UNIT 15 EVOLVING TRENDS IN DATA PROTECTION AND INFORMATION SECURITY

Structure

15.1 Introduction

15.2 Objectives

15.3 Privacy

15.4 E-governance

15.5 Information Warfare

15.6 Legal Issues with Retention of Electronic Records by the Government and other Private Agencies

15.7 Data Transfer Regime

15.8 Summary

15.9 Terminal Questions

15.10 Answers and Hints

15.11 References and Suggested Readings

15.1 INTRODUCTION

With the coming of age of the Internet and information systems, the legal systems which deal with them, have been forced to evolve rapidly. Though the changes in law have had to deal with a number of issues in the broad area of cyber laws, the most vibrant of those have been concerned with privacy, information security, information warfare, e-governance, e-commerce and crimes on the Internet. The fact that the laws in this regard are presently evolving along with the fact that there are differences in approach between most national legal systems lends to the colourful mosaic that the province of law seems to be bathed in. For example, while in the US, the regime regarding information gathering by websites is more geared towards self-regulation, in Europe, the EU has led the way with a number of quite compulsory policies in this regard.[1]

15.2 OBJECTIVES

After studying this unit, you should be able to:

- explain the issues that have spawned debate in the area of privacy;
- know the meaning and underlying framework requirements in respect of e-governance;
- describe the issues in respect of grave threat to national security of countries on account of information warfare;
- explain the legal issues in respect of retention of electronic records; and
- describe the working in general of data transfer regimes.

15.3 PRIVACY

Two major issues which have spawned considerable debate and even some laws in the area of privacy, especially in the context of growing internet use are unsolicited commercial e-mail and 'cookies' and other technological features that web site operators sometime use to track visitors to their sites or to may be build a profile of the specific Internet user.

In a string of decisions[2], unsolicited e-mail has been deemed to be trespassing to personal property and even permanent injunctions have been issued prohibiting commercial mailers from mailing subscribers of some providers. Here the mailer's first amendment rights to free speech have generally not been allowed as the other party is not the government. The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 though have been quite effective in getting control of this problem. This Act is directed at decreasing the number of spam e-mails[3]. It basically requires mass marketers to provide an opt out provision in their e-mail lists and also fixes liability and also requires them to provide a physical address. This structure is in fact very similar to the do not call lists which exist for telemarketers[4].

However in India, such legislation has not yet been brought into effect. In the news is a case dealing with unsolicited telemarketing has made headlines. Dr. Harsh Pathak Public Interest Litigation (PIL), is seeking a direction to be issued by the Supreme Court to banks and telephone service providers to stop making unsolicited telemarketing calls. On February 7, 2005 the Supreme Court issued notices to the Union of India, which has also been made a party to the suit based on the argument that it is the duty of the state to prevent violation of the rights of citizens and the state so far has failed to do so, and a host of mobile phone service providers and banks, pursuant to the PIL.

As alleged that the defendants currently use mobile communication links to market their services and products by making unsolicited calls or "cold calls" and such unsolicited calls violate the Right to Privacy of the user, the suit also throws up several interesting points of discussion. Do unsolicited calls by themselves violate privacy, since they do not in an unauthorized manner interfere in any personal conversation or disclose personal information to any unauthorized person? Or is the objection based on the sharing of phone numbers, of users, between commercial entities? Would such sharing of phone numbers, and their usage for cold calls, be violative of any privacy related law? Would the Supreme Court read such a prohibition as a measure to safeguard the Right to Life and Liberty of consumers in Article 21? These are questions which will go a long way in determining the right to Privacy on the Internet as well since the principles are the same.

However when the issue turns to cookies and other tracking features of websites, there are very few legislative provisions which govern these in US or in Europe. Rather the focus is on industry self regulation and thus the setting of industry standards and policies. These systems are designed to both preserve the privacy of users and also garner information for webmasters and online marketers for information about current/potential customers. In this regard the Open Profiling Standard (OPS) and World Wide Web Consortium's Platform for Privacy Preferences Project (P3P) were standards which were supposed to give users control over the amount of information that they reveal over the Net. This shows how the information industry can have an important role in the safeguarding of private individual's information on the Internet. The importance of this lies in the speed with which the companies comply with the industry guidelines and

respond to the pressures of the marketplace. Besides newer systems especially those under the Uniform Computer Information Transactions Act (UCITA) talk about licensing of personal information to websites. An advantage of this contractual approach to protecting information privacy is that multiple interests of people can be accommodated and the idea of consent with regard to use of personal data is also satisfied.[5]

