CONSUMER PRIVACY

1 Who is a consumer?

According to the Consumer Protection Act,1986, a consumer is a broad label for any person who buys any goods or services for consideration with the intent of using them for a non-commercial purpose. In the typical sense, when people think of themselves being a consumer, they might think about what they purchase through a physical exchange of money for goods or services, ranging from things as simple as fruit or grain to home appliances to cable television, either in a store or through an online exchange where you enter in your credit card information and receive your purchase. Certain services that consumers use may, by their very nature, put an extraordinary amount of sensitive personal information into the hands of vendors. Typical examples include hospitals, banks and telecommunications.

2 What is Consumer Privacy and how may it be breached?

Consumer privacy is concerned with the manner in which information disclosed by a consumer to a vendor is collected and used. Specific issues include: behavioral advertising, spyware, identity management, and data security/breach, Increasingly, data that is collected from consumers is stored in databanks. This is then used for both legitimate purposes (such as marketing, research etc) and illegitimate extraneous purposes (as when this data is sold in bulk to third parties). Additionally, the privacy of consumers may be compromised by actions of third parties that are facilitated by the negligence of the vendors (as for instance hacking into databases). The following international examples illustrate the kinds of privacy threats that the collection of data from consumers may pose[1].

Example 1) Toysmart – an online company- collected personal information from its users, promising to keep it private. In 2000, Toysmart entered bankruptcy and in an attempt to avoid losing everything tried to sell its database despite its strict privacy policy. This example illustrates how vendors may attempt to monetize the personal information of customers exceeding the terms of the contract entered into with them.

Example 2) In 2006 it was found that AOL's research site had a stored file that contained information collected from more than 600,000 users between March to May of 2006. Though the file did not indicate each user by name, it was eventually found that there was enough information to correlate specific individuals to their user number. The example of AOL's demonstrates the danger of online privacy breaches through either oversight or negligence of the vendor in adopting adequate security measures.

Example 3) Similar to the previous example ChoicePoint – an all-purpose information broker, whose database contains information about nearly every adult American citizen, had its system hacked. The thieves had access to the names, addresses, social security

1 Examples drawn from: Oussayef, Karim. Selective Privacy: Facilitating Market Based Solution to Data Breaches by Standardizing Internet Privacy Policies. 14 B.U Journal Sci & Tech L. 105 2008.

numbers, driver's license numbers, credit reports, and legal judgments of up to 145,000 people.

3 What are the consequences of a privacy violation to the consumer?

At its most innocuous level, the disclosure of one's personal information to those whom one would not ordinarily voluntarily disclose them to could lead to unwanted spamming and marketing. Greater threats include those of blackmail, and the impairment of the individual's ability to buy a home, pursue potential employment opportunities, or gain access to credit.

4 How is consumer privacy protected- internationally[2]?

4.1 Broad guidelines:

4.1.1 The OECD Privacy Guidelines:

Though not a law, the OECD Guidelines drafted in 1980 provide a useful set of 'fair information practices' within which privacy of consumers may be evaluated. Briefly, the 8 principles declared were: 1) Collection limitation principle (there should be limits to the collection of data), 2) data quality principle (data should be accurate and relevant to the purpose collected), 3) purpose specification principle, 4) use limitation principle, 5) security safeguards principle, 6) openness principle (there should be openness about data policies and changes thereof), 7) individual participation principle (enabling the individual to find out if data is being held about him and to obtain a copy of the data and make corrections) and 8) accountability principle.

4.1.2 The EU Data Protection Directive (also known as Directive 95/46/EC*)*

This is a broad directive adopted by the European Union designed to protect the privacy

2 The information in section 5.1 can be found in the American Bar Associations book: International Guide to Privacy

of all personal data of EU citizens collected and used for commercial purposes, specifically as it relates to processing, using, or exchanging such data. The Directive establishes a broad regulatory framework which sets limits on the collection and use of personal data, and requires each Member State to set up an independent national body responsible for the protection of data. The Directive prohibits the transfer of protected personal information outside the EU unless the receiving country applies similar legal protections. The basic guidelines of the Directive are:

Notice: Data subjects must be notified of the: identity of the collector of their personal information, the uses for which the information is being collected, how the data subjects may exercise any available choices regarding the use or disclosure of personal information, where and to whom information may be transferred, and how data subjects may access their personal information.

Consent: "Unambiguous consent" of a data subject is required before any personal information may be processed. Special categories such as race, religion, political of philosophical beliefs, health, union membership, sex life, and criminal history have additional processing requirements.,

Consistency: Controllers and processors may only use information in accordance with the terms of the notice given,

Access: Controllers must give data subjects access to personal information.

Security:Organizations must provide adequate security, using both technical and other means to protect the confidentiality and integrity of the data.

