# Chapter 4

## PRIVACY IN CYBERSPACE

**Information privacy is a social goal, not a technological one. To achieve information privacy goals will require social innovations, including the formation of new norms and perhaps new legal rules to establish boundary lines between acceptable and unacceptable uses of personal data.**

**Pamela Samuelson**[457]

### 4.1 Introduction

Information and Communication Technologies (ICT) have fulfilled Justice Brandeis' 1928 prophesy in his landmark dissent in Olmstead v. United States[458]. Our private lives are now exposed by electronic retrieval and publication of personal information. While Justice Brandeis was primarily concerned about governmental intrusion into private lives, his prophesy and his description of the right to privacy as "the right to be let alone-the most comprehensive of rights and the right most valued by civilized men" should apply equally to such intrusion by non-governmental entities. ICT provides both an economical and efficient means of

---

[457] Pamela Samuelson, Privacy as Intellectual Property?, 52 STAN. L. REV. 1125, 1169 (2000).

[458] A famous legal article titled "The Right to Privacy" written by Samuel Warren and Louis Brandeis and published by the Harvard Law Review in 1890. In this article authors had shown concern for privacy more than a century ago about how new technologies could affect privacy. They wrote: " recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone'. Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops'. For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of the invasion of privacy by the newspapers, long keenly felt, has been but recently discussed by an able writer. The alleged facts of a somewhat notorious case brought before an inferior tribunal in New York a few months ago, directly involved the consideration of the right of circulating portraits; and the question whether our law will recognize and protect the right to privacy in this and in other respects must soon come before our courts for consideration." The article Right to Privacy by the authors is available at http://freedomlaw.com/Brandeis.htm , visited 1 4 May 2005.
The case, Olmstead V U.S. 227 US 438 (1928), with Justice Brandies dissenting, available at http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=us&vol=277&invol=438 , visited on 14 May 2005

finding needed information. Yet, as increasing amounts of personal information are collected and revealed electronically, there is growing concern over the resulting loss of privacy[459].

Uses of new technologies raise policy issues that are often defined in terms of invasion of privacy. Supporting this contention, one commentator, Patricia Mell, notes that the use of computers to manage information has considerably blurred the demarcation between public and private realms[460]. Unfortunately, this blurring of the realms of privacy by the influx of technological advances only adds to the problem we are now striving to address. This contention also supports a similar, and ever present condition, which Arthur Miller noted in 1971, by stating that, "it is essential to expose the ways computer technology is magnifying the threat to informational privacy - a threat that we have faced in some form ever since man began to take notes about himself and his neighbors[461] and which have also been supported by the 1978 and 1993 Louis Harris poll"[462]. Yet, another legal scholar, Henry Perritt observes "in the long run, adoption of information technologies will blur the boundaries between citizen and agency and between agency and court. Blurring of these boundaries may necessitate rethinking the definitions of some of the basic events that define the administrative process, public participation, and judicial review."[463]

Noted constitutional scholar Lawrence Tribe recommends, that "policy makers look not at what technology makes possible, but at the core values the Constitution enshrines."[464] Principles, such as those that underlie privacy, must be "invariable …

---

[459] Susan E. Gindin, Lost And Found In Cyberspace: Informational Privacy in the Age of the Internet, available at http://www.info-law.com/lost.html , visited 20 May 2005

[460] Priscilla M. Regan, Privacy, Technology And Public Policy, University of North Carolina Press (September 1995) at p 2 .

[461] Miller Arthur,, The Assault On Privacy, Signet publications. New York,1971 at p 23

[462] ibid

[463] Henry H. Perritt Jr., The Electronic Agency and the Traditional Paradigms of Administrative Law, 44 ADMIN. L. REV. 79, 80 (1992).

[464] Tribe Laurence, The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier, Keynote address at the First Conference on Computers, Freedom and Privacy (Boston, March 1991) available at http://www.swissnet.ai.mit.edu/6095/ articles/tribe-constitution.txt, visited 13 Sep 2005

despite accidents of technology."[465] Thus, an irony now presents itself: the very technology that simplifies our lives simultaneously complicates our legal analysis of this most fundamental of concepts.

The Internet offers many benefits. Web sites provide a vast world of information, entertainment, and shopping at our fingertips. Electronic mail, instant messaging, and chat rooms enable us to communicate with friends, family, and strangers in ways we never dreamed of a decade ago.

The Internet has become an indispensable tool for data retrieval, communication, and business transactions. Companies increasingly look to the Internet to attract potential clients and customers and to stay in contact with current clients and customers. But with the ease in collecting and processing information on the Internet and the depth and richness of the data available, there exists the danger that Internet business transactions can render a party's information susceptible to interception, misappropriation, or other loss. The Internet exposes companies to the danger that third parties may access private, confidential client data, resulting in potential liability to the companies. The privacy and security concerns generated by the Internet increase the importance of a company's privacy policy[466].

The Constitution of India does not contain a provision granting a general right to privacy. But 'Right to Privacy' has been recognized by the Indian Judiciary as implicit in Art. 21 and Art.19 (1) (a) of the Constitution in many cases. Right to privacy has many dimensions and the most likely aspect of privacy that would be affected in cyberspace is informational privacy. There are currently no laws in India requiring websites to disclose how the information they gather about visitors is used, and online businesses are largely free to use data obtained on their websites without oversight by the consumer. In India, consumers have no statutory right to control the dissemination of their personal information to others by third parties.

---

[465] ibid

[466] Wendy S Meyer, Insurance Coverage for Potential Liability Arising from Internet Privacy Issues, journal of Corporation Law, Winter 2003

### 4.2 Aspects of Privacy

Privacy is a basic human right recognized all over the world and in cyberspace it is the most flagrantly violated right of the individual.

People enjoy having private spaces, and want to keep them. Key aspects include the following:

- Privacy is the interest that individuals have in sustaining a 'personal space', free from interference by other people and organizations[467];
- Privacy has multiple dimensions, including privacy of the physical person, privacy of personal behaviour, privacy of communications, and privacy of personal data. The last two are commonly bundled together as 'information privacy'[468];
- Individuals claim that data about themselves should not be automatically available to other individuals and organizations, and that, even where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use[469]; and
- Dataveillance or intellectual privacy is the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons[470];

#### 4.2.1 Privacy under International Law

Universal Declaration of Human Rights defines Right to Privacy under Art.12 as follows;

---

[467] Clarke , Roger, Information Privacy On the Internet Cyberspace Invades Personal Space , http://www.anu.edu.au/people/Roger.Clarke/DV/IPrivacy.html

[468] ibid
[469] ibid
[470] ibid

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

Art.17 of he International Covenant on Civil and Political Rights (ICCPR) and European Convention for the Protection of Human Rights and Fundamental Freedoms (Art 8) are expressed similarly, and an extensive jurisprudence has developed in Europe interpreting Art 8 of the Convention. The European Court has measured member countries laws and procedures against Art 8's guarantees, and often found them wanting (for example, the United Kingdom's)[471].

The lack of any constitutional recognition of the right to privacy has led to a similar patchwork in the judicial response to privacy issues. The Supreme Court of India in several cases has held that Right to privacy is implicit in Art.21 of the Constitution which guarantees right to life and personal liberty[472].

The right to privacy as it has been developed in these cases reflects the values of a 19th century liberal democracy whose primary concern was to protect the individual from inappropriate interference from the state. The nature of communications networks now makes the need to protect against potential invasion of personal autonomy by private interests or individuals, equally pressing. The common law has been slow to develop tort remedies for invasion of personal privacy. There is little existing legal framework to help the courts determine new questions of privacy that arise from communications networks, such as: the limits to be placed on employer surveillance and data-tracking of employees; the determination of ownership of

[471] Cronin P Kevin & Weikers N Ronald, Data Security and Privacy Law:Combating Cyberthreats,Thomson –West, US, 2004

[472] In Kharak Singh V State of UP ( AIR 1963 SC 1295), domiciliary visit by the police without the authority of a law , was held to be violative of Art.21 , assuming that a right of privacy was a fundamental right derived from the freedom of movement guaranteed by Art.19(1)(d) as well as personal liberty guaranteed by Art.21. Also in People's Union for Civil Liberties V Union of India (AIR 1997 SC 568) it was held that telephone tapping infringes right to privacy, if not resorted to by just, fair and reasonable procedure. Again in 'X' v 'Hospital Z' Supreme Court held that right to privacy is an essential component of the right to life but is not absolute and may be restricted for prevention of crime, disorder or protection of health or morals or protection of rights and freedom of others.

electronic mail messages created by employees while at the workplace; and the potential electronic intrusion of telemarketers into Indian homes.

### 4.3 Commodification, Privacy and Free Alienability

Personal information is an important currency in the new millennium. The monetary value of data is large and still growing and corporates are moving quickly to profit from this[473]. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information. Moreover, a strong conception of personal data as a commodity is merging in the United States and individual Americans are already participating in the commodification of their personal data[474].Commodification of personal data falls into four broad categories (1) lists of those who are willing to commodify their personal data (2) lists of those who wish to receive tailored ads and the particular interests of those persons (3) lists of transactional activities such as purchases that follow, the release of commodified personal data and (4) privacy metadata which comprises information about one's privacy preferences[475].

Metadata are a relatively common phenomenon in the information age and is capable of creating privacy metadata. Metadata are information about information; they are, for example, found in the popular text-processing software like Microsoft Word, which permits association of rich metadata with documents[476]. Metadata in Word can include the author's name and initials; the names of previous document authors; the name of the author's company or organization ; the name of the one's computer ; the name of the network server or hard disk where the document was

---

[473] Jennifer Sullivan & Christopher Jones, How Much Is Your Playlist worth? Wired News, Nov 3, 1999, available at http://www.wired.com/news/technology/1,32258-0.html, visited 4 Nov 2005

[474] Schwartz M Paul, Property, Privacy and Personal Data, Harvard Law Review, Vol117:2055, May 2004, at p 2057

[475] Lessig , Lawrence, Code and Other Laws of Cyberspace, Basic Books, New York, 1999 at p 142-63

[476] See Microsoft Corp, OFF: How To minimize Metadata in Microsoft Office Document (Microsoft Knowledge Base article No.223,396) available at http://support.microsoft.com/default.aspx?scid=kb;en-us;223396, visited 10 Apr 2005

saved; document revisions; hidden text or cells; and personalized editing comments[477]. All these metadata can be associated with a single document.

The personal data market will increasingly include privacy metadata and this metadata will in turn be commodified and contribute to additional privacy invasions. Already in the offline world and in no small irony, direct marketers generate and sell lists of people who have expressed interest in protecting their privacy[478]. Analogous to these marketing lists of those who wish to protect their privacy, privacy metadata can include information concerning an interest in not receiving certain kinds of solicitations or not receiving telemarketing calls at certain times. These meatadata will be highly marketable[479].

Personal data inalienability is any restriction on the transferability, ownership or use of data. In the context of these new technologies, inalienability relates to restrictions on the exchange of personal data, even restrictions contrary to individual's wishes. In other words, even if someone wants to engage in data trade, society may wish to limit her ability to do so. A principle of free alienability for personal information would mean, in contrast, that an individual has a right to do what he wants with his data. Alienability is yet to emerge as a policy issue for adware[480] and spyware[481] because the makers of these products generally offer inadequate notice of their data practices. It would be difficult for adware and spyware companies to make an argument for free choice to trade personal data in the absence of sufficient notice of data collection and processing practices. Informed consent to adware and spyware

---

[477] ibid

[478] For battle over privacy metadata in the context of traditional telephony see US West Inc., V FCC 182 F.3d 1224, 1228 (10th circuit, 1999), available at http://www.kscourts.org/CA10/cases/1999/03/98-9501.htm , visted on Nov 5, 2005

[479] Schwartz M Paul, Property, Privacy and Personal Data, Harvard Law Review, Vol117:2055, May 2004, at p 2070

[480] Spyware and adware are controversial applications of networked computing. Smart Computing Magazine defines spyware as a program that "installs itself without your permission, runs without your permission and uses your computer without your permission. Adware is something but not always, delivered as part of spyware; the definitional line between the two depends on whether the computer user receives adequate notice of the program installation. See Tracy Baker, Here's Looking at you, Kid: How to Avoid Spyware, SMART COMPUTING, Sept.2003 at 68

[481] Developments in the Law-The Law of Cyberspace, The Harvard Law Association, Vol 12:1574,1999

would require notice of such practices, without it, there is no free choice to trade data[482].