As far as the US and Europe are concerned they have basic and in some cases stringent laws which protect the privacy of all individuals in their geographies. These laws lay down the basic principles of protection of privacy and the means and methods to protect them. However as technology evolves, these privacy laws will find it difficult to keep up in pace with the new implications of technology. For example, biometrics has become an area of technological innovation, which is a growing trend, and there are privacy implications of the use of biometrics. "Biometric" means a fingerprint, retina or hand scan of a person which is stored in information systems and this information can be accessed to validate the person for identification purposes. Biometrics is mostly being used by Government Authorities who can access further personal information stored on the information systems to confirm the identity of the person. However this process of validation using biometrics can be undertaken on the street, in airports, schools, banks, swimming pools or office buildings. Therefore this process of validation can be very invasive and the Government and even private entities may be able to maintain huge amounts of information about individuals in their data banks. Effective legislations controlling the use of biometrics will be another trend to watch out for in the coming years.

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 3 Min.*

What are some of the common universal standards pertaining to cookies and other tracking features of websites?

.....

.....

.....

.....

.....

.....

15.4 E-GOVERNANCE

E-governance represents the application of information technology for the improvement of administration. Basically it means that the Government of a country will interact with its citizens wherever possible through the Internet and information systems. Further the Government will use information technology and systems in the day to day running of the various departments ranging from passport and land revenue departments to the judiciary. In order to enable this process of e-governance it is essential to ensure that there is an effective legal framework which guides and nurtures e-governance. While in the US and in Europe there have been sufficient number of guidelines and legislations in this regard, in India this is yet to happen. Therefore one trend of legislations, which we

can expect in the near future, is that relating to e-governance. While the Information Technology Act, 2000 does set the context for e-governance and enables various transactions in the e-governance sphere a lot more needs to be done in this area. An effective legal framework ensures that governments have the opportunity to keep pace with the new era of global communication and efficiently provide citizens with valuable services. This framework should identify and address the various transactions, which happen in the e-governance model such electronic payments, electronic contracting and also disputes which arise during e-transactions. There should also be a regulator similar to the Telecom Regulatory Authority of India to ensure that transactions in the e-governance space are smooth and in accordance with applicable law.

Please answer the followings Self Assessment Question.

Self Assessment Question 2 *Spend 3 Min.*

What should an effective legal framework seek to achieve in the area of E-governance?

.....

.....

.....

.....

.....

.....

15.5 INFORMATION WARFARE

The growing dependence of countries on information systems means that critical infrastructure and even defensive and offensive capabilities of countries depend upon information systems. These information systems are vulnerable to the growing attacks in cyberspace. Computer-based information operations akin to hacking, could provide adversaries of a country with an asymmetric response to that country's military superiority by giving them the potential to cripple critical infrastructure and even defense capabilities of the country[6]. Therefore, it does not matter if the conventional military forces of a country are strong, a small country with negligible military presence can hack into the ballistic missile control systems of the enemy and disable it. Further, it can hack into and cripple the public transport system of its enemy, thereby causing immense loss of life and property without dropping a single bomb on the enemy. The complexity of computer networks is growing faster than the ability to understand and protect them by identifying critical nodes, verifying security, and monitoring activity. Attacks on a country's military, economic, or telecommunications infrastructure can be launched from anywhere in the world. Weapons of "mass effect," such as denial-of-service attacks, are likely to proliferate in the coming decade. Viruses and worms are likely to become more controllable, precise, and predictable—making them more suitable for weaponization[7]. Therefore countries are looking to adopt stronger penalties for hacking and attacks such as denial of service attacks. National governments are also strengthening laws, which oblige companies and organizations handling information systems to protect such information systems. This is especially because most IT systems of critical infrastructure and even some defence installations are outsourced to private companies and therefore

the risk of a compromise is higher in such cases. Growing threat to the national security of countries through information warfare would mean that countries will adopt more stringent laws relating to information security.

15.6 LEGAL ISSUES WITH RETENTION OF ELECTRONIC RECORDS BY THE GOVERNMENT AND OTHER PRIVATE AGENCIES

With more and more electronic records being kept on the net or otherwise, issues of security and privacy have come up to the fore in this regard as electronic data can be easily manipulated. The problems arise with regard to how much information is being recorded, to what purpose it is being recorded and what the security provisions are as regards the prevention of misuse of this information. The consent of the person whose information has been so collected as well as the scope for him/her to change such information which has been collected are also relevant issues.

