# UNIT 12 PRIVACY POLICY

**Structure**



## 12.1 INTRODUCTION

Privacy is a fundamental human right and a cornerstone of a democratic society. It lies at the foundation of the rule of law, the secret ballot, doctor-patient confidentiality, lawyer-client privilege, the notion of private property, and the value our society places on the autonomy of the individual[1].

The concept of information privacy is distinct from other aspects of privacy such as physical intrusion and surveillance. Information privacy means the claim of individuals to determine for themselves when, how and to what extent information about them is or may be communicated to others. It may also be defined as the individual's ability to control the circulation of information relating to him or her. Many people are unaware that when they go online, they leave an electronic record of their movements and unwittingly provide personal information to people and organizations that track such data.

Globalisation and the growth of electronic technologies have challenged the ability of states to ensure the privacy rights of their citizens. Many countries concerned about the protection of their citizen's personal information have adopted privacy laws and fair information practices. Information privacy initially emerged as a value that could not be taken or misused by government without due process of law. This concept was later developed into a set of best practice principles, both in the US and in the European

Union for ensuring fair processing, minimal intrusion and limited purposes in respect of the use of personal data.

Information privacy was most profoundly affected by the rapid developments in information technology such as the increased use of computers and the setting up of national databanks wherein the choice of the individual is seen as central to the concept of privacy both in allowing physical intrusion and the sharing of information. It is almost ironic that privacy is being threatened over Internet, as initially, Internet was perceived as a technology that would afford its users a considerable level of anonymity and also provide a forum which would encourage and foster freedom of individual expression.

## 12.2 OBJECTIVES

After studying this unit, you should be able to:

- appreciate the judicial trends in India relating to information privacy;
- know the distinction between privacy in tort law and contract law;
- familiarize yourself with the concepts of information privacy in e-commerce;
- appreciate that information privacy is most greatly affected by rapid developments in information technology; and
- know the three types of legal approaches to information privacy.

## 12.3 INFORMATION PRIVACY – LEGAL APPROACHES TO ITS PROTECTION

There are various different legal approaches concerned with the protection of information privacy such as the Nordic, Civil and Common law approaches. The Nordic approach for instance is defined as a combination of legal remedy available to the individual through rights of access and the administrative regulation of computerised records. This approach pioneered information legislation.

The Civil law approach differs from the Nordic approach in as much as it relies upon statements of general principle. Its clear influence has been seen on two significant doctrines in the development of privacy law namely, the US Constitution to protect certain types of behaviour including a right to privacy from government surveillance into an area where a person had a 'reasonable expectation of privacy and matters relating to marriage, procreation, child-rearing and education. The second significant doctrine was developed through the European Convention of Human Rights (ECHR), a codification of international human rights law.

The Common law approach seeks to apply privacy protection principles through the medium of individual cases. In the UK for instance, the emphasis had been on particular legal remedies against particular infringements. Judges often developed such rights without reference to Parliament. However, following the implementation of the first Data Protection Act in 1984, this trend has been somewhat eclipsed, with the UK establishing a supervisory body to police the legislation.

Please answer the following Self Assessment Question.

**Self Assessment Question 1** *Spend 3 Min.*

What are the three main legal approaches to protection of information privacy?

.....

.....

.....

.....

.....

.....

## 12.3.1 Indian Scenario

In the Indian context, the rapidly growing services sector has resulted in both Indian and trans-national corporate entities building up vast, exhaustive and detailed customer databases with a view to providing personalised services such as insurance, personal banking, credit cards etc. These databases contain confidential personal information and may be used by corporates for their own purposes or for that of their affiliates. Also, these databases form a valuable corporate asset, which finds many takers in the market for individual information.

In this regard, any use, disclosure and retention of such information need to be strictly regulated, through an established privacy enforcement regime. Any prospective Indian privacy law would need to incorporate several facets of the above model, which, comprehensively deals with the collection, and use of personal information. With the emergence of an increasingly uniform set of norms governing commercial legal issues across the globe, it becomes imperative for Indian law makers and the legislature to take note of the void that prevails in the critical area of individual privacy protection.