### 4.4 The Lack of Privacy in Cyberspace

In cyberspace, as in today's real world, there seems to be confusion in regard to what privacy is and what it is not. One scholar, Ruth Granson highlights recent efforts to fully comprehend privacy: "the concept of privacy is a central one in most discussions of modern Western life, yet only recently have there been serious efforts to analyze just what is meant by *privacy*." Over the years, the conception of the nature and extent of privacy has been severely bent out of shape. The definitions and concepts of privacy are as varied as those in the legal and academic circles who explore privacy. Another scholar, Judith DeCew, examines the diversity of privacy conceptions: "the idea of privacy which is employed by various legal scholars, is not always the same. Privacy may refer to the separation of spheres of activity, limits on governmental authority, forbidden knowledge and experience, limited access, and ideas of group membership consequently privacy is commonly taken to incorporate different clusters of interest."[483]

At one time, privacy implied that individuals could be secluded, but that has radically changed. Logistical barriers created by geography once protected a person. This too, though, has radically changed. The geographical wall of protection, which incidentally was not created by our legal system, has been removed by the development of the Internet, and more recently, by the World Wide Web. The loss of these once formidable barriers has not been accounted for in the scholarship available today[484].For today, "effective protection of personal data and privacy is developing into an essential precondition for social acceptance of the new digital networks and services." Privacy can no longer be assumed, even in the security of

---

[482] Schwartz M Paul, Property, Privacy and Personal Data, Harvard Law Review, Vol117:2055, May 2004, at p 2065

[483] Robert A. Reilly, Conceptual Foundations of Privacy: Looking Backward Before Stepping Forward, 6 RICH. J.L. & TECH. 6 (Fall 1999) , available at http://www.richmond.edu/jolt/v6i2/article1.html, visited 22 May 2005

[484] ibid

one's own home. Instead, privacy is a condition that is much easier to violate, and thus, is much more difficult to establish and protect[485].

The way in which we continue to view privacy has not significantly changed across time, and in some cases, change has been actively resisted. Yet somehow, privacy has evolved from a small single function business into a complex conglomerate. A basic paradigm shift in the way we conceptualize privacy is in order. For at this instance, "privacy" should be viewed as a foundational concept in the same manner that life, liberty, and the pursuit of happiness are foundational concepts in our society. In order to begin to accomplish this paradigm shift, it is first necessary to revisit the cultural evolution of "privacy" so that we can fully analyze the ramifications and impact of emerging technologies[486].

### 4.5 Electronic Invasion of Privacy

An individual's privacy may be invaded electronically in several ways: first, by the significant amount of personal information which is available in online databases; second, by the transactional information collected as the individual participates in online activities which specifically identifies the individual; and third, by the massive computerized databases which are maintained by governments and non-governmental entities, that may be subject to security breaches[487].

Many people expect that their online activities are anonymous. They are not. It is possible to record virtually all online activities, including which newsgroups or files subscriber accesses, which web sites are visited and reading of e-mails. This information can be collected by a subscriber's own ISP and by web site operators[488].

"Online communications" are communications over telephone, cable networks, or wireless systems using computers. Examples of online communications include

---

[485] ibid
[486] Cronin P Kevin & Weikers N Ronald, Data Security and Privacy Law: Combating Cyberthreats, Thomson-West, New York, 2004 at 1-49
[487] ibid at p 2-7
[488] Privacy Rights In cyberspace, http://www.privacyrights.org/fs/fs18-cyb.htm

connecting to the Internet through an Internet Service Provider (ISP) such as America Online or Earthlink, or accessing the Internet from a public library or community computer center. Mobile access to the Internet is increasing via hand held Personal Digital Assistants (PDAs), pagers, and other devices[489].

The Internet raises some unique privacy concerns. Information sent over this vast global network may pass through dozens of different computer systems on the way to its destination. Each of these systems is operated by its own administrator and may be capable of capturing and storing online communications. Furthermore, online activities can potentially be monitored by Internet Service Provider (ISP) and by web sites that we visit[490].

The informational consequences of activities in cyberspace result from the generation, storage, and transmission of personal data in three areas: (1) personal computers; (2) Internet Service Providers ("ISPs") (3) Web sites, and (4) Spyware. Visitors to cyberspace sometimes believe that they will be fully able to choose among anonymity, semi-anonymity, and complete disclosure of identity and preferences. Yet, in each of the three areas, finely granulated personal data are created—often in unexpected ways. Moreover, most people are unable to control, and are often in ignorance of, the complex processes by which their personal data are created, combined, and sold[491].

### 4.5.1 Personal Computers

When tied to a network, an individual's personal computer makes access to the Internet available at her desk[492]. For some people, this machine may be no more than a necessary evil; they imagine the computer to be a glorified typewriter. For

---

[489] Privacy Rights Clearinghouse / UCAN ,June 1995. Revised August 2003 available at http://www.privacyrights.org/fs/fs18-cyb.htm, visited on 23 Jun 2005

[490] ibid

[491] Paul M. Schwartz, Privacy and Democracy in Cyberspace, Vanderbilt Law Review, Vol. 52:1609

[492] Reno V ACLU, 521 U.S. at 844-49; Nathan J. Muller, Desktop Encyclopedia Of Telecommunications, 3rd Edition, McGrawhill, New York,1998, at p 168-70 .

others, it is an evocative object, perhaps even a kind of friend with whom one can have an intense relationship[493].The computer is not always a silent and loyal friend, but sometimes, the recorder and betrayer of Monica Lewinsky's confidences. A personal computer records and reveals its users' confidences in a number of ways[494].

First, information deleted from a personal computer is generally easily recoverable, whether from the machine's hard drive or elsewhere. Our own digital experiences provide examples of how computer files may be deleted, but not destroyed. Deletion removes data from the hard disk drive's directory of files and marks the disk space where the file is still stored as available for reuse[495].In time, another file may be written over this area, but in the period before deleted data are overwritten, anyone with access to the computer can locate and restore the deleted file with relatively simple commands found in many software utility programs[496]. Even if files have been written over, or, more drastically, "wiped" by programs that hash over the designated disk space, software utility programs are sometimes capable of recovering the underlying data from the computer[497]. Moreover, deleted files can be found not only on a personal computer's hard drive but also on another personal computer or elsewhere in a networked system[498].

As these examples show, a personal computer can betray confidences by failing to destroy files that its users sought to remove by use of a "delete" button. This

---

[493] *See* Reno v. ACLU, 521 U.S. 844, 868-73 (1997) (describing some of the myriad forms on online behavior);

[494] Volokh, Eugene, Freedom of Speech, Cyberspace and Harassment Law, 2001 Stan.Tech.Rev 3, available at http://stlr.stanford.edu/STLR/Articles/01_STLR_3 or www.papers.ssrn.com , visited on 2 Sep 2004 ; in this article author brings out the ramification of e-mail during the controversy of Clinton-Lewinsky scandal highlighting how technology can be used to violate privacy;

[495] Ron, White," How Computers Work " 4th ed., Random House Publications, New York, 1999 at p 78-79

[496] ibid at p 81

[497] David S., Bennahum, *Daemon Seed: Old email never dies*, WIRED, May 1999, at p 100, 102

[498] Jerry ,Adler, When E-Mail Bites Back, NEWSWEEK, Nov. 23, 1998, at p 45 (noting that in its investigation of Microsoft, the Justice Department has obtained an estimated 3.3 *million* Microsoft documents, including megabytes of e-mail messages dating from the early 1990s and is using them to contradict Gate's own videotaped testimony in the most significant antitrust case of the decade".

machine causes a further problem for privacy, however, through its storage of information about Internet activities. Computers' Web browsers, such as Netscape Navigator or Microsoft Internet Explorer, contain software protocols that create files about Web sites that have been visited. Anyone with physical access to a computer can access these data in a matter of seconds either by looking at drop down files on the browser's location bar or by accessing the "History" menu item found on both Netscape Navigator or Microsoft Internet Explorer. Even more significantly, remote access to these files is possible from the Internet by exploiting security flaws in Web browsers[499].

Cyberspace behavior also results in the recording of data in computer cache files. In order to increase the computer's speed of access to information, these special memory subsystems duplicate frequently used data values, such as Web pages frequently visited[500].Cache files exist on a computer's hard drive and, more temporarily, in its random access memory ("RAM")[501].From the Web, it is possible to access cache files through "JavaScripts" and "Java applets" that permit the remote uploading of these files[502].These terms refer to programming languages for writing Web applications; both allow routines to be executed on an individual's personal computer remotely from the Web[503].

### 4.5.2 Cookies

When we "surf" the web, many web sites deposit data about our visit, called "cookies," on our hard drive so that when we return to that site, the cookie data will reveal that we have been there before. The web site might offer us products or advertisements tailored to our interests, based on the contents of the cookie data.

---

[499] Bryan, Pfaffenberger , "Protect Your Privacy on the Internet", John Wiley & Sons, Bk&CD-Rom edition , USA, 1997 at p 85
[500] Microsoft Press Computer Dictionary, 3d ed. 1997 , at p 382
[501] ibid at , p 73
[502] ibid, at p 82
[503] Bryan Pfaffenberger , "Protect Your Privacy on the Internet", John Wiley & Sons, Bk&CD-Rom edition , USA, 1997, at 120-40

Most cookies are used only by the web site that placed it on our computer. But some, called third-party cookies, communicate data about us to an advertising clearinghouse which in turn shares that data with other online marketers. Our web browser and some software products enable us to detect and delete cookies, including third-party cookies[504].

A personal computer linked to the Internet can reveal confidences by their acceptance of "cookies," also known as "persistent client-side hypertext transfer protocol files."[505] These terms refer to identification tags and other blocks of data that a Web site sends to and stores on the hard drive of the computer of anyone who visits it[506].When an individual returns to this same site at a later date, her browser automatically sends a copy of the cookie back to the Web site; the data identify her as a previous visitor and allow the site to match her to details regarding her prior visit[507]. As the Microsoft Computing Dictionary explains, "cookies are used to identify users, to instruct the server to send a customized version of the requested Web page, to submit account information for the user, and for other administrative purposes." This definition is, however, misleadingly soothing: cookies are a ready source of detailed information about personal online habits[508].

To begin with, anyone who sits at another's computer or has remote access to it through an internal network can examine the machine's cookies to gain the names of the Web sites that placed these blocks of data[509]. In addition, access to the cookies placed on one's computer is available from the Internet. Cookies are

---

[504] Privacy Rights In cyberspace, http://www.privacyrights.org/fs/fs18-cyb.html , visited on 23 Aug 2005

[505] Microsoft Dictionary, supra note 500, at 119. Somewhat confusingly, the disks found inside a standard floppy disk case or a zip drive are also called "cookies."

[506] See Persistent Cookie FAQ ,visited Sept. 2, 2003, http://www.cookiecentral.com/-faq.htm, visited on 2 Nov 2005

[507] See ibid

[508] Paul M. Schwartz, Privacy and Democracy in Cyberspace, Vanderbilt Law Review, Vol. 52:1609 at p 1624

[509] *See* MICROSOFT DICTIONARY, supra note 500, at p 92 (providing a definition of "clickstream" data);

designed to report back exclusively to the Web site that placed them and to reveal only a particular identification number assigned by that site on previous visits. Nevertheless, access to cookies from the Internet can turn this numerical tag and information associated with it into "personal information." Once Web sites identify a specific visitor, they can match her to their rich stores of "clickstream data," which is information about the precise path a user takes while browsing at a Web site, including how long she spent at any part of a site[510]. Such finely grained information exists because, after all, a person only "moves" about cyberspace by means of a series of digital commands that her computer sends to HTTP (Hyper Text Transport Protocol) servers[511].A Web site's collection of the names and addresses of its visitors is one way that this linkage takes place. One way that this linkage takes place is by a Web site's collection of the names and addresses of its visitors, which often occurs through different kinds of registration requirements or through participation in a sweepstake at the site[512].Disclosure is not generally made, however, regarding the consequences of registration or participation in these sweepstakes. In addition, some browsers can be set to provide one's name and home address, thereby furnishing another means for the site that set the cookie to identify a specific computer user[513].As for technical limitations aimed at restricting the reading of a cookie to the Web site that set it, these can be made ineffectual. At the simplest level, nothing forbids the company that set a cookie from using it to gather personal data and then selling this information to third parties or sharing it with an affiliate[514].In addition, under the right circumstances, a third party can gain

---

[510] ibid

[511] Knag, Jerry , Information Privacy in Cyberspace Transactions, 50 STAN. L. REV. 1193, 1198 (1998) (explaining that in cyberspace, "you are invisibly stamped with a bar code").

