

---

# UNIT 10 THE REGULABILITY OF CYBERSPACE

---

## Structure

- 10.1 Introduction
- 10.2 Objectives
- 10.3 Desirability of Regulation of Cyberspace
  - 10.3.1 Need for Regulation of Cyberspace
- 10.4 How Cyberspace can be Regulated
- 10.5 Legal and Self Regulatory Framework
  - 10.5.1 Filtering Devices and Rating Systems
- 10.6 Government Policies and Laws Regarding Regulation of Internet Content
- 10.7 Regulation of Cyberspace Content in the United States
  - 10.7.1 Communications Decency Act 1996(CDA)
  - 10.7.2 Internet Online Summit (December 1997)
  - 10.7.3 COPA
  - 10.7.4 CIPA
  - 10.7.5 Other Related Legislation
- 10.8 Regulation of Cyberspace Content in Australia
- 10.9 Regulation of Cyberspace Content in European Union
- 10.10 Regulation of Cyberspace Content in United Kingdom
  - 10.10.1 Related Legislation in UK
- 10.11 Regulation of Cyberspace Content in India
- 10.12 International Initiatives for Regulation of Cyberspace
  - 10.12.1 Organization for Economic Cooperation and Development (OECD)
  - 10.12.2 UNESCO
- 10.13 Summary
- 10.14 Terminal Questions
- 10.15 Answers and Hints
- 10.16 References and Suggested Readings

---

## 10.1 INTRODUCTION

---

Internet is not a physical or tangible entity but rather a giant network which interconnects innumerable smaller groups of linked computer networks. The term 'online' (relating to the form of communication and its mode of transmission by telecommunication lines) can also be used. There has been a rapid increase in the use of the online environment where millions of users have access to internet resources and are providing contents on a daily basis. This content can be accessed from any computer connected to the network

though the content may be actually stored on a number of different computers or 'servers' which need not be in the same jurisdiction as the person who is accessing the material. Internet users may be completely unaware where the resource being accessed, is in fact physically located. This computer networking has been very helpful for businesses of all types for a variety of commercial transactions and consumer services. Apart from transactions involving physical goods, delivery of digitized information products such as music, photographs, novels, motion pictures, multimedia works and software can also be done online. In future also it leads to an increase of economic and creative interactions and inevitably also leads to expansion of disputes involving acquisition, use, possession, processing and communication of information.

The rules for regulating business interaction in a country are different from rules for online commerce. Every country in the world is regulated by law, which is the primary source of regulation. Social norms which guides ones behaviour also function as secondary regulatory constraint. The third constraint is the market which regulates through price mechanism by limiting the amount which a person can spend on different needs; another constraint may be the nature of the world in which we exist. In the real world, the person or the entity with whom interaction relating to business is going on can be located; and thereby the validation of a transaction is facilitated. But in Cyber Space it is very difficult, since parties to a transaction may be sitting in adjoining rooms or in distant locations but the network offers no way to know it. It is often argued that cyberspace is unavoidable but it is not regulable, its behaviour can't be regulated. According to Dr. Dan L. Burk, Assistant Professor of Lawseton Hall University, there is simply no coherent homology between Cyberspace and real space, and screening or blocking of Internet resources by country is nearly impossible. On the other hand it is argued by Lawrence Lessing in his article, "The Laws of Cyberspace", that Cyberspace has the potential to be the most fully and extensively regulated space that has ever been known – anywhere at any time in our history. According to him just as in real space, behaviour in Cyberspace is regulated by four sorts of constraint i.e. law, social norms, market and codes (also called architecture).

Every technological revolution brings with it a new spate of legal issues and legal problems to be addressed. The real purpose of our study is to stress the need for regulation of Cyberspace and the possibility and scope of its regulation.

---

## 10.2 OBJECTIVES

---

After studying this unit, you should be able to:

- explain the need and desirability for regulation of internet content both in developed and developing countries;
- discuss that in relation to harmful content on on-line services, the greater emphasis is on self-regulatory scheme of industry governance;
- discuss the nation's legal policies and framework for regulating cyberspace;
- state the desirability for international framework of principles, guidelines and rules for global communication; and
- discuss the need for coordinated national, if not international criminal laws to deal with illegal content on online services.

