UNIT 11 DATA PROTECTION POSITION IN INDIA, EU AND US

Structure

11.1 INTRODUCTION

This unit seeks to discuss the data protection regimes across the European Union, the United States and India. It purports to highlight the individual stages of their evolution while drawing out a comparative analysis between the same.

Information, particularly digital information which can be stored, searched and manipulated so easily, is a fundamental economic resource, but also a powerful weapon which, in the wrong hands, can do incalculable damage to individuals. Just as technology does not stand still, data protection rules must also continually evolve if they are to be effective in a world where the collection and exploitation of personal data is becoming forever easier and more convenient.

In the past, the overwhelming amount of effort involved in accessing information held on paper files in a multitude of different locations was a real limitation that hindered the mass collection and processing of personal data. Now, new technologies that enable companies and governments to engage in the mass collection and processing of personal data bring with them new risks.

11.2 OBJECTIVES

After studying this unit, you should be able to:

- describe the data protection scenario in India;
- explain the data protection regime in the EU;
- describe the privacy policy in the United States;
- familiarize yourself with the safe harbour framework between the US and EU; and
- explain the data protection regulation in the UK.

11.3 SCENARIO IN INDIA

There is no separate data protection legislation in our country, the National Task Force on Information Technology and Software Development had submitted an 'Information Technology Action Plan' to the Government in July 1998.

In May 2000, the Information Technology Act of 2000 was passed by the Legislature providing for a comprehensive regulatory environment for e-commerce.

Section 2(1) (o) of the IT Act defines 'data' as a 'representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer'

Section 43 Explanation (ii) defines 'computer database' as 'a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network'.

The IT Act also provides for civil and criminal liabilities for violation of data protection couched in the term 'cyber contravention' as section 43 carries an exhaustive list of penalty for damage to computer, computer system etc. S/s. (b) stipulates that if any person downloads copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium. Section 72 deals with the issue of breach of confidentiality and privacy. It provides that a person who has access to confidential information under the powers conferred on him under the Act and discloses such information can be punished with imprisonment for upto two years or a fine of Rs. 1 lakh or both. The scope of the section is limited as interception of confidential information has been left untouched.

The Indian government is well aware of this issue and in an attempt to overcome the problem; the Indian Department of Information Technology announced in June 2003 its plans to pass a Data Protection Act in line with the EU requirements. A bill is being drafted jointly by the Department of Information Technology and the National Association for Software Service Companies (NASSCOM), which is India's main trade association for the IT industry.

The aim is to allow India to be officially designated by the European Commission as a country that can be assumed to ensure an adequate level of protection. This would clear the path for any data processing operations involving personal data originated in the EU to be carried out by India-established companies, as they would have to meet the same requirements as EU-based companies. However, the procedure to determine whether a third country is safe from a data protection perspective is rather cumbersome and bureaucratic.

EU law in particular restricts businesses transferring data to countries with weak privacy protection, and with Indian IT wage costs rising – albeit still far behind those in the US and Europe – India wants to eliminate reasons for potential customers to outsource elsewhere. European firms are severely restricted in terms of the Data Protection Directive of 1995 as to what data can be transferred or stored in countries without equivalent

rules and enforcement procedures. At present, India has no such regulations, and relies on individual contracts negotiated between the main company and the Indian outsourcing contractor to address the data protection issues.

Please answer the follwoing Self Assessment Question.

Self Assessment Question 1 *Spend 3 Min.*

Which bodies are drafting the bill pertaining to data protection?

.....

.....

.....

.....

.....

.....

11.4 EU DATA PROTECTION DIRECTIVE

In Europe, data protection laws have been in existence in some countries for over twenty years. In an effort to harmonise all of the EU Member States' data protection laws and encourage the enactment of these laws in Member States lacking data protection legislation, the Council of European Union adopted Council Directive of 24 July 1995 on the Protection of Individuals with Regard to the processing of Personal Data and on the Free Movement of Such Data. The Directive took effect in October 1998.

The Directive identifies two main objectives: protection of the right of privacy and prevention of obstacles to the free flow of information within the EU. Article 1(1) states that, "...Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data." Article 1(2) states that, "Member States shall neither restrict nor prohibit the free flow of personal data between Member States".