[512] Bryan Pfaffenberger **,**Protect Your Privacy on the Internet, John Wiley & Sons, Bk&CD-Rom edition , USA, 1997, at 59-60

[513] *See* Netscape, Cookies and Privacy Frequently Asked Questions , available at http://www.home.netscape.com/products/security/resources/faq.cookies.html (explaining that "cookies can be used to store any information that the user volunteers"), visited 2 Sep 2003

[514] As an example, Microsoft purchased Hotmail, a free Internet e-mail service, to gain access to Hotmail's existing customer base of 9.5 million subscribers. See Microsoft Finds Free Email for MSN , available at http://www.wired.com/news/news/business/story/-9450.html . Since Microsoft's purchase of this company at the end of 1997, Hotmail has grown to 28 million accounts. Polly

information from a cookie without recourse to the company that set it. Because most cookies are placed in the same disk files, third parties on the Web can use malicious code to upload the contents of an entire cookies file. Moreover, a series of different software "bugs" permit the overriding of restrictions set on the sharing of cookies[515]. Finally, a recent news story reported that some existing cookie files are accidentally being transmitted to Web sites other than the ones that set them[516]. In some cases, these transmitted data include identification information, including PINs (Personal Identity Numbers), used at the site that set the cookies. The current best explanation for this software problem is that computer crashes or other hardware problems "corrupted" the cookie files.[517]

### 4.5.3 DoubleClick Shock and Cookies

Use of cookies to gather user's information and its legal implications was first considered by courts in Doubleclick case. In a class action lawsuit against DoubleClick[518], a number of plaintiffs complained the internet advertising company's use of cookies to track web surfers violated the Electronic Communiation Privacy Act (ECPA). The Court dismisses claims advanced by the plaintiff class under the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and the Wiretap Act arising out of Doubleclick's use and placement of "cookies" on plaintiffs' computers. Doubleclick uses such "cookies" to gather information about the users' use of Doubleclick client web sites. Because

---

Sprenger, Hotel Hotmail, available at http://www. wired.com/-news/news/business/story/18617.html , visited on 23 Oct 2005

[515] See Cookie Exploit, available at ,http://www.cookiecentral.com/bug/-index.shtml , visited 3 Sep 2005

[516] See What's in them Cookies? Web Site is Finding Out, PRIVACY TIMES, Feb. 15, 1999, at p 1

[517] ibid

[518] DoubleClick, a Delaware corporation, is the largest provider of Internet advertising products and services in the world. Its Internet-based advertising network of over 11,000 Web publishers has enabled DoubleClick to become the market leader in delivering online advertising. DoubleClick specializes in collecting, compiling and analyzing information about Internet users through proprietary technologies and techniques, and using it to target online advertising. DoubleClick has placed billions of advertisements on its clients' behalf and its services reach the majority of Internet users in the United States

Doubleclick's clients consented to such information gathering, the court held that Doubleclick's activities did not run afoul of either the Electronic Communications Privacy Act or the Wiretap Act. The court also dismissed the claims plaintiffs advanced under the Computer Fraud and Abuse Act because any damages caused by Doubleclick's activities did not meet the threshold required by the Computer Fraud and Abuse Act[519].

The information gathered by Doubleclick falls into three categories, described by the court as GET, POST and GIF. Typically a user accesses a Doubleclick client web site in response to a query to a search engine. Doubleclick will gather information contained in this query string, known as GET information (get me information about ....). Doubleclick will also gather information about a user that he POSTs to a Doubleclick web site in response to a query by the site, such as a request for that user's name and e-mail address. Lastly, Doubleclick will use a GIF tag to track the users' movements thru the client web site, such as the pages in the site the user visited. Doubleclick will gather this information as well[520].

Doubleclick uses this information to select the advertising the user will see when he visits a Doubleclick client web site. The user will send a command seeking access to a web site. The command will go to the servers housing that web site, which will deliver the site's contents, minus advertising, to the user. The user will also receive a link that instructs the user's computer to send a communication automatically to Doubleclick's servers. This will cause the user's computer to send a communication to Doubleclick's servers, which communication provides the number of the cookie Doubleclick has placed on the user's computer. Doubleclick uses this information to identify the user and determine the appropriate advertising that should be presented to him. Doubleclick then causes that advertising to appear on the web site the user sought by sending it to his computer. In addition, Doubleclick will update the users' profile with information of the type noted above that is gathered during this

[519] In Re DoubleClick, Inc. Privacy Litigation, 154 F.Supp.2d 497 (S.D.N.Y. 2001) available at http://www.nysd.uscourts.gov/courtweb/pdf/D02NYSC/01-03797.PDF , visited on 2 Nov 2005
[520] ibid at p 7

particular web site query. Users can prevent Doubleclick from obtaining this information by visiting Doubleclick's web site and requesting an opt-out cookie, or by configuring their browsers so as to prevent any cookies from being placed on their computers[521].

The plaintiffs contended that this conduct violated the Electronic Communications Privacy Act, 18 U.S.C. Section 2701[522] . ("ECPA"), the Wiretap Act, 18 U.S.C. Section 2510[523], and the Computer Fraud and Abuse Act, 18 U.S.C. Section 1030[524], ("CFAA"), plaintiffs commenced this class action suit. Plaintiffs also asserted a number of state law claims, including invasion of privacy and trespass.

Doubleclick argued that its conduct was exempt from the ECPA because it was authorized by its clients, to whom plaintiffs' communications were directed. The court agreed, and dismissed plaintiffs' ECPA claims. The court found that the facility through which the electronic information services at issue (communications between plaintiffs and the Doubleclick client web sites) was provided was the

---

[521] ibid at p 8

[522] It is a violation of the ECPA to "access without authorization a facility through which an electronic information service is provided ... and thereby obtain[] ... access to a wire or electronic communication while it is in electronic storage in such system ...". The statute contains an express exception, however, exempting from its coverage "conduct authorized ... (2) by a user of that service with respect to a communication of or intended for that user." 18 U.S.C. 2701(c)(2).

[523] This section states that “Any person who intentionally intercepts ... [an] electronic communication" violates the Wiretap Act. However, the statute contains an express exception for one who intercepts such a communication "where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortuous act ...".

[524] It is a violation of the Act to "intentionally access a computer without authorization ... and thereby obtain ... information from any protected computer ...". However, the statute sets a damage threshold that must be met before a claim for damages can be pursued. Under the statute, 18 U.S.C. Section 1030(g), "any person who suffers damage or loss by reason of a violation of this section may maintain a civil action ... to obtain compensatory damages and injunctive relief or other equitable relief. Damages for violations involving damage as defined in section (e)(8)(A) are limited to economic damages ...". Under section 18 U.S.C. section 1030(e)(8), damage is defined as "any impairment to the integrity or availability of data, a program, a system or information that - (a) causes loss aggregating at least $5000 in value during any 1-year period to one or more individuals; (b) impairs medical care; (c) causes physical injury; (d) threatens public health or safety."

service by which plaintiffs were provided access to the Internet from their home or other PCs. The court further found that Doubleclick's client web sites were authorized users of those services. Lastly, the court found that each of the communications as to which Doubleclick gather information were communications addressed to its clients web sites (either seeking access to that web site (a GET), or a portion thereof (a GIF) or responding to a query on that web site (a POST)[525]. As Doubleclick's clients authorized Doubleclick to access that information, the gathering in question was exempt from the ECPA. It should be noted that Doubleclick does not gather information from the users' computer, or any information other than that derived from the users' use of a Doubleclick client web site. The court further held that accessing "cookie" identification numbers fell outside the ambit of the statute, because the statute only covered communications in "electronic storage", which relates only to communications "temporarily stored" or "for a limited time." "The cookies long term residence on plaintiffs' hard drives place them outside of Section 2510(17)'s definition of 'electronic storage' and hence the protection under exception clause"[526]

The court found that Doubleclick had intercepted electronic communications between plaintiffs and Doubleclick's clients. However, the court further held that Doubleclick's client web sites had consented to such interception. Thus, Doubleclick's acts were exempt from the Wiretap Act provided the interception was not for the purpose of committing a criminal or tortuous act[527].

Lastly, the court held that plaintiffs could not establish a claim against Doubleclick for violating the CFAA because they could not establish the requisite damage there under. Plaintiffs argued that this damage threshold did not apply because it was inapplicable to a "loss" caused by Doubleclick's actions. As noted above, the statute creates a cause of action in any individual "who suffers damage or loss by reason of

[525] In Re DoubleClick, Inc. Privacy Litigation, 154 F.Supp.2d 497 (S.D.N.Y. 2001) available at http://www.nysd.uscourts.gov/courtweb/pdf/D02NYSC/01-03797.PDF at p 25, visited on 2 Nov 2005
[526] ibid at p 45
[527] ibid at p 56

a violation ...". While the court conceded there was "ambiguous" and "inconsistent" language in the statute, it held that the Legislative history and existing case law indicated that whatever type of injury a plaintiff sustained, be it damage or loss, had to meet the statutory minimum[528].

The implications of Doubleclick case is that if user consents to the collection of personal information by a cyberspace entity, then he cannot complain. However, there is an obligation on the part of the collector to adhere to accepted principles of data collection or as outlined in OECD guidelines for personal data collection.

### 4.5.4 Internet Service Providers (ISP)

Access to the Internet generally requires an individual to utilize an ISP, which is the entity that supplies Internet connectivity. ISPs can take roughly two forms. First, commercial entities, such as American Online ("AOL"), provide access to the internet for a monthly fee. Second, other entities, such as employers or schools, supply Internet access, often without a fee; these bodies either function directly as an ISP or outsource this task to another company[529].

ISPs obtain access to detailed and sometimes highly sensitive information about their customers' behavior on the Internet. ISPs can combine these data with profiling information, which their clients share with them, as well as with information purchased from direct marketing companies[530]. Many outside entities, both governmental and commercial, are increasingly seeking access to these rich databases of personal information[531].

ISPs are in an advantageous position to tie together the information that exists about anyone who surfs the Web. First, the ISP has highly accurate data about the identity of anyone who uses its services. This information is within its grasp because the ISP generally collects the client's name, address, phone number, and credit card number

[528] ibid at p 59

[529] See Lawrence Lessig, The Path of Cyberlaw, 104 YALE L.J.1743, 1748-49 (1995) (noting how a systems operator at a university can monitor activities of students and faculty on the Internet).

[530] See Edward C. Baig et al., Privacy, BUS. WK., Apr. 5, 1999, at 84 ("Personal details are acquiring enormous financial value. They are the new currency of the digital economy.").

[531] ibid

at the time it assigns an account[532]. Second, the ISP has detailed information about the Internet behavior of each of its customers. Through its role as an entrance ramp to the Internet, the ISP gains access to clickstream data and other kinds of detailed information about personal online habits[533]. It can easily take these scattered bits of cyberspace data, pieces of which at times enjoy different degrees of practical obscurity, and make them into "personal information" by linking them to the identity of its customers[534].

The question whether ISPs should disclose the identity of its subscribers without warrant was considered by US court in Timoty McVeigh v. Cohen[535]. AOL was involved in this case which was the chief provider of Internet access in the United States with over nineteen million subscribers[536]. In 1996, AOL surrendered subscriber information about Timothy McVeigh, one of its customers, to the United States Navy, which believed that these data gave it grounds to court martial him. The contested investigation had started because McVeigh, a highly decorated enlisted man assigned to a nuclear submarine, had sent an e-mail to a crew member's wife, who was a volunteer for a charity[537].AOL provides its subscribers with up to five different e-mail names, or "aliases," per account; McVeigh used his AOL account to join in a charity drive, but inadvertently sent his communication under his e-mail name "boysrch."[538] Through an option available to AOL subscribers, the crew member's wife searched through the "member profile directory" to locate additional information about the sender of this e-mail[539].Although this profile did not include his full name, address, or phone number, it specified that "boysrch" was an AOL subscriber named Tim, who lived

---

[532] Kang, Jerry , Information Privacy in Cyberspace Transactions, 50 STAN. L. REV. 1193, 1198 (1998) at p 1233

[533] ibid at p 1234

[534] ibid at p 1234

[535] 983 F. Supp. 215 (D.D.C. 1998) (finding ECPA bars government from obtaining a user's private information from an online service provider absent a warrant, subpoena, or court order) available at http://www.tomwbell.com/NetLaw/Ch05/McVeigh.html , visited on 23 Dec 2005

[536] ibid

[537] ibid

[538] ibid

[539] ibid

in Honolulu, worked in the military, and identified his marital status as "gay."[540] At this moment, the ISP's role became critical. Once McVeigh's e-mail and the directory information were brought to the Navy's attention, a military investigator promptly contacted AOL[541]. Without identifying himself as representing the government, the investigator explained that he wished to find out the identity of "boysrch". Despite its established policy otherwise, AOL promptly turned over subscriber data that linked McVeigh to this specific account[542].

The court held that the action of AOL illegal under the Electronic Communications Privacy Act of 1996 ("ECPA"). The ECPA, enacted by Congress to address privacy concerns on the Internet, allows the government to obtain information from an online service provider, as the Navy did in this instance from AOL,but only if (required to satisfy two conditions) viz.,

a) it obtains a warrant issued under the Federal Rules of Criminal Procedure or state equivalent; or

b) it gives prior notice to the online subscriber and then issues a subpoena or receives a court order authorizing disclosure of the information in question[543].