A very relevant example will be the way in which health information is stored and used according to law especially in light of the fact that health services are the sector in which a lot of outsourcing happens and thus a lot of client information is shared. The Health Insurance Portability and Accountability Act of 1996, called the HIPAA is a part of a new breed of legislations which address privacy and security issues in quite specific fields like electronic healthcare transactions. The HIPAA governs health plans, health care providers who transmit any health information in electronic form in connection with a transaction covered by HIPAA and also health care clearinghouses. The ambit of HIPAA though extends, importantly to outsourcers also, as the Act requires the covered entities to impose HIPAA obligations on entities which are the business associates, who deal with the covered entity and do a function/service which involves the use of individually available health information of the covered entities and which receive health information. The HIPAA provides for two kinds of standards—privacy standards and security standards. The privacy rule prevents the disclosure or use of protected health information (information about health which can be used to identify an individual) unless specifically authorized by the individual or under the law. The security rule is a subset of the former and comes into effect when the protected health information is either transmitted by electronic media or kept in electronic media. The security rule and the privacy rule set a number of procedures which have to be diligently followed by the covered entities when handling confidential information. These standards not only include risk analysis and risk management but assessment systems to be in place. The standards for security rule are similar and tougher compared to those of the privacy rule.The business associates of the entities have these procedures in their contracts thus completing a very careful system as regards confidentiality. Thus HIPAA shows how sector specific laws have been evolving in the light of new practices, which have emerged after the large scale adoption of practices which are based on electronic retention of data and high speed data communication.[8]

Interestingly, governmental records of individuals are a very big problem especially when the security systems of most government networks are suspect and susceptible to hacker attacks. The problem here is that the government acquires a huge amount of personal information about each person in its different departments. To safeguard this information in US, there is the Privacy Act of 1974, 5 U.S.C. § 552a et seq. which

prohibits the disclosure of a record without the consent of the subject of the record. These records can only be used to accomplish a stated agency purpose. However what is relevant is that whenever such governmental records are involved, the usage of such records for law enforcement, tax collection, disciplinary or counter-intelligence purposes is prohibited. But after the 9/11 attacks, the issue of data retention has acquired a different dimension. The US Patriot Act and the EC directives recently give much wider powers for blanket retention of personal data. For example, in the UK the Anti-terrorism, Crime and Security Act 2001(which bases itself on the EC directives) contains provisions which allow communications service providers to retain data about their customers for national security purposes. This usage of ISPs to store data for the government (supposedly voluntarily) is quite odd, but even worse is the fact that the UK government acknowledges that this data retained might be used for the purposes which are not related to national security. Such a contention flies straight in the face of a fundamental tenet of Data Protection regimes — that the information retained may not be used for purposes other than what it is retained for.[9] These new developments in data retention cause concern, as not only are they dis-proportional to the threats faced, thus are also quite purposeless in that the objective will not be served by any blanket retention of data.

Please answer the following Self Assessment Question.

Self Assessment Question 3 *Spend 3 Min.*

What does the HIPAA stand for and what does it seek to address?

.....

.....

.....

.....

.....

.....

15.7 DATA TRANSFER REGIME

The data transfer regimes need to be studied because in their zeal to protect the processing of personal data of Europeans outside of Europe. The European Union issued Data Protection Directive 95/46/EC of the European Parliament which requires that in case personal information needs to be transmitted outside the EU to a country then it can be done only to countries which ensure an adequate level of protection for the subject of data. An adequate level of protection will only be when the country has specific legislation with regard to the informational privacy of individuals with a formal enforcement mechanism[10]. As a result quite a few countries were not able to reach the standards that were required by EU. Therefore to get around it, the EU allows the data exporter to ensure that adequate safeguards are in place where the data is to be transferred and in that case such transfer of data will be allowed. This is a cumbersome process as the contract clauses have to be tailored to suit this. Therefore presently in EU there have been efforts get together certain binding corporate rules, which will allow corporates to establish adequate safeguards without introducing them into the contracts. Though as of now regulatory approval has to be sought in each country for

the binding rules, there are plans to have one stop approval for authorization from all countries for the rules. Enforcement mechanisms suggested for these binding rules vary from self regulation to flexible regulatory frameworks. This concept of binding corporate rules is a new approach and can just hold the key in quicker establishment of uniform data protection norms all over the world, especially since the initiative will rest with the companies in this situation.[11]

These are only a few trends in the growing and dynamic world of information technology or cyberlaws which need to be addressed in the coming years in order to make cyberspace a safe and secure place for transactions.

Please answer the following Self Assessment Question.

Self Assessment Question 4 *Spend 3 Min.*

What are the concepts of adequate level of protection and adequate safeguards as per the EU Directive?

.....