Under the terms of the Directive, there is an obligation to collect data only for specified and legitimate purposes. The term processing includes collecting, recording, altering, and making data available in any form. Therefore, either the person concerned has the consent for processing, or processing is necessary to carry out a contract to which the person involved is a party, or to carry out pre-contractual measures undertaken at the request of the person. Processing can also occur where it is necessary for compliance with legal obligations. Finally, where the activity involved is an assignment of public interest, processing may be allowed where it does not involve an infringement of fundamental rights and freedoms.

The Directive covers the private and public sectors, but does not apply to data processed for national security, defense, and public security purposes.

Any company from outside the EU that wishes to transfer personal information about an EU citizen outside the EU must either: 1) take the data to a country whose privacy regime is judged to have "adequate" data protection, based on the EU ideals or, 2) the company demonstrates in other ways that its operations meet the EU's Data Protection standards.

Articles 25 and 26 of the Directive clearly state that, as a rule, the receiving third country has to ensure an adequate level of protection. The adequacy of the level of protection shall be assessed in light of all the circumstances surrounding a data transfer operation; particular consideration shall be given to the rules of law in force in the third country in question.

Member States with strong data protection traditions have established powerful governmental agencies to oversee these issues and protect subjects' rights. The agencies require businesses to register, report – and even justify – the kind of personal data they are collecting on employees and customers and how they intend to use it. The EU Directive encourages the establishment of these enforcement agencies in third countries, as well, as a means of providing the "adequate" protection needed to receive data from the EU.

Short of creating a national commission, the European Directive sets out two other ways of satisfying the record safeguard requirements. One is an industry wide code protecting the release of data for a specific sector — such as telecommunications or banking. The other is a system of individual contracts between the company seeking to transfer the data and the data protection commission of the European country.

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 3 Min.*

What are the three steps that a non-EU Company must take in order to transfer personal information about an EU citizen outside the EU?

.....

.....

.....

.....

.....

.....

11.5 PRIVACY POLICY IN THE UNITED STATES

There is no single law in the United States that provides a comprehensive treatment of data protection or privacy issues. In addition to the constitutional interpretations provided by the courts and the international agreements mentioned above, there have been a number of laws and executive orders dealing specifically with the concept of data protection. The most important and broad based of these laws are *the Privacy Act of 1974* and the *Computer Security Act of 1987*.

The *Privacy Act* (PL 93-579) is a companion to and extension of the *Freedom of Information Act (FOIA)* of 1966. *FOIA* was primarily intended to provide access to government information. It did exempt the disclosure of personal and medical files that would constitute "a clearly unwarranted invasion of personal privacy". This provision was initially used to deny access to people requesting their own records. So the *Privacy Act* was also adopted both to protect personal information in federal databases and to provide individuals with certain rights over information contained in those databases. The act has been characterised as "the centerpiece of U.S. privacy law affecting government record-keeping". The act was developed explicitly to address the problems posed by electronic technologies and personal records systems and covers the vast

majority of personal records systems maintained by the federal government. The act set forth some basic principles of "fair information practice," and provided individuals with the right of access to information about themselves and the right to challenge the contents of records. It requires that personal information may only be disclosed with the individual's consent or for purposes announced in advance. The act also requires federal agencies to publish an annual list of systems maintained by the agency that contain personal information.

Matching and Privacy Act. These laws deal exclusively with personal information held by the federal government and do not have any authority over the collection and use of personal information held by other private and public sector entities. This act amended the *Privacy Act* by adding new provisions regulating the use of computer matching. Computer matching is the computerised comparison of information about an individual for the purpose of determining eligibility for Federal benefit programs, or for the purpose of recouping payments or delinquent debts under such programs.

In general, matching programs involving Federal records must be conducted under an agreement between the source and recipient agencies. This agreement describes the purpose and procedures for the matching and establishes protections for the matched records and is reviewed by a Data Integrity Board and each agency involved in matching activities must establish such a board. While the law provides no special access rights to individuals; agencies must notify individuals of any findings based upon a computer matching program before taking any adverse actions, and individuals must be given the opportunity to contest such findings.