Further the court observed that "…….In these days of "big brother," where through technology and otherwise the privacy interests of individuals from all walks of life are being ignored or marginalized, it is imperative that statues explicitly protecting these rights be strictly observed. Certainly, the public has an inherent interest in the preservation of privacy rights as advanced by Plaintiff in this case. With literally the entire world on the world wide web, enforcement of the ECPA is of great concern to those who bare the most personal information about their lives in private accounts through the Internet."[544]

This clearly demonstrates that right to privacy is limited by statutory provisions. Had the Navy department obtained warrant before taking the information from AOL, the action of the department could have been valid under ECPA and plaintiff

[540] ibid
[541] ibid
[542] ibid
[543] See 18 U.S.C. § 2703 (b)(A)-(B), (c)(1)(B).
[544] Supra Note 535

might have been left with the only option of questioning reasonableness of the order.

What is pertinent to note here that the court could not have protected the privacy of a private individual under ECPA enjoyed by Mcveigh, Navy officer because of the congressional mandate "Don't Ask, Don't Tell, Don't Pursue"[545]. The problem with the ECPA is that it permits ISPs to disclose subscriber information to entities other than the government and in cyberspace most of the entities are non-governmental.

This is clearly demonstrated by a Michigan court in Jessup-Morgan v. AOL, Inc[546]. In this the court held that ECPA does not regulate disclosure to private individual of identity of a subscriber of an electronic communication service. In this case AOL disclosed the private information of plaintiff subscriber who was facing the charge of offensive posting after being served with subpoena.

This disclosure fits in with a pattern of behavior on AOL's part; it has sold different kinds of subscriber information to third parties, such as direct marketers, and even proposed sale of home phone numbers before a storm of protest forced it to change this plan[547].

### 4.5.5 Web Bugs

A web bug is a graphic in a web site or an "enhanced" e-mail message that enables a third party to monitor who is reading the page or message. The graphic may be a standard size image that is easily seen, or it may be a nearly invisible one pixel graphic. E-mail messages that include graphic displays like web sites are known as enhanced messages, also called stylized or HTML e-mail. The web bug can confirm when the message or web page is viewed and record the IP address of the viewer.

---

[545] In McVeigh, Judge sporkin observed "at this point in history, our society should not be deprived of the many accomplishments provided by people who happen to be gay.The Don't Tell, don't Ask . Don't Pursue was a bow to society's growing recognition of this fact.

[546] 20 F. Supp. 2d 1105 (E.D. Mich. 1998) available at http://www.tomwbell.com/NetLaw/Ch05/Jessup-Morgan.html, visited on 26 Dec 2005

[547] Seth Schiesel, American Online Backs Off Plan to Give Out Phone Numbers, N.Y. TIMES ON THE WEB 1-3 (July 25, 1997) http://www.nytimes.com/library/cyber/week/-072597aol.htm

The IP address is a multi-digit number that uniquely identifies a computer or other hardware device (such as a printer) attached to the Internet[548].

According to a recent survey by the Federal Trade Commission ("FTC"), up to eighty-five percent of Web sites collect personal information from consumers[549]. A widespread capture, sharing, and commercialization of personal data take place on this part of the Internet. Web sites collect personal data through cookies, registration forms, and sweepstakes that require surrendering e-mail addresses and other information[550]. Other invasions of privacy relating to Web sites involve archives of comments made on the "Usenet" or to "list servs"; the deceptive promises that Web sites sometimes make about privacy practices; and, finally, an increase by Web sites of the availability of information about behavior both in cyberspace and in Real Space[551]. These additional problem areas will now be examined in turn. Participation on the "Usenet" or in a "list serv" has significant informational consequences. The Usenet allows participants to post communications into a database that others can access; list servs are listings of names and e-mail addresses that are grouped under a single name[552]. Although sending messages to these areas feels like an ephemeral activity, an individual may be creating a permanent record of her opinions. Transcripts of contributions to both the Usenet and list servs are sometimes collected and archived, often without disclosure to participants and without restrictions on further use[553]. One such catalogue of these comments, "www.deja.com," provides four different archives, including one for "adult" messages.

---

[548] Privacy Rights In cyberspace, available at ,http://www.privacyrights.org/fs/fs18-cyb.html , visited 12 Jan 2005

[549] See FTC, PRIVACY ONLINE: A REPORT TO CONGRESS 7-14 (June 1998) ,available at http://www.ftc.gov/os/1999/07/SFAtestimony.htm , visited on 23 Sep 2005

[550] ibid at p 88-89

[551] ibid at p 141-146

[552] Microsoft Press Computer Dictionary, 3 ed, 1997, at p 286

[553] See, e.g., Deja.com , available at , http://www.deja.com , visited don 3 Sep 2005

The FTC's enforcement action in 1998 against the GeoCities company provides a further illustration of weak privacy practices at Web sites[554]. GeoCities markets itself as a "virtual community"; it organizes its members' home pages into forty different areas, termed "neighborhoods." In these areas, members can post a personal Web page, receive e-mail, and participate in chat rooms[555].Non-members can also visit many areas of GeoCities. According to the FTC, GeoCities engaged in two kinds of deceptive practices in connection with its collection and use of personal information[556]. First, although GeoCities promised a limited use of the data it collected, it in fact sold, rented, and otherwise disclosed this information to third parties who used it for purposes well beyond those for which individuals had given permission[557]. Second, GeoCities promised that it would be responsible for maintenance of the data collected from children in the "Enchanted Forest" part of its Web site[558]. Instead, it turned such personal information over to third parties, whom it had dubbed "community leaders."[559] Finally FTC settled the issues with Geocities[560]. Through the enactment of the Children's Online Privacy Protection Act in 1998, however, Congress has created strong pressure to end at least some deceptive practices regarding the collection and use of children's personal data on the Internet. Yet, adults on the Web are unprotected by this law.

---

[554] *See* GeoCities, File No. 9823015 (Fed. Trade Comm. 1998) (agreement containing consent order). The Geo-Cities Consent Order can also be found at http://www.ftc.gov/os/1998/-9808/geo-ord.htm , visited on 3 Sep 2005

[555] ibid

[556] For a discussion, *see* FTC, Analysis of Proposed Consent Order to Aid Public Comment , available at http:www.ftc.gov/os/1998/9808/9823015.-ana.htm, visited on 3 Sep 2005. The GeoCities Web site was available at http://www.geocities.com, but now part of Yahoo., visited on 23 Sep 2005

[557] ibid

[558] ibid

[559] ibid

[560] Despite the adverse publicity, GeoCities continued to grow, and just five months after the settlement and at the peak of the internet boom, Yahoo agreed to buy the company in a stock deal reported to be worth $3.6 billion. The deal was completed in May 1999 and today GeoCities is a fully integrated part of Yahoo's diverse offerings of web services.

### 4.5.6 Spyware and Adware

Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes is known as spyware. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware[561] and freeware[562] applications do not come with Spyware[563]. Once installed, the Spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers[564].

Spyware programs usually collect information from a user's computer – personal information, such as a name or an email address and send it back to their host server[565].

Some Spyware programs collect information using "keystroke loggers[566]," which capture information about the user's computer activities, including cookies and time spent on certain sites. Some capture all keystrokes users make; others are more

---

[561] Software distributed freely, but with certain conditions applying to it. Either the software is released on a trial basis only, and must be registered after a certain period of time, or in other cases no support can be offered with the software without registering it. In some cases direct payment to the author is required, Legend Communications, available at www.legend.co.uk/resources/gloss.html , visited 20 Jan 2006

[562] Software which is distributed free by the author. Although it is available for free, the author retains the copyright, which means that it cannot be altered or sold. Introduction to Internet Research, available at valencia.cc.fl.us/lrcwest/lis2004/glossary.htm, visited 20 Jan 2006

[563] Tribal Justice Information system, available at www.tjiss.net/glossary_s.html , visited on 20 Jun 2006

[564] *See* http://www.webopedia.com/TERM/s/spyware.html , visited 20 Sep 2005

[565] A recent study found that the average computer houses 28 items of monitoring software, unbeknown to the user.( Source: Internet Service Provider Earthlink and Webroot Software )

[566] Keystroke logging (often called keylogging) is a diagnostic used in software development that captures the user's keystrokes. It can be useful to determine sources of error in computer systems and is sometimes used to measure employee productivity on certain clerical tasks. Such systems are also highly useful for law enforcement and espionage—for instance, providing a means to obtain passwords or encryption keys and thus bypassing other security measures. However, keyloggers are widely available on the internet and can be used by anyone for the same purposes, available at http://en.wikipedia.org/wiki/Keylogger, visited on 2 Sep 2005

focused, recording Web sites visited, passwords, emails, credit card numbers, and so on. Most keyloggers are invisible and save recorded keystrokes into a log file that is transmitted periodically back to the host server. Some can even record both sides of instant messaging chat conversations (for example, MSN® Messenger and Yahoo!® Messenger)[567].

Although similar, adware is distinguished from spyware by the fact that, when downloading adware, the user is first given an opportunity to agree to its being placed on his or her computer. The explanation of an adware program and what it will do is often buried in a long, complex End-User License Agreement (EULA) that many users simply scroll through and accept without reading completely. In practice, adware acts as spyware. Both may trigger the display of pop-up or banner advertisements, and both may gather and transmit information from the user's computer[568].

Spyware is fast-becoming the biggest PC annoyance these days, degrading system performance, tracking our computing habits, popping up annoying advertisements, and even stealing our important personal information. Detecting and removing spyware can be difficult, since it occurs in so many different forms[569].

### 4.5.7 Marketing uses and SPAM

Records of browsing patterns are a potentially valuable source of revenue for online services and commercial web site operators. Direct marketers can use such data to develop targeted lists of online users with similar likes and behaviors. Such data can also lead to unsolicited e-mail, known as "spam". Additionally, browsing data may prove embarrassing for users who have accessed sensitive or controversial materials online.

---

[567] ibid

[568] eLearners.com, available at http://www.elearners.com/resources/advertising-glossary.asp, visited on 20 Jan 2006

[569] Crystal Blackshear, Tiffany Carlisle, Kara Cook, And Sean Faulkner The Dangers Of Adware And Spywarelaw And The Internet, Fall 2004, available at http://gsulaw.gsu.edu/lawand/papers/fa04/blackshear_carlisle_cook_faulkner/ , visited at 20 Jan 2006

In US spam is regulated through the CAN-SPAM Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing Act). This enactment establishes requirements for those who send commercial email, spells out penalties for spammers and companies whose products are advertised in spam if they violate the law, and gives consumers the right to ask e-mailers to stop spamming them.

The law, which became effective January 1, 2004, covers email whose primary purpose is advertising or promoting a commercial product or service, including content on a Web site. A "transactional or relationship message" email that facilitates an agreed-upon transaction or updates a customer in an existing business relationship may not contain false or misleading routing information, but otherwise is exempt from most provisions of the CAN-SPAM Act.

The Federal Trade Commission (FTC), US consumer protection agency, is authorized to enforce the CAN-SPAM Act. CAN-SPAM also gives the Department of Justice (DOJ) the authority to enforce its criminal sanctions. Other federal and state agencies can enforce the law against organizations under their jurisdiction, and companies that provide Internet access may sue violators, as well[570].

### 4.6 Privacy policies and web seals

Many Governments urge commercial web site operators to spell out their information collection practices in privacy policies posted on their web sites. Most commercial web sites now post policies about their information collection practices. But most of these policies provide for "opt-out" option , which is cumbersome and inconvenient for net users.

Website privacy policies are a recent phenomenon, having come into existence in the late 1990s. The universal feature of website privacy policies is that they are accessible as a link from the home page of many websites. Many sites also have links to the privacy policy from areas within the site, such as from internal pages

[570] Facts for Business, available at http://www.ftc.gov/bcp/conline/pubs/buspubs/canspam.shtm , visited on 3 Sep 2005

that request customer data. Privacy policies range from a half-page to ten pages in length. In terms of their apparent intent and rhetorical structure, privacy policies are hybrid documents that reflect both public relations and legal concerns. On the one hand, privacy policies often have a chatty and disarming tone that clearly seems motivated by an attempt to create an air of closeness and intimacy between the site and its users. On the other hand, privacy policies are becoming more legalistic in tone[571]. Privacy policies typically begin with some warm and fuzzy language about the online entity's respect for its users' privacy. Typical in this regard are statements such as, "At 1-800-flowers.com, we recognize and respect the importance of maintaining the privacy of our customers and members."[572] Some of the more scrupulous sites explicitly acknowledge the privacy rights of users in their opening remarks. Wal-Mart's privacy policy states, "We believe that you have a right to know, before shopping at Walmart.com or at any other time, exactly what information we might collect from you, why we collect it and how we use it."[573] Nike's privacy policy begins, "Nike is committed to respecting the privacy rights of all visitors to our web site."[574]

In the opening statements of their privacy policies, some sites are explicit in stating that their goal is to create a relationship of confidence and trust with consumers. The Walt Disney privacy policy begins, "The Walt Disney Internet Group is committed to helping you make the most of your free time on the Internet within a trusted environment . . . . We hope that this disclosure will help increase your confidence in our sites and enhance your experience on the Internet."[575] The introduction to the

---

[571] Hetcher, Steven ,Changing The Social Meaning Of Privacy In Cyberspace, Harvard Journal of Law & Technology Volume 15, Number 1 Fall 2001

[572] 1-800-flowers.com Privacy statement, *at* http://www.1800flowers.com/flowers/security/index.asp, visited on 11 Oct. 2004

[573] Walmart.com Security & Privacy, *at* http://www.walmart.com/cservice/ca_securityprivacy.gsp , visited on 11 Oct. 2004. Wal-Mart has an exemplary privacy policy. Sites of old economy firms like Wal-Mart are of particular interest, as they demonstrate the penetration of the growing ethos of Internet privacy beyond the now outdated notion of the dot.com economy. The Internet was never a marketplace but rather a technology platform.

