous remailers, proxy servers and digital cash. Users should be aware that not all tools effectively protect privacy. Some are poorly designed while others may be designed to facilitate law enforcement access.

9. CONCLUSION

No doubt, privacy on the Internet is in a fragile state, however, there is new hope for its resuscitation. Crafting proper privacy protections in the electronic realm has always been a complex endeavor. It requires a keen awareness of not only changes in technology, but also changes in how citizens use the technology, and how those changes are pushing at the edges of existing laws. From time to time these changes require us to reexamine our fabric of privacy protections. In an environment where there are not proper legislations, the only protection against the violation of right of privacy over Internet is strong technological backbone.

Footnotes

1. Marc Rotenberg, Protecting Human Dignity in the Digital Age (UNESCO 2000).
2. Nature and scope of the right to privacy and the problem of the protection of this right in India: Comparative Perspective to USA and UK – Thesis submitted by Prof.SN Parikh
3. Ibid 2
4. Ibid 3
5. Volume 1, Book 10, Number 509 (Sahih Bukhari); Book 020, Number 4727 (Sahih Muslim); Book 31, Number 4003 (Sunan Abu Dawud).(www. Privacyinternational.org/survey/phy2003/overview)
6. Richard Hixson, Privacy in a Public Society: Human Rights in Conflict 3 (1987). See also, Barrington Moore, Privacy: Studies in Social and Cultural History (1984).
7. See Jeffrey Rosen, The Unwanted Gaze (Random House 2000). (www. Privacyinternational.org/survey/phy2003/overview)
8. Ibid 7
9. James Michael,. Justices of the Peace Act, 1361 (Eng.), 34 Edw. 3, c. 1. (www. Privacyinternational.org/survey/phy2003/overview)
10. Entick v. Carrington, 1558-1774 All E.R. Rep. 45.
11. Speech on the Excise Bill, 1763. See- www.privacyinternational.org/survey/phy2003/overview
12. See Jeanne M. Hauch, Protecting Private Facts in France: The Warren & Brandeis- Tort is Alive and Well and Flourishing in Paris, 68 Tulane Law Review 1219 (May 1994).
13. See Prof. Dr. Juris Jon Bing, Data Protection in Norway, 1996, available at www.jus.uio.no/iri/rettsinfo/lib/papers/dp_norway/dp_norway.html.
14. Universal Declaration of Human Rights, adopted and proclaimed by General Assembly resolution 217 A (III) of December 10, 1948, available at http://www.un.org/Overview/rights.html.
15. See, Marc Rotenberg, The Privacy Law Sourcebook: United States Law, International Law and Recent Developments (EPIC 2003).). (www. Privacyinternational.org/survey/phy2003/overview)
16. International Covenant on Civil and Political Rights adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of December 16, 1966, entry into force March 23 1976, available at http://www.unhchr.ch/html/menu3/b/a_ccpr.htm.
17. International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, adopted by General Assembly resolution 45/158 of December 18, 1990, available at http://www.unhchr.ch/html/menu3/b/m_mwctoc.htm.
18. Convention on the Rights of the Child adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of November 20, 1989, entry into force September 2, 1990, available at http://www.unhchr.ch/html/menu3/b/k2crc.htm.
19. See, Lee Bygrave, "Data Protection Pursuant to the Right of Privacy in Human Rights Treaties," 6 International Journal of Law and Information

Technology 247-284 (1998), available at http://folk.uio.no/lee/publications.