---

## 10.3 DESIRABILITY OF REGULATION OF CYBERSPACE

---

### 10.3.1 Need for Regulation of Cyberspace

The following reasons can be cited in favour of the above proposition:

- 1) The most visible and readily sensational concern is about the use of internet particularly for the distribution of obscene, indecent and pornographic content. The use of internet for child pornography and child sexual abuse and the relative ease with which the same may be accessed calls for strict regulation.
- 2) The challenge that Cyberspace is posing to traditional notions of jurisdiction and regulation is another factor. The increasing business transaction from tangible assets to intangible assets like Intellectual Property has converted Cyberspace from being a mere info space into important commercial space. The attempt to extend and then protect intellectual property rights online will drive much of the regulatory agenda and produce many technical methods of enforcement.
- 3) With the inventions of new technologies, the media has enhanced the possibility of invasion of the privacy of individual and bringing it into the public domain. The major area of concern where some sort of regulation is desirable is data protection and data privacy so that industry, public administrators, netizens, and academics can have confidence as on-line user.
- 4) Encryption is the process of converting a message or document into a form which hides the content of the communication from the eyes of an eavesdropping third party and needs to be decrypted if its content is to be read. New cryptographic techniques (cryptography is the process used to encode/encrypt electronic information) are commonly cracked in a relatively short time by computational force or by other analytical means. Therefore another area in which regulation has assumed importance is in the debate over whether the public should be permitted to use 'cryptography' or not.
- 5) Internet has emerged as the 'media of the people' as the internet spreads fast there were changes in the press environment that was centered on mass media. Unlike as in the established press, there is no editor in the Internet. In the press and publication environment, editors check the truthfulness of facts and circulate them once the artistic values are confirmed. On the internet however, people themselves produce and circulate what they want to say and this direct way of communication on internet has caused many social debates. Therefore the future of Cyberspace content demands the reconciliation of the two views of freedom of expression and concern for community standards.
- 6) Another concern is that, money laundering, be 'serious crime' becomes much simpler through the use of net. The person may use a name and an electronic address, but there are no mechanisms to prove the association of a person with an identity so that a person can be restricted to a single identity or identity can be restricted to a single person. Viruses, rumor-mongering, hate-mail and mail box bombardment are all describable phenomena and because of the fear of retribution all are more likely to use fake identity or may be anonymous mailers rather than a readily identifiable person. Therefore Cyberspace needs to be regulated to curb this phenomenon.

Please answer the following Self Assessment Question.

**Self Assessment Question 1**

*Spend 3 Min.*

Describe the need for regulation of cyberspace?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

---

**10.4 HOW CYBERSPACE CAN BE REGULATED**

---

In “Code and other Laws of Cyberspace”, Lawrence Lessing argues that the architecture (code) of the internet i.e. The hardware and software of Cyberspace that define the system can be a form of regulation. It is a set of rules implemented or codified in the software by the code writers, requiring the constant certification of identity.

In “A Non delegation doctrine for the digital age” (Cited: 50 Duke L.J. 5), James Boyle argued that regulation of the internet can increasingly rely on a three fold strategy:

- i) Privatization: The state can use a private body to achieve those goals which it could not get directly and then implement that body’s decision through mandatory technological arrangements. For e.g. for Copyright enforcement in Cyberspace, the Clinton administrations original plan was to make Internet Service Providers (ISPs) strictly liable for copyright violations by their subscribers – thus creating a private police force, largely free of statutory and constitutional privacy constraints with strong incentives to come up with innovative surveillance and technical enforcement measures.
- ii) Propertization: According to him, first of all an attempt is to be made to extend and then protect intellectual property rights online. This will produce many technical methods of enforcement.
- iii) Technological Controls the system is to be designed so as to hardware in desired regulatory features. For e.g. Digital texts and music could be encoded to a particular person. Detection devices could be built in to players, so that others cannot play one’s music. Unique identifiers could be built into computer chips, so that a person’s computer would broadcast a universal ID with an associated set of legal characteristics as you roamed the net.