Onward transfer: Personal information may not be transferred to a third party unless that third party has signed a contract with the individual or organization which binds them to use the information consistently with the notice given to the data subjects

Enforcement: Each EU country has established a Data Protection Authority that has the power to investigate complaints, levy fines, initiate criminal actions, and demand changes in businesses information handling practices.

4.2 Specific Sectoral Legislation and privacy policies

(a) The US takes a sectoral approach to protecting consumer privacy. Legislation that

protects consumer privacy includes: Gramm-Leach Bliley Act, Health Insurance Portability and Accountability Act, and the Children's Online Privacy Protection Act. Also, the CAN-SPAM Act bans the sending of commercial electronic messages that contain false information.

The most comprehensive act for the consumer is the Fair Credit Report Act, which was passed in 1970. Enforcement of the Act is vested in the Federal Trade Commission. The FCRA applies to how consumers information is collected and used, and applies to insurance, employment, and other non-credit consumer transactions. Under the FCRA the information that is protected is broadly defined as 1. Consumer Report- any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer' s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumers eligibility for credit, insurance, and employment purposes.

Furthermore the FCRA:

(a) provides the right for consumers to ensure the accuracy of their data.
(b) includes “right to know” provisions to enable consumers to know all information in their files
(c) grants consumer dispute rights
(c) limits disclosure of information
(d) requires opt-out options

5 Consumer Privacy in India

Broadly, there are four potential avenues for the protection of consumer privacy in India.
Firstly, individual organizations may voluntarily commit to protect the information of their clients through “Privacy Policies” These become a component of the contractual commitments between the service providers and customers and are enforced through ordinary civil litigation.
Secondly, certain professions and industries have codes of privacy that they must

statutorily abide by. This is true of such professions as the medical profession and the legal profession in India and the entire banking industry and the telecom industry. Rigorous privacy norms are set for each of these industries by their respective apex governing bodies. Penalties for breach include derecognition and monetary penalties.

Thirdly, consumer privacy may be enforced by the specialized Consumer Dispute Tribunals under the Consumer Protection Act in India.

Lastly, the newly amended Information Technology Act imposes an obligation on anyone controlling data to indemnify against losses caused by the leakage/improper use of that data.

Each of these mechanisms is discussed in some details below:

5.1 Privacy Policies:

Several Indian companies have publicly stated privacy policies that they display on their website. We have profiled the privacy policies of two such companies as a sample.

Airtel: Defines personal information, informs users how their information will be used, describes which third parties will have access to your information, provides the ability to opt-out of commercial SMSs, provides an email address for privacy concerns.

Rediff: Provides email for customer support, states what personal information is collected from you, what information is collected from you by cookies, what information is collected about you and stored, who will collect the information about you, how the information will be used to advertise to you and tailor to your preferences, states the rights that advertisers have to your information, disclaimer of responsibility for any other websites linked to the page, states that the information released in a chat room is considered public information, defines third party usage, defines security measures taken, lays out what choices the consumer has regarding collection and distribution of their information, contains opt-out clauses, defines personal information, defines cookies, explains that consumers have the ability to correct inaccurate information, requires youth consent.

Examples of Indian organizations without a privacy policy on websites: Canara bank,

Andhra Bank, Indian railways, Air-India, BSNL, State Bank of India.

Note: The International Guide to Privacy suggests the following be included in privacy policies: description of the personal information collected by the website and third party, description of how the information is used and list of parties with whom it may be shared, a list of the options available regarding the collection, use, sharing and distribution of the information, a description of how inaccuracies can be corrected, a list of the websites that are linked to the organization's site and a disclaimer that the organization is not responsible for the privacy practices of other sites, a description of how the information is safeguarded (both physically and electronically) against loss, misuse, and alteration, consent for use of personal information.

5.2 Professional/Industrial Regulations

As mentioned above, several professional bodies have privacy guidelines which their members must abide by.

5.2.1 Advocates

Rules of Professional Conduct have been framed under the Advocates Act and establishes a code of conduct to be followed by lawyers in order to protect the confidence, information, and data of a client. It is important to note that the obligation of confidentiality continues even after the client relationship is terminated. The Evidence Act further buttresses the confidentiality of clients by making information passed between lawyer and client subject to a special privilege.

5.2.2 Medical Practitioners

Similarly, in 2002, the Medical Council of India notified the Indian Medical Council (Professional conduct, Etiquette and Ethics) Regulations which contain ethical injunctions backed by disciplinary action in cases of breaches. Several of these relate to privacy, for instance

- Every physician is required to maintain medical records pertaining to indoor patients for a period of 3 years from the date of commencement of the treatment.