## 12.3.2 Judicial Trends in India Relating to the Concept of Individual Privacy

In the Indian context, although there is no statutory enactment expressly guaranteeing a general right of privacy to individuals in India, elements of this right, as traditionally contained in the common law and in criminal law, are recognised by Indian courts. These include the principles of nuisance, trespass, harassment, defamation, malicious falsehood and breach of confidence. In addition, several pieces of discrete legislation also recognise this right: for example, the Children Act 1960, which prohibits the publication of names and other particulars of children involved in proceedings under the Act; the Hindu Marriage Act 1955, which imposes similar restrictions on the publication of reports concerning proceedings of matrimonial disputes; and the Copyright Act 1957, which prohibits the unauthorized publication of certain documents, photographs, etc. The Code of Criminal Procedure, 1973, also permits restrictions to be imposed on the publication of reports concerning certain legal proceedings, e.g. rape trials.

Under the Indian Constitution, Article 21 of the Indian Constitution is a fairly innocuous provision in itself i.e. "No person shall be deprived of his life or personal liberty except according to procedure established by law". However, the above provision has been deemed to include within it's ambit, inter-alia, the Right to Privacy — "The Right to be left alone".

Please answer the following Self Assessment Question.

**Self Assessment Question 2** *Spend 2 Min.*

Which provision of the Indian Constitution seeks to protect information privacy?

.....

.....

.....

.....

.....

.....

## 12.3.3 Privacy in Tort Law

The Right to Privacy is further encompassed in the field of Torts. The tort of Defamation involves the right of every person to have his reputation preserved inviolate. It protects an individual's estimation in the view of the society and its defenses are 'truth' and 'privilege', which protect the competing right of freedom of speech. Essentially, under the law of torts, defamation involves a balance of competing interests. The only concession for an action, which involves infringement of right to privacy, would be for reasons of, prevention of crime, disorder, or protection of health and morals or protection of rights and freedom of others.

## 12.3.4 Privacy under Contract Law

There exist certain other means by which parties may agree to regulate the collating and use of personal information gathered, viz. by means of a "privacy clause" or through a "confidentiality clause". Accordingly, parties to a contract may agree to the use or disclosure of an individual's personal information, with the due permission and consent of the individual, in an agreed manner and/or for agreed purposes. Under Indian laws, the governing legislation for contractual terms and agreements is the Indian Contract Act. Therefore, in a contract which includes a "confidentiality clause" i.e. where an organization/company agrees to maintain the confidentiality of information relating to an individual, any unauthorized disclosure of information, against the express terms of the agreement would amount to a breach of contract inviting an action for damages as a consequence of any default in observance of the terms of the contract[6].

For example, in the case of an insurance contract, globally, contracts of Insurance are contracts of "Utmost good faith" (Uberrimae Fidei) and the contract is voidable where all material facts are not disclosed. However, the duty of utmost good faith is reciprocal and the insurance company has a corresponding duty to disclose clearly the terms of its offer and duly abide by them. Therefore an insurance proposal, which contains a confidentiality clause regarding personal information provided by the customer, cannot be disclosed without his prior consent. Any breach of such term would invite an action for breach of contractual terms by the insurer-customer.

In regard to a customer-insurance company relationship, an insurance company may, solicit personal information about an individual wherein details could be sought, relating to an individual's family, cultural background, ethnic origin, caste, childhood, education, medical history, information regarding one's immediate family, their age, profession etc. or, in case of data processing companies, there may be queries with regard to an

individuals' professional pursuits, income, investment decisions, preferences, spending patterns and so on. Despite an express authorization from their customers, with regard to sharing of personal information by corporate entities, there may still be instances where disclosure of certain sensitive and embarrassing information could invite legal action from an individual, claiming that the actions of a company which made an unauthorized disclosure resulted in causing such mental agony, anguish, and social stigma, which he would not have otherwise had to bear or face.[2]

### 12.3.5 EU Privacy Directive

The EU privacy directive is an important foundation for workplace privacy in Europe. The directive applies to the processing of personal data wholly or in part by automatic means. It establishes common rules for the EU to encourage freer flow of personal data within the union, thus furthering a unified European market and protecting citizens right to privacy.