Blocking software or Internet contents grading system are other forms of regulations based on technology. In Korea, the government has started the internet contents grading system. The system forces the sites designated as 'content harmful to minors' to attach an electronic tag that the blocking software can catch. Especially the Korean government categorises homosexual sites as content harmful to minors and those sites are often blocked.

---

## 10.5 LEGAL AND SELF REGULATORY FRAMEWORK

---

In any country the role of government is seen as the provider of legal and regulatory framework within which its subjects have to function. In this context of regulation of cyberspace it can be said that the Internet's design precludes central control which may be regulated by government to make the information economy safe, secure, certain and open. Rather in the last few years outstanding progress has been made in identifying appropriate structures for industry self-regulation with the minimum appropriate level of government intervention. The development of technology to permit content labeling and the early growth of complaint hot lines in a number of countries have helped to provide the ingredients for self-regulatory schemes. Here we will discuss some of the major developments in the area of national and international cooperative, major developments for effective online industry regulation in various countries, and end-user voluntary use of filtering/ blocking technologies. This approach is taken in United Kingdom, Canada, New Zealand and a considerable number of Western European countries.

But the idea that Cyberspace should be presumptively self-governing has resounded in thoughtful scholarship and has been criticized by many scholars and it has been argued that the selective government regulation of Cyberspace is warranted to protect and promote liberal democratic ideas. However in this unit we will not go into the jurist's debate whether Cyberspace can be self regulated or not but try to find out the possibilities in the existing legal framework in various countries for regulating internet content.

### 10.5.1 Filtering Devices and Rating Systems

'Filters' are software tools used to block access to unwanted material. By the 1990's, concerns about problematic content on on-line services had prompted the development of a range of content filter software and rating systems including the Platform for Internet Content Selection ('PICS'); for example, E-mail filters automatically delete the bulk of unread e-mail messages commonly known as 'spam' and can also be customized to delete incoming messages from particular sources. There can be site blocking filters to screen out specified websites or websites containing specified keywords that the system presumes to relate to other objectionable content. Site blocking filters also may use a protocol 'PICS' developed by the World Wide Web Consortium ('W3C') to develop common protocols for the World Wide Web's evolution and ensure its interoperability. Organizations in several countries have established labeling schemes, which conform to the PICS standards, designed for use by parents and schools. For example, RSACi (Recreational Software Advisory Council labeling scheme for the Internet) rating system addresses the level of violence, sex, nudity, and language on a website and operates as a classification of the content on an Internet site rather than making a judgment about its appropriateness for any given audience or purpose. Such an approach has advantages over those filtering programmes that operate on a keyword basis to exclude offensive

material but inevitably, a significant amount of useful, inoffensive content is also blocked. However its major disadvantage is that it is limited to rating functions, rather than more general information. Consequently, it is not adapted to perform more complex information retrieval searches. Other labeling schemes are Safe surf, Cyber Patrol and SurfWatch.

In 1997 W3C created the 'Metadata Activity', which includes the Resource Description Framework (RDF) Working Group. RDF is a protocol for description of Internet content based on a set of 105 'categories' of information, known as the 'Dublin Core', which is used to Filter out obscene content. However it does not deal with controversial content or aim to protect children from harmful content, but describes those aspects of content such as authorship, publishers, date and source in a similar way to that developed by library catalogues and facilitates more effective searching. Examples of its applications include search engine data collection and digital library collections. Therefore it has not been widely used as an alternative to those schemes that eliminate content on the basis of controversial content alone (see speech by Gareth Grainger).

Please answer the following Self Assessment Question.

<b>Self Assessment Question 2</b>	<i>Spend 3 Min.</i>
What do you mean by the term filters? Give examples.	
.....	
.....	
.....	
.....	
.....	
.....	

---

## 10.6 GOVERNMENT POLICIES AND LAWS REGARDING REGULATION OF INTERNET CONTENT

---

According to Electronic Frontiers Australia (EFA, March 2002) report on government policies regarding internet censorship in various countries, government policies can be classified into the following four categories:

- 1) The policy to encourage self regulation.
- 2) Criminal law penalties (Fines or Jail Terms) applicable to content providers who make content "unsuitable for minors" available online.
- 3) The government has also mandated blocking of access to content deemed unsuitable for adults; for example Australia, China, Saudi Arabia, Singapore etc.
- 4) A number of countries have either prohibited general public access to the internet or require internet users to be a registered / licensed by a government authority before permitting them restricted access.