[574] Niketown.com Privacy Policy, available *at* http://niketown.nike.com/info/privacy.jhtml, visited on 11 Oct 2004

[575] Disney.com Privacy Policy, *at* http://disney.go.com/legal/privacy_policy.html , visited on 11 Oct 2003

Wal-Mart privacy policy states that, "The security of your personal information is very important to us. . . . We value your trust very highly, and will work to protect the security and privacy of any personal information you provide to us and will only use it as we have described in our Privacy Policy."[576] Sears.com states, "We value the trust you place in Sears, Roebuck and Co . . . . We want to ensure that you understand what information we gather about you, how we use it, and the safeguards we have in place in order to protect it."[577]

Some sites make it apparent that they judge the moral relationship between website and consumer to be a two-way street. The first paragraph of the MadonnaFanClub.com privacy policy states that the site "always respects the privacy of Fan Club members and visitors to our website."[578] The last paragraph of the short document states that, "All information contained on this site is copyrighted. Your cooperation in respecting these copyrights is appreciated."[579] Here, a core normative principle is at play. Because the site holds itself out as respectful, it is appropriate by the lights of the ordinary moral principle of reciprocity to ask for respect in return. Privacy policies that are more legalistic in tone would be unlikely to make the same request for reciprocal treatment.

On the whole, however, privacy policies are increasingly employing more overtly legalistic formulations[580]. For example, Weather.com states, "This statement and the policies outlined here are not intended to and do not give you any contractual or other legal rights."[581]Toyota's privacy policy in part reads, "Toyota does not assume

---

[576] Walmart.com Security and Privacy, available *at* http://www.walmart.com/cservice/ca_securityprivacy.gsp , visited on 11 Oct 2004

[577] Sears, Roebuck and Co. World Wide Web Site Customer Information and Privacy Policy, available at http://www.sears.com , visited on 2 Oct 2004.

[578] Madonna Fan Club Privacy Statement, available at http://www.madonnafanclub.com/privacy.html , visited on 11 Oct 2004.

[579] See Eric, Roston, How to Opt Out of Database Sharing; Who's Got Your Number?, TIME, July 2, 2001, at 46.

[580] See Eric ,Roston, How to Opt Out of Database Sharing; Who's Got Your Number? TIME, July 2, 2001, at 46.

[581] Weather.com Privacy Statement, available *at* http://www.weather.com/common/home/privacy.html , visited on 3 Jul 2004

any responsibility for the accuracy, completeness or authenticity of any information contained on this site. This site and all information and materials contained herein, is provided to you "as is" without warranty of any kind."[582]Toyota further states, "Toyota shall not be responsible for any harm that you or any person may suffer as a result of a breach of confidentiality in respect to your use of this site or any information you transmitted to this site."[583] Toyota's harsh legalistic tone illustrates the tension between a privacy policy crafted as a document meant to create trust in users and a legal document meant to protect the company against potential liability. The use of more legalistic language is perhaps not surprising, given that privacy policies are starting to play a role in lawsuits[584]. If privacy related lawsuits become more prevalent, privacy policies may become even more legalistic.

In the past few years, most websites have begun to address privacy concerns to one extent or another[585]. There are a number of common practices that websites are beginning to adopt. To some extent, these practices track the fair information practice principles that are being promoted by the privacy entrepreneurs. The FTC has noted that it is not possible to specify in detail how the privacy principles should be implemented, as the meaning of the principles will vary depending on the particular activities of the site in question[586]. Several surveys conducted to understand the privacy policies indicate how complex and varied the personal data practices of websites are becoming[587].

---

[582] Toyota Privacy Policy, available at http://www.toyota.com/html/privacy/index.html ,visited on 11 Oct 2003

[583] ibid

[584] See Judnick v. DoubleClick, No. CU-421 (Main Cty. Sup. Ct., filed Jan. 27,2000)

[585] See Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace, A Federal Trade Commission Report to Congress 10 (May 2000), available at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (discussing the Commission's survey findings, which demonstrate continued improvement with eighty-eight percent of websites in the random sample posting at least one privacy disclosure), visited on 2 Nov 2005

[586] See Federal Trade Commission, Privacy Online: A Report to Congress (June 1998), available at http://www.ftc.gov/reports/privacy3/toc.htm , visited 2 Nov 2005

[587] See Federal Trade Commission, Fair Information Practices in the Electronic Marketplace, available at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf , visited on 7 Nov 2005

Privacy seals signify that a company respectfully uses the personal information we provide. Privacy seals are the most difficult to obtain, as they require the company to undergo an extensive certification process that exposes internal data collection and usage processes. A privacy seal is the only type of seal that probes what happens behind the scenes. Seal programs also offer ongoing monitoring, and one can file a complaint with the issuing authority if you feel there has been misconduct[588]. Examples include TRUSTe, BBB Online Privacy, and ESRB Privacy.

### 4.6.1 The Platform for Privacy Preference (P3P)

Predictably, many people complain that websites' privacy policies are difficult to understand, sometimes because they are vague and other times because they are full of legalese. Partially as result of this complaint, the World Wide Consortium (W3C) has developed something called the Platform for privacy Preference, commonly known as P3P, a technological approach to interpreting and applying privacy policies. As sated by the W3C :

"At most basic level, P3P is standardized set of multiple questions, covering all the major aspects of a Web site's privacy policies. Taken together, they present a clear snapshot of how a site handles personal information about its users. P3P enabled websites make this information available in a standard, machine readable format. P3P enabled browsers can read this snapshot automatically and compare it to the consumer's own set of privacy preferences. P3P enhances user control by putting privacy polices where users can find them, in a form users can understand, and most importantly , enables users to act on what they see."[589] Any website may choose to implement P3P, but no law requires any website to do so.

---

[588] How Do You Make Sense of Web-Based Seals? , available at http://www.truste.org/articles/seals_comparison.php , visited on 20 Jan 2005

[589] Platform for Privacy Preferences (P3P), available at www.w3c.org/p3p , visited on 20 Sep 2005

In theory, P3P should help consumers protect their privacy online. In practice, however, the impact of P3P is unclear. Although, by early 2002, six of the top ten websites had adopted P3P, and the other four websites were considering it[590], the technology has not yet been widely implemented and it is not certain that consumers really understand it. In one article criticizing Microsoft's adoption of P3P in version 6 of the internet browser, two lawyers said that the technology is expensive to implement and maintain; lacks enforcement and security; confuses consumers; and could create unclear legal consequences, such as if the P3P technology cannot accurately convey a subtle distinction in a website's privacy policy[591].

Ultimately, until the acceptability of P3P becomes better known, consumers and businesses should not ignore it. In particular, consumers should understand the limits of P3P, how their web browsers interpret it, and how to respond to the messages P3P can provide. And businesses should pay particular attention to whether consumers are demanding that the site they visit implement P3P. If this privacy technology takes off, drafting a P3P complaint privacy policy could become very important for a website's success[592].

### 4.7 Workplace monitoring

Employee empowerment with information technology is not without problems. Individuals who access the Internet from work should know that employers are increasingly monitoring the Internet sites that an employee visits. Legal requirement in such cases is that employer must communicate privacy policies of the organization clearly to employees. However, "expectation of privacy by employees" in certain situations limits the employer's right to surveillance.

Irrespective of the nature of the company, all companies are feeling the impact of the technological revolution. The most obvious example is the increased use of e-

[590] Gigalaw, available at http://www.gigalaw.com/articles/2002-all/carnor-2002-04-all.html , visited on 20 Sep 2005

[591] Gigalaw, available at http://www.gigalaw.com/articles/2002-all/harvey-2002-04-all.html, visited 20 Sep 2005

[592] Isenberg, Doug, "The Giga Law- Guide to Internet Law- The One-Stop Legal Resource for Conducting Business Online", Random House Trade Paperback Edition, New York, 2000

mail and the internet at more traditional, 'old economy' companies. This increased use of technology has resulted in a new wave of sexual harassment and racial hatred claims. Particularly, e-mail messages are now providing the evidentiary basis for aggrieved employees who claim discrimination, harassment or retaliation[593].

In Smyth v. The Pillsbury Company[594], the court found that an employee who transmitted inappropriate and unprofessional messages over the company's e-mail system could not have had a reasonable expectation of privacy. Once an employee disseminated the communication over the network provided by the employer, the message was no longer private. The court flatly declared that no "reasonable expectation" of privacy could exist in e-mail communications voluntarily made by an employee[595].

In the case of Strauss v. Microsoft Corp[596]., it was found that off-color comments made through email were admissible in a sex discrimination case. In this case, Karen Strauss, a former assistant editor of the Microsoft Systems Journal sued that Microsoft discriminatorily denied her promotion to technical editor and terminated her in retaliation for her complaints regarding that promotion. In support of her allegations, Strauss offered evidence of sexiest remarks and e-mail messages allegedly referred to another female employee as the "Spandex Queen" and included his offer to a temporary receptionist that he would pay her $500 if he could call her "Sweet Georgia Brown". The supervisor also allegedly proclaimed himself 'president of the Amateur Gynecology Club'[597].

Some of the most damaging evidence offered by Strauss came in the form of mass e-mail messages distributed throughout the workplace by coworkers. One such message contained a satirical essay titled "Alice in UNIX Land." Still another

[593] Isenberg, Doug, "The GigaLaw- Guide to Internet Law", Random House Paperbacks, New York, 2002 at 299
[594] 914 F. Supp. 97, E.D. (Penn. 1996), available at http://www.fidnalaw.com , visited 22 Sep 2005
[595] ibid
[596] 1995 US Dist. Lexis 7433 (1995), Strauss v. Microsoft Corp., 856 F. Supp. 821, 825 (S.D.N.Y. 1994), available at http://www.findlaw.com , visited on 24 Nov 2005
[597] ibid

e-mail, forwarded by her supervisor included a parody of a play titled "A Girl's Guide to Condoms." In total, Strauss proffered four e-mail messages gathered from Microsoft's own network. Although the e-mail messages and remarks were unrelated to the promotion and termination decisions at issue, the court found that the evidence was relevant and admissible. As a result, Strauss arguably possessed the added ammunition to support her allegations of gender discrimination[598].

Microsoft case illustrates the potential damages presented by the informal use of e-mail in the workplace. Although inappropriate e-mail messages typically form the basis of harassment suits, they also serve as powerful evidence in support of discrimination and retaliation suits[599].

Recently an administrative law judge in New York has found that surfing the Web at work is equivalent to reading a newspaper or talking on the phone. The judge recommended the lightest possible punishment for a city worker accused of disregarding warnings to stay off the Internet[600]. This again clearly shows the fluid state of law in relation to protection of privacy in cyberspace.

### 4.8 Law Enforcement Access

In order for law enforcement officials to gain access to subscriber transactional records, authorities usually must obtain a court order demonstrating that the records are relevant to an ongoing criminal investigation.

Some of the legislation used by US authorities for the enforcement which impact on privacy over the cyberspace area as follows;

---

[598] ibid

[599] Isenberg, Doug, "The GigaLaw- Guide to Internet Law", Random House Paperbacks, New York, 2002 at p 302

[600]Silicon Valley, http://www.siliconvalley.com/mld/siliconvalley/news/editorial/14417425.htm, visited on 24 Apr 2006

(a) Fair Credit Reporting Act, 1970[601] (FCRA)- This Act places limits on the use of consumer reports, that is, "information by consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living" where the information is for, among other things, credit , insurance, or employment purposes. Businesses creating, distributing or using consumer reports must comply with FCRA.