Further, the *Computer Security Act of 1987* (PL 100-235) also deals with personal information in federal record systems. It protects the security of sensitive personal information in federal computer systems. The Act establishes governmentwide standards for computer security and assigns responsibility for those standards to the National Institute of Standards. The law also requires federal agencies to identify systems containing sensitive personal information and to develop security plans for those systems.

In the U.S. there is an assortment of federal and state constitutional, statutory, and case law which provide informational privacy protections. Congress has responded to the need for informational privacy and security protections by enacting statutes in a piecemeal fashion to address specific privacy needs. For example, the Privacy Act regulates federal government record-keeping, and there are statutes which regulate specific personal data, such as credit reports, bank records, and videotape rental records. Several bills addressing privacy issues have been introduced in the 105th Congress, but there has been no action on them.

Please answer the following Self Assessment Question.

Self Assessment Question 3 *Spend 3 Min.*

Briefly enumerate the US laws that deal exclusively with information held by the federal government and in federal record systems.

.....

.....

.....

.....

.....

11.5.1 International Safe Harbour Privacy Principles and FTC

There is substantial interest in data privacy issues, on the part of the government, private industry, privacy advocates, and individuals. In 1997 alone, four separate federal government bodies issued lengthy reports on data privacy issues after extensive research. The Federal Trade Commission (FTC) also held a four-day public hearing, in which privacy advocates and representatives of the information industry and of technology companies presented their views on the best means for protecting privacy. Some proposed technological privacy protection measures have been endorsed both by industry groups and by some privacy advocates, but these parties disagree on the most effective means for protecting privacy. In general, the information industry favours the use of self-regulatory measures for data privacy protection, which privacy advocates recognise as valuable components of privacy protection, but insufficient without some sort of enforcement mechanism.

A number of information industry groups have issued voluntary codes of conduct and guidelines for fair information collection by their members. Mandatory codes of conduct have recently been adopted by some industry groups. For example, in December 1997, mandatory guidelines were issued by the Individual Reference Services Group (IRSG Group), which includes companies, such as LEXIS-NEXIS, which sell personal data via their online services; the three credit reporting companies—Equifax, Experian, and Trans Union; and other companies which sell personal information. The IRSG guidelines require that annual compliance audits be conducted by independent third parties, and the guidelines prohibit members that are information suppliers from selling data to those found violating the guidelines.

In July 1997, the Clinton Administration issued *A Framework for Global Electronic Commerce* which generally favors a laissez-faire, market-driven approach to regulating the Internet in an effort to stimulate economic commerce. The Administration indicated that it currently supports the use of self-regulatory codes of conduct by industry along with technological privacy protection measures as the preferred means for privacy protection. The officials of the Administration state that they will look for codes of conduct that are backed up by an enforcement mechanism which might take the form of a dispute resolution mechanism such as an arbitration process included in the code of conduct, or an audit system to verify compliance with codes. The official also suggested that the Federal Trade Commission might have a role in enforcing codes of conduct, for example, by instituting unfair trade practice actions against companies that fraudulently claim to follow a code.

The FTC has announced that it shall institute such actions under the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce. . . ." The FTC is also taking steps toward ensuring that U.S. Web sites follow fair information practices when collecting personal data. In March 1998, the FTC would have conducted a comprehensive survey of U.S. commercial Web sites to determine how many provide privacy statements on their Web sites, and to evaluate the quality of the privacy statements. In evaluating quality, the FTC used factors such as how prominently the privacy statement is posted, and whether Web site visitors can "opt-out" of any aspects of the information collection and handling process. This follows a short survey of 126 child-oriented Web sites which the FTC conducted in October 1997, where the FTC found that most of those sites collect personally identifiable information from children without seeking parental permission and without providing a privacy policy statement. In its report regarding the study, the FTC indicated that it

would notify the owners of the offending sites that their data collection practices may constitute deceptive or unfair practices, in that it is a deceptive practice to misrepresent the purpose for which information is being collected from children, and that it is likely to be an unfair practice to collect the information "and sell or otherwise disclose that information to third parties without providing parents with notice and the opportunity to control the collection and use of the information".