However concerns over access to content on internet vary markedly around the world and this is reflected by the respective regulatory policies, which we will now discuss below.

---

## **10.7 REGULATION OF CYBERSPACE CONTENT IN THE UNITED STATES**

---

The exponential growth in the usage of on-line services in the United States in the late 1980s and early 1990s led to demands for its operations to be regulated.

### **10.7.1 Communications Decency Act 1996 (CDA)**

The Section 502 of the CDA amended sections 223(a) and (d) of Title 47 of the United States Code ('USC'). It prohibits the making and transmission of obscene or 'indecent' material to a minor by means of a telecommunications device, and the use of an interactive computer service to send or display 'patently offensive' material to minors. The provisions also prohibited a person from knowingly permitting a telecommunications facility under that person's control to be used to commit these offences. However Supreme Court in *American Civil Liberties Union v, Janet Reno, Attorney General of the United States; American Library Association, Inc. v, United States Department of Justice* (the 'CDA Case', 1997) declared unconstitutional the above two statutory provisions as a violation of both freedom of speech and personal privacy.

### **10.7.2 Internet Online Summit (December 1997)**

One of the consequences of the US Supreme Court's rejection of the CDA in July 1997 was the calling of an Internet on-line Summit, entitled 'Focus on Children', to examine alternative strategies to promote children's interests on-line. The Summit's main focus was on the issue of appropriate content for children and personal safety, it also emphasized the need to enforce existing obscenity laws and laws against child pornography. At the Summit, the US Internet Service Provider ('ISP') industry announced its new 'zero tolerance' policy against child pornography, involving full cooperation with law enforcement agencies, and the use of the Cyber tip line also announced at the summit. Strategies for specialist training for police officers in the investigation of computer crime were put forward.

### **10.7.3 COPA**

In 1998 US Congress enacted Children Online Protection Act (COPA), which was very narrow in scope and covered only communications that were made for commercial purposes on the World Wide Web but the same was struck down by Supreme Court in *Aschcroft vs American Civil Liberties Union* (2004).

### **10.7.4 CIPA**

In 2000 Children Internet Protection Act (CIPA) was passed. This Act requires the schools and libraries to install filters on computers used by minors and adults.

### **10.7.5 Other Related Legislation**

The two legislations which need to be mentioned here are:

- i) Uniform Electronic Transactions Act, 1999 (UETA) - to remove barriers to electronic commerce by validating and electronic records and signatures. However the substantive rules of contract remain unaffected by it.

ii) Uniform Computer Information Transaction Act, 2000 (UCITA)

According to UCITA, for a transaction to be 'Computer Information Transaction', the main focus of the transaction must be acquiring the computer information, access to it, or its use and not a mere incident of another transaction. The act applies to contracts for the development or creation of computer information, such as software development contracts and contracts to create a computer database. This Act does not apply to many cases in which one person provides information to another person for another transaction such as making an employment or loan application.

---

## 10.8 REGULATION OF CYBERSPACE CONTENT IN AUSTRALIA

---

In Australia, the growth in the use of the Internet and the concern for abusive content on the internet led to the establishment of the Australian Broadcasting Authority ('ABA') which was established pursuant to the Broadcasting Services Act 1992 by the Commonwealth of Australia for the regulation of broadcasting media in Australia. The ABA's 1996 report on content of on-line services, recommended in favour of a scheme of industry substantial self-regulation for on-line services with voluntary codes of practice supported by the labeling of on-line content using PICS and identified the advantage of PICS protocol in Australia. Following on from this Report, on 15 July 1997 the Australian Minister for Communications and the Arts and the Australian Attorney-General announced 47 principles for a national approach to regulate the content of on-line services (Internet), 'inferring' towards the view that 'material accessed through on-line services should not be subject to a more onerous regulatory framework than 'off-line' material such as books, videos, films and computer games'. For the investigation into matters relating to future regulatory arrangement of online services ABA formed a children and content online task force which works in three key areas (a) contact and safety issues (b) illegal content and (c) unsuitable content areas that affect children and has also developed a set of practical recommendations, aiming to address this.