(b) Electronic Communications Privacy Act, 1986[602] (ECPA)- The ECPA has been used , with varying success, in a number of internet related cases. The law became effective many years before the rise of the internet as a popular communications medium, but it is probably the one preexisting law that has the greatest applicability to online privacy today. In general, the ECPA governs the interception of "wire, oral or electronic communications." Although ECPA does not refer to the internet, a number of lawyers believe the Act's reference to 'electronic communications' applies to certain online activities. The ECPA defines 'electronic communications' as "any transfer of signs, signals, writing, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system that affects interstate or foreign commerce".

---

[601] The Fair Credit Reporting Act (FCRA) is an American federal law (codified at 15 U.S.C. § 1681 et seq.) that regulates the collection, dissemination, and use of consumer credit information. It, along with the Fair Debt Collection Practices Act (FDCPA), forms the base of consumer credit rights in the United States.

[602] The Electronic Communications Privacy Act of 1986 (ECPA Pub. L. 99-508, Oct. 21, 1986, 100 Stat. 1848, 18 U.S.C. § 2510) was enacted by the U.S. Congress to extend government restrictions on wire taps from telephone calls to include transmissions of electronic data by computer

(c) Health Insurance Portability and Accountability Act, 1996[603] (HIPPA) – Along with financial information, health care information is probably the most strongly protected and personal data that exists. Therefore, it's no surprise that the US Congress has passed laws that specifically protect certain health related information, HIPPA in 1996. As per the provisions of the Act, health providers are required to give clear written explanations of their privacy practices; the Act limits the disclosure of health information for non-health related purposes; compels the appointment of privacy officer; and sets civil and criminal penalties for violating privacy[604].

(d) Gramm-Leach-Bliley, 1999[605] (GLB)- This law limits the instances in which financial institutions may disclose nonpublic personal information about a consumer to nonaffiliated third parties and requires then to disclose privacy polices to all of its customers.

### 4.9 Privacy Regulation

In 1970 the German state of Hesse enacted the first data protection statute; Sweden followed in 1973 with the first national statute. Today, Austria, Belgium, the Czeh Republic, Denmark, Finland, France, Germany, Hungary, Iceland, Ireland, Italy,

---

[603] The Health Insurance Portability and Accountability Act (HIPAA) was enacted by the U.S. Congress in 1996.According to the Centers for Medicare and Medicaid Services' (CMS) website, Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The AS provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the US health care system.

[604] Health and Human Services, available at http://www.hhs.gov/news/press/2001pres/01fsprivacy.html, visited on 23 Sep 2005

[605] The Gramm-Leach-Bliley Act, also known as the *Gramm-Leach-Bliley Financial Services Modernization Act*, Pub. L. No. 106-102, 113 Stat. 1338 (November 12, 1999), is an Act of the United States Congress which repealed the Glass-Steagall Act, opening up competition among banks, securities companies and insurance companies. The Glass-Steagall Act prohibited a bank from offering investment, commercial banking, and insurance services. The Gramm-Leach-Bliley Act (*GLBA*) allowed commercial and investment banks to consolidate.

Luxembourg, the Netherlands, Norway, Portugal, Spain, Switzerland and the United Kingdom have broad privacy or data protection statutes.

These omnibus laws are often supplemented by other laws and regulations that apply to specific types of processing activities for specific subject matter. United States has broad category of legislations for the purpose of individual data protection.

European data protection laws are notable generally for four features: typically they apply to both public and private sectors; they apply to a wide range of activities, including data collection, storage, use, and dissemination; they impose affirmative obligations (often including registration with national authorities) on anyone wishing to engage any of these activities; and they have few, if any, sectoral limitations they apply without regard to the subject of data.

### 4.10 Children's Online Privacy

Although privacy on the internet is a 'hot-button' topic in general, children's privacy is certainly the hottest. As children are less able to appreciate the ramifications of disclosing personal information, they may become victims of child predators and molesters when they go online. The US Federal Trade Commission (FTC) has reported, "An investigation by the FBI and the Justice Department revealed that Chat rooms and Bulletin boards are quickly becoming the most common resources used by predators for identifying and contacting children."[606]
Children's Online Privacy Protection Act (COPPA) was enacted by US Congress in 1998 to regulate and control the website operators collection or maintenance of personal information about children who are under thirteen. In general COPPA requires that operators of websites directed to children and operators who knowingly collect personal information from children do the following;

[606] Federal Trade Commission, available at http://www.ftc.gov/os/1999/9910/64fr59888.htm , visited on 26 Jan 2006

(a) provide parents notice of their information practices[607]

(b) obtain prior verifiable parental consent for the collection, use and/or disclosure of personal information from children with certain limited exceptions for the collection of online contact information such as e-mail addresses etc[608];

(c) provide a parent, upon request, with means to review the personal information collected from his child[609];

(d) provide a parent with the opportunity to prevent the further use of personal information that has already been collected , or the future collection of personal information about that child[610];

(e) limit collection of personal information for a child's online participation in a game, prize offer other activity to information that is reasonably necessary[611] ; and

(f) establish and maintain reasonable procedures to protect the confidentiality , security and integrity of the personal information collected[612].

But accomplishing these goals is not an easy task. Indeed, after the FTC issued the Children's Online Privacy Protection Rules, many websites that had collected information from children simply decided that the law was either too complicated or too costly and they simply stopped collecting personal information from children altogether[613]. SurfMonkey , a community site for children, reportedetdly spent $50,000 to $100,000 to comply with the law's numerous legal requirements[614].

No doubt laws required for protecting privacy of individuals, but the tendency of human beings is to ignore laws which are difficult to comply even with honest

---

[607] Children's Online Privacy Protection Act of 1998 ,Title Xiii-Children's Online Privacy Protection, Sec. 1303. Regulation Of Unfair and Deceptive Acts And Practices In Connection With The Collection And Use Of Personal Information from and About Children on the Internet.

[608] ibid Sec.1303
[609] ibid Sec.1303
[610] ibid Sec.1303
[611] ibid Sec.1303
[612] ibid Sec.1303
[613] GigaLaw, available at http://www.gigalaw.com/2000/articles/isenberg-2000-07a.html , visited on 29 Dec 2005
[614] See Surf Monkey website, available at http://www.surfmonkey.com/, visited on 3 Sep 2005

attempt to obey them. COPPA is the only internet specific privacy law in US, but it is very controversial and it can be complicated. But ignoring COPPA can be painful and costly.

### 4.11 EC Directive on Data Protection and Safe Harbor Treaty

In July 1990 the commission of European Community published a draft Council Directive on the Protection of individuals with regard to the Processing of Personal Data and on the free movement of such data. The Directive requires EU member states to enact laws governing the processing of personal data. The Directive defines 'processing' broadly as "any operation or set of operations", whether or not automated, including but not limited to "collection, recording, organization, storage, adaptation or alteration, retrieval or otherwise making available, alignment or combination, blocking, erasure or destruction". "Personal data" are defined equally broadly as "any information relating to an identified or identifiable natural person". This would include not only textual information but also photographs, audiovisual images, and sound recordings of an identified or identifiable person[615].

In Europe, privacy is viewed as a "human rights" issue and in the United States, it is more often seen as a matter for contractual negotiation. US privacy advocates will, on occasion, engage in some amount of cost/benefit analysis when arguing for certain data restrictions. In contrast, European advocates argue that the preservation of privacy must be seen as sacrosanct and cannot be bent to serve commercial ends[616].

There have been obvious differences in US and European privacy approaches for decades, they took on a more serious when the European Union adopted its "Data Protection Directive". The Directive requires that the purpose of data collection and

[615] Fred H. Cate ,Privacy in the Information Age (1997), available at http://brookings.nap.edu/books/0815713169/html/14.html , visited on 20 Nov 2005

[616] ibid at p 33

the manner in which the data are to be used must be disclosed clearly to data subjects, especially , any secondary uses for direct marketing purposes must be spelled out. In addition, data subjects must be allowed to inspect and correct data about them. The Directive demands that Member states "take necessary measures to ensure that data subjects are aware of the existence of their right to object to secondary data uses". Further, it requires that a firm discontinue using a consumer's data for secondary purposes once a "justified objection" is received[617].

Discussion between the European Union and the US in relation to transboundary movement of personal data was finalized in July 2000 and an agreement was drawn known as "Safe Harbor" agreement. Under this agreement US firms wishing to handle personal data regarding European citizens must register with the US Department of Commerce, must agree to adhere to principles that are largely consistent with the more demanding approach and must provide an annual certification to the US department of Commerce[618].

### 4.12 OECD Guidelines on the Protection of Personal Data Protection

The OECD ( Organization for Economic Co-operation and Development) Guidelines on the Protection of Privacy and Transborder Flows of Personal data was adopted on 23 September 1980, and represent international consensus on general guidance concerning the collection and management of personal information. By setting out core principles, the guidelines play a major role in assisting governments, business and consumer representatives in their efforts to protect privacy and personal data, and in obviating unnecessary restrictions to transborder data flows, both on and off line.

The preamble of OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines) states that the development of

[617] ibid at p 35
[618] ibid at p 41

automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data. Privacy protection laws are required to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data[619]. Part two of the OECD Guidelines outlines principles of data collection applicable to all member countries of OECD. These principles which are regarded as Fair Information Practices (FIPP) and enforced by FTC are as follows;

(a) Collection Limitation Principle - There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject[620].

The provision of notice of a website's personal-data-related activities is the first of the fair practice principles. The principle of notice is a second order principle that supports each of the other principles[621]. It is only when a user has knowledge of the data related activities of a website that the user can make informed decisions about how to interact with the site regarding each of the other privacy principles[622]. At first glance, notice might seem like a straightforward requirement with which to comply. A site simply writes down a description of its data related practices and creates a link to this text. For some sites with simple and minimal data related practices, the provision of straightforward notice is possible. For example, the "Official Madonna Fan Club" site's privacy policy, when printed out, is only half a

[619] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

[620] ibid , principle no. 1

[621] Hetcher ,Steven, Changing the Social Meaning of Privacy in Cyberspace, Harvard Journal of Law & Technology Volume 15, Number 1 Fall 2001 at p 129

[622] ibid at p 31

page long and contains three short paragraphs[623]. The site is able to state in a straightforward manner, "We do not sell, rent or trade your personal information with others."[624] This site uses personal data in order to process commercial transactions, such as merchandise sales and membership dues. The site claims not to use cookies or other passive means of data gathering[625].Notice becomes difficult to provide, however, when a site has complex data related practices. The first layer of complexity is introduced by means of the manner in which data is collected. Users of course understand that data is being collected from them when this data is explicitly provided by them. More opaque is data collection by means of cookies and other means of so called passive tracking of user online activities. Many sites provide definitions of arcane terms such as "cookies" and "IPO addresses," and offer explanations of their importance for privacy purposes[626]. For many sites, how the personal data is gathered is the determining factor in whether the data becomes "personally identifiable information" or "personal information," as compared to "anonymous information." The information that people explicitly volunteer to the website such as name, address, social security number, age, etc. is personally identifiable in the sense that it can be traced back to particular individuals. By contrast, websites collect information through the use of cookies on such activities as the users' visitation to various sites. Sites typically state that this information is

---

[623] Madonna Fan Club Privacy Statement, available *at* http://www.madonnafanclub.com/privacy.html , visited 11 Oct 2003.

[624] ibid

[625] Weather.com Privacy Statement, available *at* http://www.weather.com/common/home/privacy.html visited on 3 July 2005.

[626] See, for example, Motorola Privacy Practices, *at* http://www.motorola.com/content/0,1037,3,00.html visited 11 Oct 2005."When you come into our site, our server attaches a small text file to your hard drive — a cookie. Your unique cookie tells us that it is you whenever you re-enter our site, so we can recall where you've previously been on our site, and what if anything, you have in your shopping cart."); Hallmark.com Privacy Policy, *available at* http://www.hallmark.com , visited 11Oct 2005) ("An IP [Internet Protocol] address is a number that is assigned to your computer when you are using your browser on the Internet. The servers that serve our web site automatically identify your computer by its IP address. We do log IP addresses, but the addresses are not linked to individual customer accounts nor are they used in any other way to personally identify our customers."

not personally identifiable[627].In other words, though the sites keep records of cookie generated information, they claim not to keep track of which personally identifiable person is attached to this information. Perhaps the most significant challenge to adequate notice arises regarding the relationships that sites have with third parties. Privacy advocates and consumers are especially concerned about the fact that personal data may be transferred to these third parties[628].Privacy policies refer to these entities as, "trustworthy third parties," "reputable third-parties,"[629] etc. The main challenge to giving effective notice is the complexity and diversity of the relationships that sites have with these third parties. The difficult issue is determining how much description is necessary in order to provide adequate notice. Some sites are moving in the direction of providing fuller descriptions of their relationships with third parties. This means, however, that their privacy policies are becoming increasingly long and complex and difficult to understand.

(b) Data Quality Principle- Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date[630].