The privacy directive applies to the processing of "personal data", defined as information relating to an identified or identifiable natural person. An identifiable person is "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".[3]

The issue of maintaining privacy and consequent protection of such confidential information of an individual was first set out under the Organization for Economic Cooperation and Development (OECD) Guidelines. The guidelines concentrated on the issue of safe and sound exchange of data travelling from one country to another, since has become very important as more and more businesses rely on e-commerce. This Directive was an important initiative to protect personal information by prohibiting the transfer of such personal data to those countries, which did not conform to the privacy protection requirements of the EU. However to promote e-commerce to and from the EU it was essential that the gap in privacy protection norms be bridged. Keeping this goal in mind the U.S. Department of Commerce and the European Commission conferred at length and evolved a "safe harbor" structure. This "safe harbor" structure was accepted and approved by the EU in 2000. This safe harbor structure was based on certain principles wherein the individual sharing personal information was to be duly notified and given a choice whether such information was to be shared or not with third parties. He was also to be informed about further transfer of such information and who would access the same and for what purpose. Adequate protection measures were put into place for securing the information and the accuracy of the information was also to be maintained. Finally a regulatory infrastructure was to be provided to address any transgressions and violations of privacy.

Please answer the following Self Assessment Question.

**Self Assessment Question 3** *Spend 3 Min.*

What is the concept of 'personal data' under the EU privacy directive?

.....

.....

.....

.....

.....

## 12.4 INFORMATION PRIVACY IN E-COMMERCE

### 12.4.1 Introduction

Internet is an important medium helping trade and commerce increase throughout the globe. The reason for this is simple, as the Internet promises reduced costs, higher margins, more efficient operations and higher profits, and all of this at a comparatively much higher speed, as it would take in the real world. It is useful to both producers and consumers in developed and developing countries as it helps them overcome the traditional barriers of distance from markets and lack of information about market opportunities. Producers and traders no longer need to maintain physical establishments requiring large capital outlays. Virtual shops and contact points on the Internet may enable storage close to the production site and distribution can be made directly to the consumer. Increased advertising possibilities worldwide may help small and medium industries and businesses in developing countries that traditionally find it difficult to reach the customer abroad. It may also enable such firms to eliminate middlemen while trying to sell their products abroad.

Implicit in the use of this medium for trade and commerce is the enormous amount of data flowing through it and the fact that everyday more data is being generated. A substantial portion of this data is not for public use or viewing. This type of data includes personal information of the individuals residing in any country, confidential and privileged information of the business houses, confidential government information. In this chapter, we look specifically at the legal issues arising out of the privacy accorded to and the privacy that ought to be accorded to the data used and generated for trade and commerce over the internet, commonly known as e-commerce.

Infringing data pertaining to consumers; circulating in the cyberspace has its impact on the trade and commerce. Three specific implications where determines how the consumer privacy concerns impact the sales of goods and services may be listed as follows, first, consumers whose privacy concerns have not been addressed will tend to delay their purchases or even forgo them. Second, some concerned consumers want to use more traditional ways of purchasing. Third, consumers who use the Internet for making purchases have to pay also the privacy costs caused by other consumers' privacy concerns. In other words, to maximize the potential of e-commerce, it seems critical to accurately understand online consumers' concerns for privacy. At the very outset it maybe clarified that 'Consumers' is not to be confused with individuals or households only. It can include governments, companies, societies etc.

Privacy issues have drawn considerable attention in the discipline of law. However, developing countries and many developed countries still lack literature on privacy concerns related to cyberspace. When we talk about dealing with Internet privacy, it implies 'information privacy'. Invasion in the privacy occurs when the information of a consumer is not used for the purpose for which it was procured. This may be in the form of circulation of information without authorization to do the same, to use the information for purposes other than that for which it was obtained, modification of information without knowledge of the consumer etc. Information privacy in e-commerce has three main elements — Consumers, Vendors and Technology. Consumers are individuals who want to buy goods or services who are willing to use the systems of e-commerce. Vendors sell products via the Internet and it is needed for buying online.

Please answer the following Self Assessment Question.

**Self Assessment Question 4** *Spend 3 Min.*

State implications of consumer privacy concerns impacting sales of goods and services?

.....

.....

.....

.....

.....

.....

### 12.4.2 Privacy Concerns

The main privacy concern is that a consumer is prompted to enter personal information like e-mail address, and this information can be packaged into a cookie and sent to the consumer's hard drive, which stores it for later identification.