### **Broadcasting Services Amendment (Online Services) Act, 1999**

This Act came into force on January 1, 2000. There is a provision for additional access prevention method other than ISP blocking of overseas hosted material at server level.

---

## 10.9 REGULATION OF CYBERSPACE CONTENT IN EUROPEAN UNION

---

The approach of a large majority of (perhaps all) European Union Member States in dealing with illegal and harmful content on the Internet appears to be in accord with the 1996 recommendations of the European Commission advocating the use of filtering software and rating systems, and an encouragement of self-regulation of access-providers. In these countries, laws regarding material that is illegal offline, such as child pornography and racist material, also apply to Internet content. With regard to material unsuitable for children, the EU Safer Internet Action Plan covering the period 1999-2002 has a budget of 25 million euro and has three main action lines;



- Creating a safer environment through promotion of hotlines, encouragement of self-regulation and codes of conduct,
- Developing filtering and rating systems, facilitation of international agreement on rating systems,
- Awareness: Making parents, teachers and children aware of the potential of the Internet and its drawbacks, overall co-ordination and exchange of experience.

---

## 10.10 REGULATION OF CYBERSPACE CONTENT IN UNITED KINGDOM

---

In September 1996 UK Government issued R3 Safety-Net action plan (now Internet Watch Foundation, IWF), developed by UK ISP trade associations and where it is agreed by Government involve industry for establishment of complaints hotline and related take-down procedures for illegal Internet content, primarily child pornography. In February 2002, the IWF announced that it would henceforth also deal with “criminally racist content”.

### 10.10.1 Related Legislation in UK

- 1) Data Protection Act, 1998 for the regulation of processing of information relating to individuals including the obtaining, holding, use or disclosure of such information.
- 2) Electronic Communications Act, 2000 to facilitate the use of electronic communications and electronic data storage.

---

## 10.11 REGULATION OF CYBERSPACE CONTENT IN INDIA

---

In India, cyber laws are contained in the Information Technology Act 2000. The main objective of the Act is to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as e-commerce, which involve the use of alternatives to paper-based methods of communication and storage of information to facilitate electronic filing of documents with the Government agencies.

### Digital Signatures [Chapter II]

Any subscriber (i.e., a person in whose name the Digital Signature Certificate is issued) may authenticate electronic record by affixing his Digital Signature. Electronic record means data record or data generated image or sound, stored, received or sent in an electronic form or microfilm or computer generated microfiche.

### Electronic Governance [Chapter III]

Where any law provides submission of information in writing or in the typewritten or printed form, it will be sufficient compliance of law, if the same is sent in an electronic form. Further, if any statute provides for affixation of signature in any document, the same can be done by means of Digital Signature.

Similarly, the filing of any form, application or any other documents with the Government Authorities and issue or grant of any licence, permit, sanction or approval and any

receipt acknowledging payment can be done by the Government offices by means of electronic form. Retention of documents, records, or information as provided in any law, can be done by maintaining electronic records. Any rule, regulation, order, by-law or notification can be published in the Official Gazette or Electronic Gazette.

However, no Ministry or Department of Central Government or the state Government or any Authority established under any law can be insisted upon acceptance of a document only in the form of electronic record.

#### **Regulation of Certifying Authorities [Chapter IV]**

The Central Government may appoint a Controller of Certifying Authority who shall exercise supervision over the activities of Certifying Authorities.

#### **Digital Signature Certificate [Chapter VII]**

Any person may make an application to the Certifying Authority for issue of Digital Signature Certificate. The Certifying Authority while issuing such certificate shall certify that it has complied with the provisions of the Act.

#### **Penalties and Adjudication [Chapter IX]**

If any person without the permission of the owner, accesses the owner's computer, computer system or computer net-work or downloads copies or any extract or introduces any computer virus or damages computer, computer system or computer net work data etc. he/ she shall be liable to pay damage by way of compensation not exceeding Rupees One Crore to the person so effected.

#### **The Cyber Regulations Appellate Tribunal [Chapter X]**

Under the act, the Central Government has the power to establish the Cyber Regulations Appellate Tribunal having power to entertain the cases of any person aggrieved by the Order made by the Controller of Certifying Authority or the Adjudicating Officer.