In the U.S., the Federal Trade Commission have enforced Fair Credit Reporting Act (FCRA) provisions and they have unofficially assumed the role of privacy watchdog. However, there should also be an alternate means of redress for aggrieved individuals, such as the private right of action which is provided by the FCRA in addition to the FTC administrative enforcement procedures. This is because the FTC does not act on behalf of individuals but rather takes action against a company or industry when it has received a sufficient number of complaints. Also, whether it is the FTC which is designated as privacy watchdog for the U.S., or it is another existing agency or one created specifically to address privacy concerns, that agency should be given responsibility for government as well as private-sector information handling so that U.S. data protection policy is comprehensive.

Federal laws providing comprehensive information privacy protections would no doubt meet the EU privacy directive's "adequate protection" requirements. A comprehensive law would require that all entities handle personal information in accordance with fair information practices, which includes giving data subjects notice regarding the collection of personal information. A comprehensive law would also provide an enforcement mechanism, which would provide sanctions against violators as well as redress for aggrieved individuals. Although data transfers may be permitted only to government entities covered by the federal privacy acts and to industries, such as the credit industry, which are regulated by legislation. For example, the EU would seem willing to accept a privacy policy based on codes of conduct as long as there is a regulatory body responsible for data privacy matters, which would oversee enforcement of the codes, provide aggrieved individuals with an opportunity for redress of privacy violations, and act as a liaison to the EU.

As a result of these differences in basic philosophy and legal development, US organizations collecting or using personal information about individuals in Europe have been very concerned about the impact of the adequacy standard as applied to types of data they receive from Europe. If such data is found not to be subject to an adequate level of protection once it has been transferred to the US from Europe, the US organizations face the prospect of interruptions in data flows, or enforcement action taken by European data protection officials.

As the world becomes "smaller" and as the EU begins to flex its muscles as an economic and political power, the United States will find itself facing the same message it has sent to other countries in the past — "play our way, or don't play at all". It is time that congress and business realises that, in order to move information out of Europe they are going to have to play the EU way.

Please answer the following Self Assessment Question.

Self Assessment Question 4 *Spend 2 Min.*

In the US which Act provides for private right of action in matters relating to data privacy?

.....

.....

.....

.....

.....

.....

11.5.2 U.S. Safe Harbor Framework

The Safe Harbor Framework negotiated between the U.S. and EU specifies that a company seeking the benefits of the Safe Harbor must be subject to the jurisdiction of a governmental body which is empowered to investigate complaints and to obtain relief against unfair and deceptive practices in case of noncompliance. Currently, the Federal Trade Commission and the Department of Transportation are the only U.S. "governmental bodies" that have been recognised by the European Commission. Therefore, only employers subject to the jurisdiction of these two agencies are eligible to join the Safe Harbor. Financial services institutions subject to the jurisdiction of banking agencies and telecommunications carriers subject to the jurisdiction of the Federal Communications Commission are not eligible to join the Safe Harbor at this time.

An eligible organization must publicly declare in its privacy policy statement that it adheres to the Safe Harbor in order to participate. Further, the employer must also self-certify to the U.S. Department of Commerce ("DOC") that it complies with the principles of the Safe Harbor which apply to both consumer and employee information.

Please answer the following Self Assessment Question.

Self Assessment Question 5 *Spend 2 Min.*

Which are the two bodies of the US recognised by the EU in case of the safe harbor framework?

.....

.....

.....

.....

.....

.....

11.6 UNITED KINGDOM

The first legislation in the UK concerning data protection was the Data Protection Act 1984. This followed the principles of the OECD Guidelines of 1980, and the Council of Europe Convention of 1981. The Act only applied to data stored on a computer.

The Conservative government in the UK was unreceptive to the idea of a Data Protection Directive, arguing that there was no need for one. The UK thus had little influence on the final text of the Directive, agreed after protracted negotiations in 1995. However, the Labour government that was elected in 1997 placed Data Protection on its agenda as a part of its wider concerns for human rights.

The Data Protection Act, implementing Directive 95/46/EC was passed on 16 July 1998. The Act faithfully transposes the provisions of the EC directive into UK law. However much of the detail was left to secondary legislation; 17 Statutory Instruments were needed before commencement. More have been introduced subsequently. The Act eventually entered into force on 1 March 2000. Minor modifications were made under the Freedom of Information Act 2000.

The Act creates new rights of access to information. It is intended to supersede the Code of Practice on Access to Government Information. The Act amends the Data Protection Act 1998 and the Public Records Act 1958.