.....

.....

.....

.....

.....

Let us now summarize the points covered in this unit.

15.8 SUMMARY

- Laws have been forced to evolve rapidly with increasing use of information systems.
- Two major issues in privacy are unsolicited commercial email and cookies and such other tracking devices
- The US and EU have basic and sometimes stringent laws to protect the privacy of all individuals in their geographies.
- India still lacks E-governance guidelines and an effective legal framework to ensure that governments provide citizens with valuable services.
- Information Warfare is about computer based information operations that could provide adversaries of a country with an asymmetric response to that country's military superiority.
- Legal issues are increasingly arising in respect of retention of electronic records in terms of how much information is being recorded, for what purpose and how the security provisions are faring in respect of the same.
- The EU Data Protection Directive provides for data export only where adequate levels of protection are present or adequate safeguards can be insured.

15.9 TERMINAL QUESTIONS

1. What is your opinion on the changing and dynamic technology and the struggle of policy and law to keep pace with this technology?
2. What are the evolving trends in privacy laws in India and the rest of the world and what measures do you think India should take in order to keep up with the changing technology?
3. How is increasing electronic retention of records becoming an issue for both protection of privacy and information security?
4. What measures need to be taken by India to ensure that an effective e-governance regime is established?
5. What is your understanding of the concept of information warfare and what counter measures must be taken?

15.10 ANSWERS AND HINTS

Self Assessment Questions

1. Some of the common universal standards pertaining to cookies and other tracking features are the Open Profiling Standard (OPS) and the World Wide Web Consortium's Platform for Privacy Preferences Project (P3P).
2. An effective legal framework in respect of e-governance should ensure that governments have the opportunity to keep pace with the new era of global communication and efficiently provide citizens with valuable services.
3. HIPAA stands for the Health Insurance Portability and Accountability Act of 1996. It addresses privacy and security issues in specific fields like electronic healthcare transactions.
4. The EU data protection directive sets out that in case personal information needs to be transmitted out side the EU, and then it can only be to countries which ensure an adequate level of protection for the subject of data. The EU however, also alternatively permits the transmission of such information if the data exporter can ensure that adequate safeguards are in place for the same.

Terminal Questions

1. Refer to section 15.3 of the unit.
2. Refer to section 15.3 of the unit.
3. Refer to section 15.6 of the unit.
4. Refer to section 15.4 of the unit.
5. Refer to section 15.5 of the unit.

15.11 REFERENCES AND SUGGESTED READINGS

1. Susan E. Gindin. "Lost and Found in Cyberspace". San Diego Law Review 34(1997):1153.

2. Cyber Promotions. Inc. v. American Online 948 F.Supp. 456, 459(E.D. Pa.1996). CompuServe Inc. v. Cyber Promotions Inc. 962 F. Supp. 1015 (S.D. Ohio 1997) and Concentric Network Corp. v. Wallace. 24 Mar. 2007 <http://www.jmls.edu cyber/casesconcent1.html>.

3. Alison Fortescue. "Data Protection and Marketing for Global Organisations". Privacy and Data Protection Journal. 4. 5. (June 2003).

4. Charles H. Kennedy. "FTC Opens New CAN-SPAM Act Proceeding". Morrison-Foerster Legal updates and News. May 2005. 24 Mar. 2007 <http:// www.mofo.com/news/updates/files/update02026.html>.

5. Pamela Samuelson. "Privacy as Intellectual Property". Stan L. Rev. 52 (2000): 1125.

6. Cyber Threat Trends and US Network Security. 1 Apr. 2007 <http://www.cia.gov/ nic/testimony_cyberthreat.html>.

7. Ibid.

8. Randall E. Colson. HIPAA and Outsourcing: The Impact of Business Associate Rules under the Final Privacy and Security Standards. Negotiating Technology Outsourcing Agreements Law Seminars International. Seattle: Washington. 2003.

9. Rowland, "Data Retention and the War Against Terrorism – A Considered and Proportionate Response?". The Journal of Information, Law and Technology 3 (2004). 2 Apr. 2007 <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004_3/ Rowland/>.

10. Susan Grindin. "As the Cyber-World Turns: The European Union's Data Protection Directive and Trans-border Flows of Personal Data". 24 Jan 1998. 2 Apr. 2007 <http://www.info-law.com/eupriv.html>.

11. Karin Retzer. "Land in Sight: The Latest Developments Concerning Data Transfers from the EU". Morrison-Foerster Legal Updates and News. Feb. 2005. 4 Apr. 2007 <http:/www.mofo.com/news/updates/files/update1428.html>.