20. James Michael, Privacy and Human Rights 1 (UNESCO 1994).
21. Simon Davies, Big Brother: Britain's Web of Surveillance and the New Technological Order 23 (Pan 1996).). (See :www. Privacyinternational.org/survey/phy2003/overview)
22. Privacy and Human Rights 2003: Overview
23. Privacy as an Aspect of Human Dignity, 39 New York University Law Review 971 (1998)
24. TRUSTe, is an industry-sponsored self-regulation watchdog group. TRUSTe: Building a Web You Can Believe In http://www.truste.org/
25. See: Global Internet Liberty Campaign Home Page http://www.gilc.org/. Also see: www.cdt.org/publications/lawreview/1999
26. See The Center for Democracy and Technology's Snoop Demonstration at http://snoop.cdt.org/ for an example of the information that can be easily captured by sites on the World Wide Web. Also see: www.cdt.org/publications/lawreview/1999
27. A cookie is a small text file that a web server writes to an Internet user's computer once the user visits a website. The text file usually contains information that allows the website to identify the individual's computer or user profile the next time he or she visits the web site. Cookies are often used by websites in order to customize advertisements, so that the content of the advertisements resembles the content of websites that the user, or more realistically the actual computer, has previously accessed. Also see, "Cookies" is a browser feature that assists Web site operators in tracking a user's activities. It was initially designed to address the "static state" problem of the World Wide Web, the fact that Web sites don't know whether a user is a first time or repeat visitor. See Joan E. Rigdon, Internet Users Say They'd Rather Not Share Their åCookies,' WALL ST. J., Feb. 14, 1996, at B6.
28. Saul Hansell, Big Web Sites to Track Steps of Their Users, N.Y. TIMES ABSTRACT, Aug. 16, 1998
29. In many countries, offline consumer-initiated financial transactions are dominated by cash and checks. The reference is to the number of transactions not to the relative economic value they represent. Many of the transactions represented are likely to involve relatively modest sums. For example, newspaper purchases, meals, and phone calls to name a few. See FRB: Federal Reserve Board Speech from Mar. 7, 1997 http://www.bog.frb.fed.us/boarddocs/speeches/19970307.htm (remarks by Federal Reserve Board Chairman Alan Greenspan at the Conference on Privacy in the Information Age, Salt Lake City, UT, Mar. 1997).
30. As financial transactions in the physical world continue to change itself to stored value cards, and smart cards, the need to build privacy protections into these payment systems becomes more important. Also see: www.cdt.org/publications/lawreview/1999
31. See Robert O'Harrow Jr., Prescription Sales, Privacy Fears, CVS, Giant Shares Customer Records With Drug Marketing Firm, WASH. POST, Feb. 15, 1998, (See-www.cdt.org/publications/lawreview.html)
32. Ibid 31

33.Cheryl Clark, Medical Privacy is Eroding, Physicians and Patients Declare, SAN DIEGO UNION TRIB., Feb. 21, 1998, at B2. www.cdt.org/publications/lawreview.html)
34.Rajiv Chandrasekaran, AOL Will Share Users' Numbers for Telemarketing, WASH. POST, July 24, 1997, See Department of Commerce Workshop on Online Privacy, June 1998 http://www.doc.gov/.
35.For an overview of recent surveys of consumer concerns with privacy see, The Center for Democracy and Technology, http://www.cdt.org/privacy/surveys/findings/introbody.html.
36.Attempts to regulate the availability of encryption on the Internet highlight the frustrations that regulators may experience. As many scholars and advocates have pointed out, national attempts to restrict the availability of encryption are likely to be ineffective. For if even one jurisdiction or one network in one jurisdiction fails to restrict it, individuals worldwide will be able to access it over the Internet and use it.
37.The record keeper would have Fourth Amendment protections. Whether the patient's privacy is protected at all would largely depend upon state law, which is scattered and inconsistent. Until a federal law protecting individual's privacy in health information is crafted to protect data regardless of where it is stored or whose control it is under, privacy is in danger. Also see: www.cdt.org/publications/lawreview/1999
38.U.S. CONST. IV. Amendment
39.18 U.S.C. ßß 2570,2711 (1994).
40.DAVID STOUT, Lewinsky's Bookstore Purchases Are Now Subject of a Subpoena, N. Y. TIMES, Mar. 25, 1998, at A1. www.cdt.org/publications/lawreview.html)
41.John Schwartz, Private Data, Public Worries, WASH. POST, June 8, 1998, at F24www.cdt.org/publications/lawreview.html)
42.United States v. Miller, 425 U.S. 435 (1976). Also see: www.cdt.org/publications/lawreview/1999
43.For a review of several privacy-enhancing technologies see, volume 42, no. 2, Feb. 1999 of the Communications of the ACM on Internet Privacy, guest editor Lorrie Faith Cranor. February 1999www.cdt.org/publications/lawreview.html)
44.Mukund Padmanabhan, "Sex, Bribes, and Videotape," The Hindu, September 8, 2001 http://www.hinduonnet.com/thehindu/2001/09/08/stories/05082523.htm.
45.Rajeev Dhavan, "Tehelka: What Next?" The Hindu, September 7, 2001 http://www.hinduonnet.com/thehindu/2001/09/07/stories/05072523.htm.
46.Manoj Joshi, "Phone-Tap Laws May Trip Cronje Case," April 15, 2000.
47.(Business Line - Internet Edition, "Nasscom Urges Laws for Data Protection," http://www.indiaserver.com/businessline/2000/06/29/stories/152939t5.htm.)
48..(National Task Force on IT & SD, Basic Background Report, June 9, 1998 http://it-taskforce.nic.in/it-taskforce/bg.htm)
49.Katz v. United States, 386 U.S. 954 (1967).