The intuitive idea is that users should have some say when it comes to the use of their personal information by websites. Some sites, however, treat choice in the narrowest sense so as to mean simple consent or assent. Toyota writes, "By using this site, you signify your assent to the Toyota Online Privacy Policy. If you do not

---

[627] The Kinkos.com privacy policy states, "Also, Kinkos uses a reputable third party to collect and accumulate other anonymous data that helps us understand and analyze the Internet experience of our visitors. . . . This information may be stored in a cookie on your computer's hard drive. However, none of this information is personally identifiable and we only share this information in the aggregate, reflecting overall web site or Internet usage trends." Kinko's Security and Privacy Policy, available *at* http://www.kinkos.com/ privacy.html, visited 11 Oct 2005.

[628] Hetcher Steven, Changing the Social Meaning of Privacy in Cyberspace, Harvard Journal of Law & Technology Volume 15, Number 1 Fall 2001 at p179

[629] Nokia.com Privacy Policy, available at http://www.nokia.com/privacy.html visited 12 Oct 2005.

[630] [630] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html , principle no.2

agree to this policy, please do not use this site."[631] Under the heading of, "Your Consent" on its site, Nike simply states, "By using our web site, you consent to our privacy policy."[632]

Many sites, however, do offer users choices other than the option of leaving. The most common choice made available to users is whether they want to have their personal data stored with, and used, by, the site. Many sites give the user the option of removing their personal data from the site. For example, Kinkos.com states, "You can easily change any of the information you have been asked to provide by Kinko's. You can also permanently remove your information from the Kinko's database."[633]

As already mentioned, websites offer two types of consent, which are widely referred to as opt-in and opt-out. With opt-out, the user must take some positive step in order to stop what would otherwise be a default process whereby user data would be available for use by the website[634]. Typically, the user cannot simply opt-out without consequence. Sites often condition access to the site or to some portion of the site on the provision of data by consumers. Thus, opting out of the provision of data entails opting out of receiving some or all of the site's services[635]. Other sites, however, simply allow consumers to opt-out of at least some of the site's collection practices without adversely affecting the consumers' abilities to benefit from the site[636].Until recently, it has been very uncommon for websites to provide opt-in as a choice to users. A small but growing number of sites are now offering users the

---

[631] Toyota Privacy Policy, available *at* http://www.toyota.com/html/privacy/index.html, visited 12 Oct 2005

[632] Niketown.com Privacy Policy, available *at* http://niketown.nike.com/info/privacy.jhtml , visited 12 Oct. 11, 2005

[633] Kinko's Security and Privacy Policy, available at www.kinko.com , visited 2 Jan 2003

[634] Motorola Privacy Practices, *at* http://www.motorola.com/content/0,1037,3,00.html visited on 12 Oct 2003 ("You also have choices with respect to cookies. By modifying your browser preferences, you have the choice to accept all cookies, to be notified when a cookie is set, or to reject all cookies. If you choose to reject all cookies you will be unable to use those services or engage in activities that require registration in order to participate.")

[635] ibid

[636] *See* jcrew.com (permitting customers to refuse cookies and decline to receive promotional emails and catalogs without limiting the customer's shopping experience).

choice to opt-in to some or all of the site's data practices. With opt-in, personal data will not be collected or used unless the user provides his explicit permission. In particular, sites that deal with more sensitive data are beginning to offer opt-in for this data[637].

(c) Purpose Specification Principle and Use Limitation Principle - The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle provides that personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except for (i) with the consent of the data subject; or (ii) by the authority of law.

(d) Access/Participation Principle- This principle prescribes that websites provide users with access to their personal data stored with the website. It is often discussed in conjunction with the principle of allowing consumers to contest data stored at the site that they deem to be incorrect. It is getting increasingly common for sites to allow users to access their data. For example, microsoft.com states, "If you ever want to review or update your profile, simply visit the Profile Center and edit your personal information. We'll ask you to disclose your Microsoft Passport (e-mail address and password) so that only you can access your profile."[638] Despite opportunities for access, fewer sites offer the ability to contest data. One that does is

---

[637] Davidson, Paul, Capitol Hill Support Brews for Internet Privacy Laws, USA TODAY, July 12, 2001, at 3B (noting that there is consensus building for requiring opt-in for more sensitive data, such as financial and medical).

[638] *See* Microsoft.com Statement of Privacy, available at http://www.microsoft.com/info/privacy.htm visited 23 Feb 2004.

nokia.com, which states, "Nokia will on its own initiative, or at your request, replenish, rectify or erase any incomplete, inaccurate or outdated personal data."[639]

(e) Integrity/Security Principle - A solid minority of sites now address the issue of security in their privacy policies. Under the heading of "Security" in its privacy policy, Sun Microsystems unhelpfully states merely that, "We intend to take reasonable and appropriate steps to protect the Personal Information that you share with us from unauthorized access or disclosure."[640]Many sites employ Secure Socket Layer[641] ("SSL") technology to protect the security of credit card information as it is transmitted to the site[642].With SSL, the website's server scrambles the data as it travels from the user's computer to the website. It is much less common, however, for sites to make remarks in their privacy policies regarding the security of the user's data as it resides on the site's server. This latter form of security is more important than protecting the data while in transit, as most significant breaches of website security have involved hackers gaining access to

---

[639] Nokia.com Privacy Policy, available at http://www.nokia.com/privacy.html visited 23 Feb 2004.

[640] Sun Online Privacy Policy, at http://www.sun.com/privacy , visited on 3 Oct 2005

[641] SSL (Secure Socket Layer) is a protocol for encrypting and decrypting data sent across direct internet connections. When a client makes an SSL connection with a server, all data sent to and from that server is encoded with a complex mathematical algorithm that makes it extremely difficult to decode anything that is intercepted. The following is a step by step illustration of how SSL works. **Step 1**. The client makes the initial connection with the server and requests that an SSL connection be made. **Step 2**. If the server is properly configured, the server will send to the client its certificate and public key. **Step 3**. The client uses that public key to encrypt a session key and sends the session key to the server. If the server asks for the client's certificate in Step 2, the client must send it at this point. **Step 4**. If the server is set up to receive certificates, it compares the certificate it received with those listed in its trusted authorities database and either accepts or rejects the connection. If the connection is rejected, a fail message is sent to the client. If the connection is accepted, or if the server is not set up to receive certificates, it decodes the session key from the client with its own private key and sends a success message back to the client, thereby opening a secure data channel. WSFTP.server, User's Guide, available at http://www.ipswitch.com/support/ws_ftp-server/guide/v5/ch10_sslconfiga2.html , visited on 3 Nov 2005

[642] Motorola Privacy Practices, available at http:/ /www.motorola.com , visited on 6 Nov 2005 ("You also have choices with respect to cookies. By modifying your browser preferences, you have the choice to accept all cookies, to be notified when a cookie is set, or to reject all cookies. If you choose to reject all cookies you will be unable to use those services or engage in activities that require registration in order to participate."

databases in storage on a firm's website[643].Increasingly, websites are addressing the issue of the security of data stored by the site. Some sites are limiting the number of employees with access to personally identifiable data as well as employing security systems to protect the data from external intruders[644].

(f) Enforcement/Redress – Next principle is that of enforcement/redress. According to this principle, the user should be provided with some means of enforcing the above principles or of receiving redress in cases of injury due to a failure to provide protective practices that instantiate the Fair information practices. Websites have done very little to promote this norm[645].

(g) Stopping Data Transfers to Third Parties- It is important to note that the fair information practice principles do not prohibit data transfers by websites to third parties. The first two principles, notice/awareness and choice/consent, are essentially an informed consent requirement. They do not prescribe a particular substantive set of privacy protections but rather stipulate that whatever data related practices a website engages in, the site should receive the informed consent of its users as to these practices (with failure to opt-out counting as a form of consent). The latter three fair information practices provide more substantive requirements of access, security and enforcement. None of these principles, however, prohibits data transfers to third parties. Nevertheless, a small number of sites do promise that they will not sell or trade data to third parties. For example, Wal-Mart states that, "We never sell or rent your personal information to any third parties under any

---

[643] Jeffrey Kluger, Extortion on the Internet; A daring hacker tries to blackmail an e-tailer — and sparks new worries about credit-card cybertheft, TIME, Jan. 24, 2000, at 56

[644] For example, MTV's website, MTV.com, states, "We have taken steps to ensure that personally identifiable information collected is secure, including limiting the number of people who have physical access to its database servers, as well as electronic security systems and password protections which guard against unauthorized access." MTV.com Terms of Use & Privacy Policy, available *at* http://www.mtv.com/sitewide/mtvinfo/terms.jhtml#privacy , visited on 24 Feb 2005

[645] For example see barnesandnoble.com ("We're so certain that our online ordering systems are secure that we back it up with a guarantee. In the unlikely event that you are subject to fraudulent charges….we will cover the entire liability for you, up to $50, as long as the unauthorized use of your credit card resulted through no fault of your own from purchases made from Barnes & Noble.com while using our secure server.") visited on 3 Mar 2005

circumstances."[646]For sites with complex data activities — even sites with no intention to sell or trade data to third parties — it will be difficult to promise to make no data transfers whatsoever. The reason is that simple corporate efficiency may require outsourcing various data related activities necessary to a firm's own internal usage of the data. Some firms are making a serious effort to protect the integrity of user data despite these third party transfers. Wal-Mart, for example, promises to only transfer data for specific purposes and then under contract[647]. This achieves a similar function to a complete prohibition on data transfers. Hallmark.com treats information in the site's Address book as highly confidential and states that the information will not be disclosed to third parties[648].

### 4.13 Digital Rights Management (DRM) and Privacy

Digital Rights Management refers to the technologies and processes that are applied to digital content to describe and identify it and to apply and enforce usage rules in a secure manner. The primary purpose of DRM is to control the access, use, distribution and disclosure of digital content online and thereby protect the interests of copyright holders in the online environment. Digital Rights Management systems are also referred to as Electronic Rights Management Systems (ERMS), Rights Management Information Systems (RMIs) and Copyright Management Systems (CMS).

The impetus for DRM is to be found in increases in telecommunications bandwidth, especially to the home, and the concomitant increases in digital file transfer and copying over the internet. Abetting the affects of bandwidth are advances in compression algorithms which improve transmission times and facilitate the storage of high-fidelity content. Duplication of content has thus become easy, cheap, and

---

[646] Walmart.com Security & Privacy, available *at* http://www.walmart.com/cservice/ca_securityprivacy.gsp, visited on 25 Mar 2005

[647] ibid

[648] Hallmark.com Privacy Policy, available at http://www.hallmark.com , visited on 22 Mar 2005

perfect. Acquisition of duplicated content has become nearly instantaneous, and free. No wonder copyright holders are looking for ways to protect their franchise. Content creation is typically expensive; its reproduction in the digital environment is not. At the same time, digital technology has presented an unprecedented opportunity to engage in communication and creative speech. Indeed the very characteristics leading copyright holders to the shoals of piracy suggest the possibility of a paradise of practically cost free delivery of content. This "paradise" is profoundly threatening to existing business models. More germane is the balancing act between internet threat and promise that DRM policy must perform. The delivery and consumption of digital content depends on satisfaction of both copyright holders and end users. Each has different concerns, ranging from piracy to privacy. Copyright policy can ignore neither[649].

In order to manage and protect the interest of the copyright holders, it is essential to have adequate identification and description pertaining to content available (i.e., metadata). Such "metadata" needs, however, to be persistently associated with the content itself so that various applications including anti-piracy services can have access to the metadata. In the analog world such association between content and its metadata can be achieved by printing an identifier onto the data carrier containing the content (e.g., by printing a bar code onto a CD cover or an ISBN onto one page in a book). This approach fails in the digital world, however, because there are no physical carriers to carry the identifiers. Hence a technology is needed that allows obtaining the metadata from looking at the content itself[650].