#### **Offences [Chapter XI]**

Tampering with computer source documents or hacking with computer system entails punishment with imprisonment up to three years or with fine up to Rs. 2 lakhs or with both.

Publishing of information, which is obscene, in electronic form, shall be punishable with imprisonment up to five years or with fine up to Rs. 10 lakh and for second conviction with imprisonment up to ten years and with fine up to Rs. 2 lakhs.

---

### **10.12 INTERNATIONAL INITIATIVES FOR REGULATION OF CYBERSPACE**

---

Today there is a need for an international framework of principles, guidelines and rules for global communications for the twenty-first century. In July 1997, the German Government hosted an International Conference in Bonn on the topic 'Global Information Networks', in cooperation with the European Commission. It was attended by Ministers from 29 European Union, EFTA, CCEC and G7/G8 countries as well as by representatives of on-line content providers, access and service providers and users of on-line services. It resulted in the adoption of the 'Bonn Declaration' of the Ministers as well as declarations by industry and user participants.

The Bonn Declaration pointed in the direction of:

- 1) using current national legal frameworks for the enforcement of criminal law provisions where appropriate in respect of on-line crime;
- 2) development by industry of common principles for schemes of self-regulation regarding content of on-line services; and
- 3) establishment of national hotlines for complaints regarding on-line content and for some appropriate interconnection and interaction between national hotlines.

Martin Bangemanns, EC Commissioner in her speech of 8 September 1997 to the International Telecommunications Union in Geneva has pointed out that there is a need for an international charter for global communications, and in particular governing activities carried out over the Internet, could provide a suitable framework covering such issues as the legal recognition of digital signatures, encryption, privacy, protection against illegal and harmful content, customs and data protection. The tools for achieving these objectives would include mutual recognition, self-regulation and, if needed, regulation.

In 29 June 1998, on invitation by Martin Bangemann, business leaders from around the world participated in a discussion on global communication issues, with the objective to explore the need for strengthened international coordination which resulted in the formation of Global Business Dialogue and it was resolved that wherever possible, it should avoid legislation, and concentrate on market-led, industry-driven, self-regulatory models and any regulation should ensure competition. It should focus on a well-defined list of issues on which quick progress can be made with the close cooperation of business, consumer groups and governments of all countries who wants to participate and work on these issues should be industry-led and coordinated with relevant international bodies. Two organizations closely involved in this process were the Transatlantic Business Dialogue and the US-Japan Business Council. Attendance at the first meeting of the GBD's Business Steering Committee took place in New York on 14 January 1999 and consisted largely of representations of major corporations from United States, Europe and Japan. However, the issue of Internet content was not considered amendable to relatively fast solutions by the GBD and so Internet content is not receiving immediate attention from this Group.

In 27 February 1999, the first meeting of the International Network of Experts on Self-Regulation for Responsibility and Control on the Internet was held at New York. This network was brought together by the Bertelsmann Foundation, a charitable foundation which owns the controlling interest in Bertelsmann Corporation, the German media and publications enterprise, as a part of its advocacy of self-regulatory solutions to the problems of Internet content. The three regulatory agencies represented at the meeting were the Australian Broadcasting Authority, the Canadian Radio Telecommunications Commission (by Mr. Ted Woodhead) and the Singapore Broadcasting Authority (by Ms. Ling Pek Ling); all of which are actively dealing with the issues of self-regulation of harmful content on the Internet.

The above study reflects different legal policies in the world for regulation of cyberspace and International efforts to deal with it. However some sort of criminal penalties should also be there in all national laws for which coordinated criminal laws are needed to deal with illegal content on on-line services.

### 10.12.1 Organization for Economic Cooperation and Development (OECD)

The OECD an international organization working in the area of data privacy and information security, established an ad hoc process of meetings (the first was on 1-2 July 1997 and second on 22 October 1997) on approaches being taken in major industrial countries for the regulation of content conduct on the Internet. The meeting acknowledged the primary role of the private sector in regulating the Internet. However at the joint OECD/Business and Industry Advisory Committee forum held on 25 March 1998 in Paris, the OECD resolved to do no further work in this area. On 19 April 2006, OECD task force on spam has recommended that Governments and industry should step up their coordination to combat the global problem of spam. It calls on governments to establish clear national anti-spam policies and give enforcement authorities more power and resources. Co-ordination and co-operation between public and private sectors are critical, the report notes.