- Article 2.2 requires physicians to maintain Confidences concerning individual or domestic life entrusted by patients to a physician. Defects in the disposition or character of patients observed during medical attendance should never be revealed unless their revelation is required by the laws of the State. The rule also requires the physician, controversially to evaluate "whether his duty to society requires him to employ knowledge, obtained through confidence as a physician, to protect a healthy person against a communicable disease to which he is about to be exposed". In such an instance, the rules advice the physician to "act as he would wish another to act toward one of his own family in like circumstances."
- Article 7.14 enjoins the registered medical practitioner not to disclose the secrets of a patient that have been learnt in the exercise of his / her profession except –
    - 1. in a court of law under orders of the Presiding Judge;
    - 2. in circumstances where there is a serious and identified risk to a specific person and / or community; and
    - 3. notifiable diseases.
- Article 7.17 forbids a medical practitioner from publishing photographs or case reports of patients without their permission, in any medical or other journal in a manner by which their identity could be made out. If the identity is not to be disclosed, however, the consent is not needed.

In one of the most important cases to have come up on the issue of privacy, a person sued a hospital for having disclosed his HIV status to his fiancé without his knowledge resulting in their wedding being called off. In *Mr. X vs Hospital Z*, the Supreme Court held that the hospital was not guilty of a violation of privacy since the disclosure was made to protect the public interest. The supreme court while affirming the duty of confidentiality owed to patients, ruled that the right to privacy was not absolute and was "subject to such action as may be lawfully taken for the prevention of crime or disorder or protection of health or morals or protection of rights and freedom of others."

This case raises certain questions which might be worthwhile to consider:

1. Are there other ways in which the situation could have been handled – such as through proper counselling. Furthermore, it is important to establish what the role of a hospital is, and where their primary interest lies in protecting their patient and their patients data, and take into consideration the importance of consent in handling and disclosing personal information.
2. The argument that there is no absolute for privacy raises questions of who is determining the limits for disclosure of the man's HIV status. If his fiancé should be informed of his results, should his workplace , community, church? Do they face the same risks as his fiancé? Who is to be the judge of this risk?

5.2.3 Banking and Telecom Industry

The Banking and Telecom industry each have regulatory authorities which have periodically issued guidelines seeking to protect the privacy of customers. Thus, for instance, RBI's Customer Service statement obliges bankers to maintain secrecy, and not to divulge any information to third parties. Likewise, the TRAI has issued regulations on unsolicited commercial communications and has initiated steps to monitor confidentiality measures taken by telecom operators. More details are provided in the accompanying briefs that exclusively deal with the banking and telecom industries. Consumer Protection Act 1986:

The Consumer Protection Act which was enacted with the objective to provide for better protection of the interests of the consumer has emerged as a major source of relief to those who have suffered violations of their privacy.

In *Rajindre Nagar Post Office vs. Sh Ashok Kriplani* a post master was accused of not delivering a registered letter, opening it, and then returning it in a torn condition. It was determined that the tearing of the letter without delivery to addressee was a grave "deficiency in service" on the part of the appellant. It was ruled that the right of privacy of the respondent was infringed upon by the postman. Under the Consumer Protection Act 1986, compensation of Rs. 1000 was awarded as to the mental agony, harassment, and loss arising from the charge of deficiency in service.

The importance of this case lies in the willingness of the courts to treat breach of privacy as a "deficiency of service".

In January 2007, the Delhi State Consumer Disputes Redressal Commission imposed a fine of Rs. 75 lakh on a group of defendants including Airtel, ICICI and the American Express Bank for making unsolicited calls, messages and telemarketing. Although this decision was reversed on appeal by the Delhi High Court it confirms a trend of Consumer Dispute Redressal Commissions willing to take up cudgels on behalf of consumers for violations of their privacy.

5.3 Information Technology Act 2000 (Amended 2008)

In 2008, the Information Technology Act was amended to include an extremely salutary relief to people when a breach of privacy is occasioned by the leakage of data from computerised databases maintained by corporates. Thus, the newly inserted Section 43A states that if a "body corporate" is possessing, dealing, or handling any "sensitive personal data or information" in a computer resource which it owns, controls, or operates, and is negligent in implementing and maintaining "reasonable security practices and procedures" and thereby causes wrongful loss or wrongful gain to any person, this body corporate will become liable to pay damages as compensation to the affected person.
The Section further stipulates that the Central Government would come up with the reasonable security practices and procedures and would also define what constituted 'personal sensitive information'.

Likewise, the newly introduced Section 72A declares that if "any person including an intermediary" secures access to any personal information about another person while providing services under the terms of lawful contract, and if he, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain, discloses such information without the consent of the person concerned, or in breach of a lawful contract, he is liable to be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

6 Conclusion

In conclusion it is important to consider many elements when looking at an effective protective regime for consumer privacy :

1. Is a comprehensive data protection of a sectoral approach more suited to the needs of India?
2. Does India want to become compliant with international standards for data protection ?
3. How will privacy policies be enforced and how will organizations be held accountable for protection of client privacy under the legislation ?
4. Will consumers be notified if their information is breached? If so – what will be included in the breach notification?
5. How can a legislation ensure that consumers are aware of their privacy rights?
6. How can a privacy legislation address the need for different levels of protection for different types of data?