50. Griswold v. Connecticut, 381 U.S. 479 (1965); Whalen v. Roe, 429 United States 589 (1977);
51. California Constitution, Art. I § I.
52. United States v. Miller, 425 US 435 (1976).
53. NAACP v. Alabama, 357 U.S. 449 (1958).
54. Reno v. Condon, 528 U.S. 141 (2000).
55. Kyllo v. United States, 533 U.S. 27 (2001).
56. City of Indianapolis v. Edmond, 531 U.S. 32 (2000).
57. Ferguson v. City of Charlestown, 532 U.S. 67 (2000).
58. 539 U.S. ____ (2003), No, 02-102, available at http://scotus.ap.org/scotus/02-102p.zo.pdf.
59. Brief amici curiae of Mary Robinson, Amnesty International U.S.A., Human Rights Watch, Interights, the Lawyers Committee for Human Rights, and Minnesota Advocates for Human Rights, available at http://www.hrw.org/press/2003/07/amicusbrief.pdf.
60. S.1053, http://thomas.loc.gov/cgi-bin/query/C?c108:./temp/~c108sCD52L.
61. See generally EPIC, Workplace Privacy, available at http://www.epic.org/privacy/workplace/.
62. Chris J. Hoofnagle, Consumer Privacy In the E-Commerce Marketplace 2002, Third Annual Institute on Privacy Law 1339, Practicing Law Institute G0-00W2 (June 2002), available at http://www.epic.org/epic/staff/hoofnagle/plidraft2002.pdf.
63. See Big Brother Inside Campaign http://www.bigbrotherinside.org.
64. See EPIC DoubleClick Pages http://www.epic.org/privacy/doubletrouble/.
65. For a detailed history and critical analysis of this agreement, see Electronic Privacy Information Center (EPIC) and Junkbusters, "Network Advertising Initiative: Principles not Privacy," July 2000 http://www.epic.org/privacy/internet/NAI_analysis.html.
66. Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982(United Kingdom), 1982, c. 11, s. 8, available at http://laws.justice.gc.ca/en/charter/.
67. Hunter v. Southam, 2 S.C.R. 145, 159-60 (1984).
68. Privacy Commissioner, 1999-2000 Annual Report, May 2000, available at http://www.privcom.gc.ca/english/02_04_08_e.htm.
69. Canadian Press, "Police Don't Know if Information Taken from Recovered Hard Drive," CBC News, February 2, 2003, available at http://www.cbc.ca/stories/2003/02/05/missingdrive_030205.