Four particular issues for consumer privacy concerns maybe summed up as: (1) visits to websites will be tracked secretly, (2) e-mail addresses and other personal information will be captured and used for marketing or other purposes without permission, (3) personal information will be sold to third parties without permission, (4) credit card information will be stolen.[4]

## 12.5 DATA PROTECTION AND EMPLOYEE'S PRIVACY

The Information age has radically altered the traditional legal and organizational framework of work by blurring the once clear boundaries between an employee's personal and professional lives. Employee's experience increased autonomy and flexibility both at work and at home with the increase in telecommuting and "mobile" working. These advances are aptly facilitated by appropriate information systems and tools supplied by employers. However, these same systems and tools facilitate the intrusion of professional life into personal sphere, and sometimes the intrusion of the employer into the private lives of its employees.

Workers of the world are exposed to many types of privacy-invasive monitoring while earning a living. These include drug testing, closed-circuit video monitoring, Internet monitoring and filtering, e-mail monitoring, instant message monitoring, phone monitoring, location monitoring, personality and psychological testing, and keystroke logging. Employers do have an interest in monitoring in order to address security risks, sexual harassment, and to ensure the acceptable performance of employees. However, these activities may diminish employee morale and dignity, and significantly erode employee's privacy rights.[5]

The term electronic monitoring encompasses three different concepts. First, it includes an employer's use of electronic devices to review and evaluate the performance of employee. For example, an employer may use a computer to retrieve and review an employee's mail messages sent to and from customers in order to evaluate the employee's performance as a customer service representative. Second, it includes

"electronic surveillance" in the form of an employer's use of an electronic device to observe the action of the employees, while employees are not directly performing the work task, or for a reason other than to measure their work performance. For example, an employer may electronically review an employee's e-mail messages as part of an investigation of a sexual harassment complaint. Electronic surveillance by an employer also includes compliance with a government search warrant seeking an employee's voice mail or e-mail communications on the employer's system. Third, electronic monitoring includes an employer's use of computer forensics, the recovery and reconstruction of electronic data after deletion, concealment, or attempted destruction of the data. For example, an employer may use specialised software to retrieve e-mail messages related to an investigation of alleged theft of its trade secrets by retrieving e-mail messages sent by an employee to someone outside the company.

Please answer the following Self Assessment Question.

**Self Assessment Question 5** *Spend 3 Min.*

What are the different concepts that form electronic monitoring?

.....

.....

.....

.....

.....

.....

Advancing technologies enhance employer capability to monitor employee use of computer networks and the Internet within the workplace. Software enables employers to secretly, and in real time, monitors employees' use of networked computers including individual monitoring of each connected computer. Software enables employers to capture the images from an employee's computer screen at random intervals and then compress those images to provide documentation of all computer work. Software may also reveal the online activities off all employee's, including web sites visited, the length of the employee visits, and whether those sites are productive or unproductive. Software enables employers to monitor employees use of chat rooms, programs run, games played, files used, bytes transferred or downloaded, time spent downloading, and e-mail sent or received.

These electronic monitoring practices have significantly eroded employee privacy rights. However employers assert there are many good business reasons to electronically monitor employees in the workplace, including (a) to monitor employee productivity in the workplace (b) to maximize productive use of the employer's computer system when employees use computers on job (c) to monitor employee compliance with employer workplace policies related to use of its computer systems, e-mail systems, and internet access (d) to investigate complaints of employees misconduct, including harassment and discrimination complaints.(e) to prevent or detect industrial espionage, such as theft of trade secrets and other proprietary information, copyright infringement, patent infringement, or trademark infringement by employees and third parties.[6]

The privacy directive has a direct and immediate effect on the human resource operations of employers. Many employment records involve processing personal data covered by

the Directive, including application forms and work references; payroll and tax information; social benefits information; sickness records; annual leave records; unpaid leave/special leave records; annual appraisal/assessment records; records relating to promotions, transfers, training, and disciplinary matters; and records related to workplace accidents. Such data can be very sensitive, as can be the manner in which it is processed by the employer.

In the United States and many third-world countries, workers have very few privacy protections in law. There are few situations where an employee has a due process right to access, inspect, or challenge information collected or held by the employer. There are patchworks of state and federal laws that grant employees limited rights. For instance, under federal law, private-sector employees cannot be required to submit to a polygraph examination. However, there are no general protections of workplace privacy except where an employer acts tortuously — where the employer violates the employee's reasonable expectation of privacy.