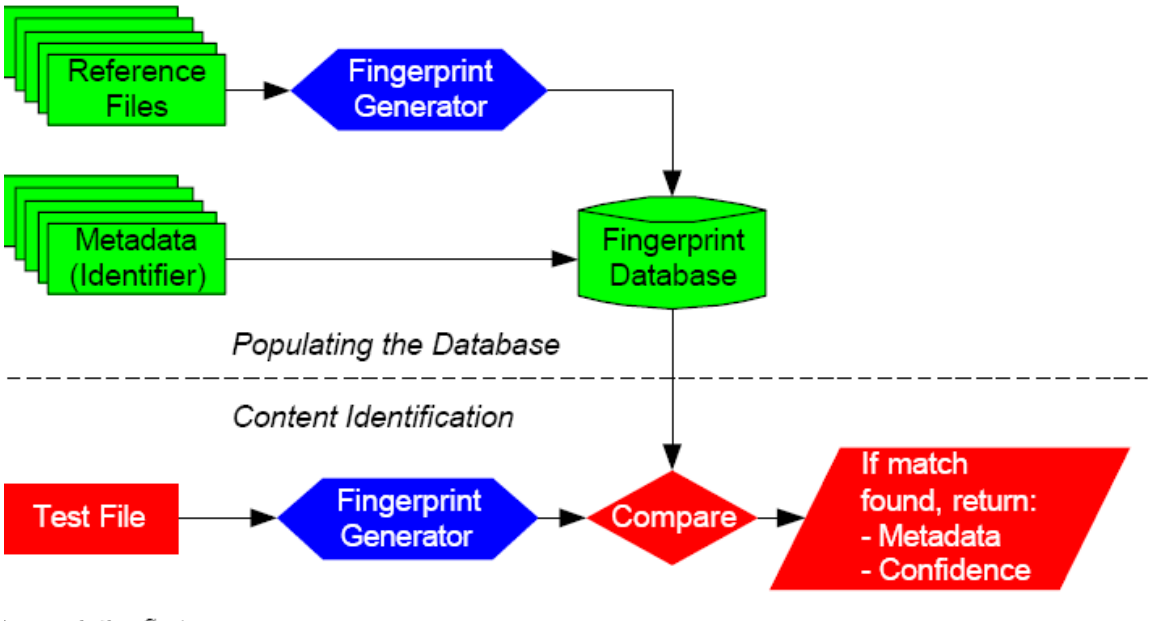
Some of the technologies used for Digital Rights Management are;

(1) **Fingerprinting**: Fingerprinting technologies can be used to identify content by the process depicted in the diagram below. Fingerprinting, or "content-based

[649] Owens, Richards and Akalu Rajen, Legal Policy and Digital Rights Management, available at http://www.cippic.ca/en/faqs-resources/digital-rights-management , visited on 4 Dec 2005

[650] WIPO, Standing Committee On Copyright And Related Rights, Tenth Session Geneva, November 3 To 5, 2003, available at www.wipo.org , visited on 4 Dec 2005

identification technologies" function by extracting the characteristics of a file and storing them in a database. When the technology is presented with an unknown file, the characteristics of that file are calculated and matched against those stored in the database, in an attempt to find a match. If a match is found, the system will return the appropriate metadata from the fingerprint database[651].



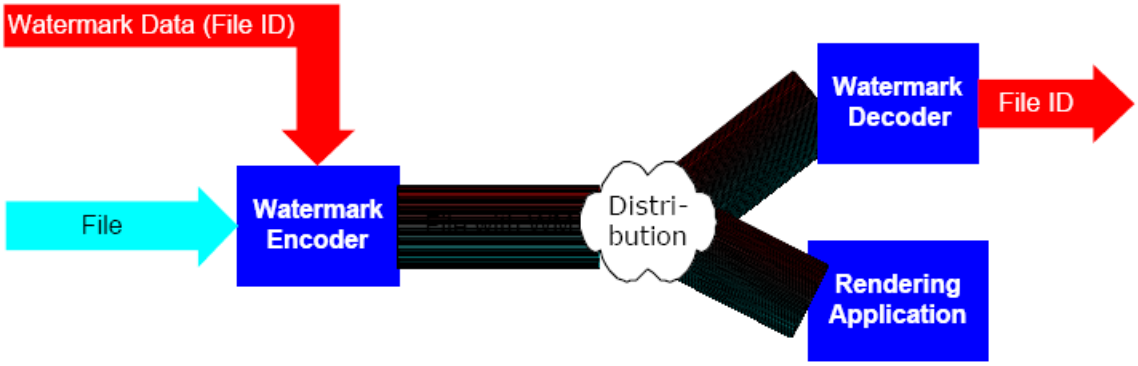

**Source**: WIPO, Standing Committee on Copyright and Related Rights, 10th Session, Geneva November, 3 to 5, 2003 document no. SCCR10/2

Fingerprints, while highly effective with certain content types, are less equipped to aid the unique identification of other content types, depending on the "detail" they provide.

Hence fingerprints are suitable for audio, video and audio-visual content as well as photographs but less for computer graphics or text.

[651] WIPO, Standing Committee On Copyright And Related Rights, Tenth Session Geneva, November 3 To 5, 2003

(2) **Watermarking:** Watermarking is also often cited when discussing copyright protection technologies. A watermark is "(imperceptibly) embedded information." This information (often a file or IP identifier) can, though imperceptible[18] to normal consumers be extracted by special software. This "watermarking detector" can, when applied to content that is suspected to be pirated, check if the content bears the watermark and thereby prove or disprove the suspicion. Typically, all files that are to be distributed are watermarked before they are allowed into the content chain[652]. A functional flow diagram of this is shown in the diagram below.




**Source**: WIPO, Standing Committee on Copyright and Related Rights, 10th Session, Geneva November, 3 to 5, 2003 document no. SCCR10/2

Similar to fingerprinting, watermarks cannot be used with all content types. Small graphic elements such as logos or text are not able to carry watermarks because of a general limitation on the amount of data that can be embedded into the content. All watermark systems known today are susceptible to being removed without substantially affecting the quality of the content itself which may lead to the situation that, when a watermarking system has been broken, the originally governed content may become uncontrollable[653].

(3) **Digital Signature**: Digital Signatures akin to hand written signatures can be used to regulate the access to digital content. It is important to see that information

[652] ibid
[653] ibid

associated with content (e.g., IDs and rights expressions) can be trusted. Such functionality can be achieved when the party adding the metadata

(a) digitally signs the metadata and

(b) is known to be authorized to add the metadata.

A digital signature provides information about the origin of a piece of information and knowledge about whether the information has been altered or not and also non-repudiation of transactions[654].

In India under Information Technology Act, 2000 (IT Act) a digital signature can be used to authenticate an electronic record. It Act being technology specific requires asymmetric technology to used for generation of digital signatures.

### 4.13.1 Implications of DRM on Privacy

The future of online privacy is increasingly linked to the future of online copyright enforcement. In their push to control the proliferation of unauthorized copies, copyright owners and their technology partners are building into the technologies of Digital Rights Management (DRM) a range of capabilities that implicate the privacy interests of users.

The potential consequences of DRM for user privacy warrant far greater attention from policymakers and systems designers than they have yet received[655].

DRM initiatives may be viewed as a series of concentric levels of control, each penetrating more deeply into the user's home electronic and computing environment. At the first level, DRM systems impose direct restrictions on what individuals can do in the privacy of their own homes with copies of works they have paid for. At the next level of control, DRM systems report back to the copyright owner on the activities of individual users. Such reporting may occur as part of a pay-per-use arrangement for access to the work or independent of payment terms;

[654] ibid

[655] Choen E Julie, DRM and Privacy, Berkley Law and Technology Journal, Vo.18, 2003, at 45-49

for example, the system might be designed to report attempts to make unauthorized copies or determine which other software programs a user is running in conjunction with the DRM protected program[656].

The capabilities of DRM systems implicate two different types of privacy interests in the circumstances of intellectual consumption. Direct functionality restrictions intrude on the seclusion, or "private space," that long-established social practice reserves to the individual or family, while forcing changes in a set of behaviors within that space[657] . In so doing, they shift the baseline conditions of user autonomy to determine the circumstances of the use and enjoyment of intellectual goods. Information supplied by DRM technologies can be used to build a dossier about the user's informational preferences and patterns of use. This information in turn can be sold to data aggregators or obtained by the government and used for a variety of purposes.

US privacy laws protecting computers and electronic communications also are unhelpful in the context of DRM. The RealNetworks and Netscape products are now the subject of class actions alleging, respectively, violations of the Computer Fraud and Abuse Act (CFAA) and the Electronic Communications Privacy Act (ECPA). However, neither statute was designed to address this sort of overreaching. The CFAA prohibits only unauthorized access to computer systems, or access that exceeds the scope of authority. The ECPA's prohibitions against interception of electronic communications do not extend to interception that is consensual or that is undertaken by one of the parties to the communication. Thus, it is difficult to see how either statute would prohibit implementation of DRM functions that have been disclosed and purportedly agreed upon.

The questions that law and policymakers must confront, then, are whether the privacy invasions caused by DRM restrictions should be legally cognizable and, if

[656] Cohen J, Copyright and Jurisprudence of self-help, Bekely Law and Technology Journal, vol.13,1998, at 1089-1143

[657] Burk D and Cohen J, Fair Use infrastructure for rights management systems, Harvard Law and Technology Journal, vol.15, 2001, at p 41-83

so, whether they may legitimately be imposed under contract[658], regardless of their invasiveness. There are good reasons to conclude that the scope of privacy in intellectual consumption is a matter of considerable public policy importance and that the law should provide at least some inalienable privacy protection for users of intellectual goods.

If we look at the provisions of Digital Millennium Copyright Act (DMCA), DRM seems to affect the fair use practices. Circumvention of digital content amounts to offence under DMCA. DRM technologies give more protection to copyright holders. Because of this, copyright holders can now determine whether their work should be allowed for fair use practices. This obviously tilts the balance of copyright protection in favour of copyright holder. Hence traditional copyright balance of copyright law may be disturbed.

### 4.14 Do Consumers really care for Privacy?

Consumer surveys overwhelmingly express concern about Internet Privacy. In a June 2005, report by Jupiter Research , 70% of online consumers said they were worried about online privacy. In another survey 93% of e-commerce users said it was very important that sites discloses their privacy practices. But what do these surveys really prove? Consumers may tell survey takers they fear for their privacy, but their behavoiur belies it. People don't read privacy policies, for example. In a survey taken last year (2004) by the Privacy leadership Initiative, a group of corporate and trade association executives, only 3% of consumers read privacy policies carefully, and 64% only glanced at or never read privacy policies[659].

---

[658] Copyright owners and other information providers argue that this baseline distribution of rights and limitations may be altered by contract, or "license," the terms of which users are free to accept or reject. If this is right, then there is no reason the range of enforceable contractual restrictions could not include restrictions that diminish user privacy. But such a position is far too simplistic. See generally, Julie E.Choen, DRM and Privacy, Communications of the ACM, April 2003/Vo.46 N0.4

[659] Goldman , Eric, The Privacy Hoax, Forbes, 10/14/2002, vol.170 Issue 8, P42

Most of the online marketers know, people will 'sell' their personal data incredibly cheaply. As internet Pundit Esther Dyson has said[660] : "You do a survey, and consumers say they are very concerned about their privacy. Then you offer them a discount on a book, and they will tell you everything." Indeed, a recent Jupiter report said that 82% of the respondents would give personal information to new shopping sites to enter a $100 sweepstakes[661].

### 4.15 Conclusion

Technology has again brought us to a critical juncture. We must now look at what technology has made possible, rather than simply at the legal principles that underlie these advances. We tend to misapply legal metaphors due to a lack of conceptual understanding of privacy itself, as well as of modern day technology. A number of critical issues must be addressed in order to move technology and society forward in tandem. Understanding the foundational concept of privacy is paramount in such a paradigm shift[662].

Technology is merely another variable to add to the equation, and should not be viewed as an insurmountable stumbling block. Just as Warren and Brandeis advocated change in the paradigm surrounding privacy in their 1890 law journal article, today we should also reassess "our metaphors, customs, and rules" to account for that which can intrude on our basic right to be let alone and not intruded upon. And, in this day in digital age, our right to have our personal data kept private must be ensured. We must accomplish this from a paradigm that has already been developed, by revisiting the conceptual foundations of privacy in light of cyberspace[663].

---

[660] ibid
[661] Sweepstakes (called prize draws in Great Britain) promotion where prizes are given away for free. They are different from a lottery or contest by requiring no purchase to enter.
[662] Robert A. Reilly, *Conceptual Foundations of Privacy: Looking Backward Before Stepping Forward*, 6 RICH. J.L. & TECH. 6 (Fall 1999) , available at http://www.richmond.edu/jolt/v6i2/article1.html, visited on 23 Sep 2005
[663] ibid

To resolve privacy issues, we must first ask what kind of human interaction we want to develop on the information highway. In other words, whether the values of individual autonomy, cultural inclusiveness and knowledge sharing will determine the environment of electronic communications, or whether the building of the information highway will be driven by the market needs of large vested interests. Privacy rights must reflect the assumptions we as a society make about personal autonomy and the need to control our own lives. Only when this debate is open to all who will likely to be affected by the changing technology, will governments be able to formulate the appropriate rules for Cyberspace.

Even though consumers let out their personal data easily, it still remains the responsibility of the State concerned to protect the interests of its netizens. Beyond the shortcomings of statutory law, courts have failed to enforce promises made by companies that collect data in cyberspace.

European model of data protection seems to be the appropriate model for Indian conditions for the protection of privacy over cyberspace. Taking a clue from developed countries in protecting netizens privacy, Indian Parliament must take steps to enact a legislation to protect the privacy of netizens.