The Code of Practice on Access to Government Information is a non-statutory scheme which requires Government Departments and other public authorities under the jurisdiction of the Parliamentary Commissioner for Administration to make certain information available to the public and to release information in response to specific requests. The Act creates a statutory right of access, provides for a more extensive scheme for making information publicly available and covers a much wider range of public authorities including: local government, National Health Service bodies, schools and colleges, the police and other public bodies and offices.

The Public Records Act 1958 reorganized the arrangements for the preservation of public records. It places a duty on the Keeper of the Public Record Office to provide reasonable facilities for inspecting and obtaining copies of such records. The statutory rights under the Act and the Information Commissioner's regulatory powers will be extended to information contained in these records.

The Data Protection Act of 1998, like that of 1984, is based on a set of Principles. The Act is designed to protect the interests of the data subject. It is concerned with personal data and the manner in which it is processed. Data users are personally responsible for complying with the provisions of the 1998 Act. It introduces a number of important changes and extends the provisions of the 1984 Act.

The Data Protection Act states that where an organization cannot comply with an access request without disclosing information relating to another individual who can be identified from that information, it is not obliged to comply with the request unless:

- the other individual has consented to the disclosure of the information to the person making the request; or
- it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

Thereby meaning that at least one of these conditions shall be met:

- The data subject must have given his consent to the processing.
- The processing is necessary for the performance of a contract involving the data subject, for other legal reasons, or for "any other functions of a public nature exercised in the public interest".
- The processing is necessary in order to protect the vital interests of the data subject.

From a security standpoint, the Data Protection Act also deals with Sensitive Personal Data, which means information related to such things as racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sexual life and criminal convictions. Therefore, for processing such information, they need to satisfy one of the conditions as mentioned hereinabove.

Please answer the following Self Assessment Question.

Self Assessment Question 6 *Spend 3 Min.*

What is "sensitive personal data" as per the UK Act?

.....

.....

.....

.....

.....

.....

Let us now summarize the points covered in this unit.

11.7 SUMMARY

- The EU Directive has two main objectives (i) protection of right of privacy and (ii) prevention of obstacles to free flow of information within the EU.
- The EU Directives covers both private and public sectors and requires a receiving country to have an adequate level of protection.
- The EU directives sets out an industry wide code protecting release of sector specific data and a system of individual contracts between the transferring entity and the data protection Commission of the EU country.
- There is no single law in the US for data protection. The various acts include the Matching and Privacy Act and the Computer Security Act.
- The FTC enforces data protection administrative enforcement procedures along with the FCRA.
- The UK follows the DPA based on a set of 8 principles. The DPA also deals with sensitive personal data.
- In India, there has been no separate data protection legislation and the Information Technology Act, 2000 regulates issues pertaining to data protection.

11.8 TERMINAL QUESTIONS

1. Briefly explain the EU directive on data protection. Also state whether the EU directive is self sufficient to address all the issues?
2. Explain the US Safe Harbor Framework.
3. Give a comparative analysis between data protection legislation in EU and US.
4. Do you think there is sufficient data protection in India? Compare the position in relation to the US and the UK.

11.9 ANSWERS AND HINTS

Self Assessment Questions

1. The Department of Information Technology and the National Association for Software Service Companies (NASSCOM).
2. It must either (i) take the data to a country whose privacy regime is adjudged to have 'adequate' data protection or (ii) the company demonstrates in other ways that its operations meet the EU standards.
3. The Matching and Privacy Act and the Computer Security Act of 1987 deal with personal information held by the federal government and such information in federal record systems.
4. The Fair Credit Reporting Act (FCRA) provides for alternate means of redress for aggrieved individuals such as the private right of action.
5. The two bodies recognised are the (i) Federal Trade Commission (FTC) and (ii) the Department of Transportation.
6. 'Sensitive Personal Data' means information related to such things as racial or ethnic origin, political opinions, religious beliefs, trade union membership, health sexual life and criminal convictions.

Terminal Questions

1. Refer to section 11.4 of the unit.
2. Refer to section 11.5 of the unit.
3. Refer to sections 11.4 and 11.5 of the unit.
4. Refer to sections 11.3, 11.5 and 11.6 of the unit.