European employers are bound by comprehensive data protection acts that limit and regulate the collection of personal information on workers. These laws specifically call for purpose and collection limitations, accuracy of data, limits on retention of data, security, and protections against the transfer of data to countries with weaker protections. These protections place employees on a more equal footing while allowing employers to monitor for legitimate reasons.

In 1996, the International Labour Organization (ILO) adopted a code of practice on the protection of workers' personal data. The ILO code is regarded as the standard among privacy advocates for protection of workers' privacy rights. The code specifies that workers' data should be collected and used consistently with Fair Information Practices (FIPs).[7]

Pursuant to the privacy directive, employees have a number of rights with respect to collection of their personal information by employers, including the rights to be informed generally about information collection practices; to access and correct personal information held by the employer; and, in some cases, to actually withhold consent to the collection and processing of data by the employer. If an employee believes his or her rights are being violated, he or she may appeal to the appropriate supervisory authority for relief, or may seek damages in a judicial proceeding. Under the privacy directive, employers are liable for monetary compensation to employees whose privacy rights are violated. They are also liable for any additional sanctions under relevant national data protection law.

Please answer the following Self Assessment Question.

**Self Assessment Question 6** *Spend 3 Min.*

What are few rights available to employees under the privacy directive?

.....

.....

.....

.....

.....

.....

## 12.6 REQUIREMENT OF A PRIVACY STATUTE

### 12.6.1 Need for a Privacy Statute

There exists in India an impending need to frame a model statute which safeguards the Right to Privacy of an individual, especially given the emergence of customer-service corporate entities which gather extensive personal information relating to it's customers. It's evident that despite the presence of adequate non-mandatory, ethical arguments and precedents established by the Supreme Court of India; in the absence of an explicit privacy statute, the right to privacy remains a de facto right, enforced through a circuitous mode of reasoning and derived from an expansive interpretation of either Constitutional law or Tort law.

The urgency for such a statute is augmented by the absence of any existing regulation which monitors the handling of customer information databases, or safeguards the Right to Privacy of individuals who have disclosed personal information under specific customer contracts viz. contracts of insurance, credit card companies or the like. The need for a globally compatible Indian privacy law cannot be understated, given that trans-national businesses in the services sector, find it strategically advantageous to position their establishments in India and across Asia. For instance, India is set to emerge as a global hub for the setting up and operation of call centers, which serve clients across the world. Extensive databases have already been collated by such corporates, and the consequences of their unregulated operations could lead to a no-win situation for customers in India who are not protected by any privacy statute, which sufficiently guards their interests. Even within the present liberal global regulatory paradigm, most governments would be uncomfortable with a legal regime, which furthers commercial interests at the cost of domestic concerns.

Issues that would need to be addressed by any prospective privacy legislation in India are:

(i) *Limited Purpose*: The particular purpose for gathering information by an organization must be specified at or before the time the information is collected.

(ii) *Safeguards*: In the case of insurance companies or other customer service-related or data processing companies, the gathering and collation of personal information on individuals would need to be conserved and secured by a regulated data security system.

(iii) *Accountability*: Corporates would need to establish a system whereby all information disclosure systems are duly audited/accounted and monitored, keeping in view the rationale/occasion for every disclosure made.

(iv) *Prior Consent*: Corporates could include express clauses in their agreements, which include an express authorization from the individual allowing the companies to use/disclose personal information for it's own internal purposes or that of it's affiliates or group companies.

(v) *Limits to Use, Disclosure and Retention*: Any information sharing with other members of the insurance industry or with other corporate entities should be made only after seeking an express authorization from the customer.

(vi) *Information-Sharing*: The confidentiality and sensitivity of such information makes it necessary for corporates to avoid any data sharing arrangement or customer information disclosure agreements without the prior consent of the individuals.[8]

Please answer the following Self Assessment Question.

**Self Assessment Question 7** *Spend 3 Min.*

Name some of the issues that privacy legislation in India would require to address?

.....

.....

.....

.....

.....

.....

Let us now summarize the points covered in this unit.

## 12.7 SUMMARY

- Information Privacy is distinct from other aspects of privacy. It is the claim of individuals to determine when, how and to what extent information may be communicated to others.
- There are three broad legal approaches to information privacy — Nordic, Civil and Common.
- India has no statutory enactment guaranteeing a right of privacy but elements in relation thereto are recognised by Indian Courts. The Indian Constitution also provides for this right under Article 21.
- The Right to privacy is further present in the law of torts and law of contract.
- The EU privacy directive provides the foundation for workplace privacy in Europe establishing common rules to encourage free flow of personal data.
- Consumer privacy concerns impact sales of goods and services in e-commerce.
- Issues of consumer privacy concerns include tracking of visits to websites, capture of e-mail addresses, sales of personal information to third parties and credit card information risks.
- Employee's privacy is threatened by many types of privacy invasive monitoring.
- Electronic monitoring practices have eroded employee privacy rights; however employers assert good business reasons.
- India requires a privacy statute to address numerous issues of concern.

## 12.8 TERMINAL QUESTIONS

1. What do you understand by 'Information Privacy'?
2. Capturing the position in the Indian scenario, elaborate the legal approach in respect of protection of information privacy.
3. Explain how information privacy and e-commerce are two sides of the same coin.
4. How are employers responsible to a large extent in diminishing the morale and dignity of employees? Comment.
5. Is there an imminent need to frame a statute in India which would safeguard the Privacy Right of an individual?

## 12.9 ANSWERS AND HINTS

### Self Assessment Questions

1. The three main legal approaches are the Nordic, Civil and Common law approaches. The Nordic approach consists of legal remedy through rights of access and administrative regulation of computerised records. The Civil approach relies on statements of general principle while the common law approach seeks to apply privacy protection principles through individual cases.
2. Article 29 of the Indian Constitution has been deemed to include the right to privacy, the right to be left alone.
3. Under the EU privacy directive, "personal data" is defined as information related to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identity number or more factors specific to his identity.
4. Three specific implications are (a) consumers whose privacy concerns have not been addressed will tend to delay or forgo their purchases (b) some may wish to use more traditional ways of purchasing (c) consumers who use the intent have to pay the privacy costs caused by other consumers' privacy concerns.
5. Three different concepts include electronic monitoring –
   (i) Employer's use of electronic devices to review and evaluate employee's performance.
   (ii) "Electronic Surveillance" to observe the actions of employees while employees are not directly performing work.
   (iii) Employers' use of computer forensics.
6. Some of the rights include the right to be informed about information collection practices: to access and correct personal information, to withhold consent to the collection and processing of data.
7. Some of the issues would be
   (a) Limited purpose
   (b) Safeguards
   (c) Accountability
   (d) Prior consent
   (e) Limits to use, disclosure and retention
   (f) Information sharing

### Terminal Questions

1. Refer to section 12.2 of the unit.
2. Refer to section 12.3 of the unit.
3. Refer to section 12.4 of the unit.
4. Refer to section 12.5 of the unit.
5. Refer to section 12.6 of the unit.

## 12.10 REFERENCES AND SUGGESTED READINGS


1. Media Awareness Network. 10 Feb.2007<www.media-awareness.ca>.
2. "Privacy Laws in India – Big Brother"s Watching You – (and you can [acute accent] do a thing about it!)". Mondaq Business Briefing. Mondaq.com. 27 Mar. 2002. 10 Mar. 2007<http://www.mondaq.com/article.asp?articleid=15723>.
3. Gail Lasprogata, Nancy J. King and Sukanya Pillay. "Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada". Stanford Technology Law Reveiew 4(2004). 11 Mar. 2007<http://stlr.stanford.edu/STLR/Articles/04_STLR_4>.
4. Kaapu, T. "The Concept of Information Privacy in E-Commerce: A Phenomenographical Analysis of Consumers' Views". Proceedings of the 28th Information Systems Research Seminar in Scandinavia, Kristiansand, Norway, 6.8-9.8(2005): 16. Plenary paper. 12 Mar. 2007 <http:/www.hia.no/iris28/files/paper_session.htm>.
5. "Workplace Privacy". Electronic Privacy Information Centre. EPIC.org. 7 Feb. 2007<http:/epic.org/ privacy/workplace/>.
6. Supra n 3.
7. Supra n 5.
8. Supra n 2.