### 10.12.2 UNESCO

The United Nations Educational, Scientific and Cultural Organization (UNESCO) was founded on 16 November 1945. At the 29th UNESCO General Conference held in Paris from 21 October to 12 November 1997 the Director-General of UNESCO made a preliminary report on the feasibility of an international instrument on the establishment of a legal framework relating to cyberspace. It recommended the preservation of a balanced use of language on cyberspace, which represented the concern of non-Anglophone countries at the domination of English as the language of the Internet. Today, UNESCO functions as a laboratory of ideas and a standard-setter to forge universal agreements on emerging ethnical issues: the organization also serves as a clearing house – for the dissemination and sharing of information and knowledge – while helping Member States to build their human and institutional capacities in diverse fields.

Please answer the following Self Assessment Question.

#### Self Assessment Question 3

*Spend 3 Min.*

State whether the following statements are true or false:

- a) In Australia, government has mandated blocking of access to content deemed unsuitable for adults.  
.....
- b) In Korea, the government has no system of Internet content grading.  
.....
- c) Australian Broadcasting Authority and Singapore Broadcasting Authority are the only two regulatory agencies in the meeting of International Network of Experts (Feb, 1999).  
.....

Let us now summarize the points covered in this unit.

---

## 10.13 SUMMARY

---

- There has been rapid increase in use of internet for various types of commercial transactions and consumer services.
- For the safe carriage and conduct of Cyberspace, regulation ought to be identified as appropriate and necessary.
- The necessity arises due to the expansion of economic and creative interaction which in term led to disputes involving acquisition, use, possession, processing and communication of information.
- The use of internet for obscene, indecent and pornographic content, rumor mongering, viruses, cyber crime, possibility of invasion of privacy of individuals, all this emphasized the need for cyberspace regulation.
- Legal policies in various countries like USA, UK, European Union, and New Zealand show that in the context of regulation of Cyberspace more emphasis is on self regulation through use of filtering/blocking technologies.
- There is need for coordinated international guidelines and principles to regulate cyberspace.
- International organizations such as OECD and UNESCO can play an important role in framing international regulatory framework for internet.

---

## 10.14 TERMINAL QUESTIONS

---

- 1) Discuss the need for Cyberspace Regulation.
- 2) What are government policies and laws regarding Cyberspace Regulation in USA, India and UK?
- 3) “Internet design precludes central control by government rather an attempt has been made for industry self regulation.” Comment.

---

## 10.15 ANSWERS AND HINTS

---

### Self Assessment Questions

- 1) Yes, there is a need for regulation of cyberspace. The use of internet for distribution of obscene, indecent and pornographic content, and child pornography; increasing numbers of business transactions through internet and issue of intellectual property rights; issues of privacy and emerging cyber crimes are major areas of concern today that point towards the need to regulate cyberspace.
- 2) ‘Filters’ are software tools used to block access to unwanted material. Examples are E-mail Filters, Site Blocking Filters.
- 3) (a) True, (b) False & (c) False

## Terminal Questions

- 1) Refer to section 10.3.
- 2) Refer to section 10.7, 10.10 & 10.11 of the unit.
- 3) Refer to section 0.5 – 10.12 of the unit.

---

## 10.16 REFERENCES AND SUGGESTED READINGS

---

1. “Anti Spam Toolkit of recommended policies and measures”. OECD Task force on Spam. 19 April 2006. 30 Dec. 2006 <<http://www.oecd-antispam-org>>.
2. “Internet Censorship: Law and Policy around the world”. Electronic Frontiers Australia (EFA). 28 Mar. 2002. 2 Dec. 2006 <<http://www.efa.org.au/>>.
3. Dr. Dan L. Burk. “Jurisdiction in a World without Borders”. Virginia Journal of Law and Technology university of Virginia, 1997. 23 Nov. 2006 <<http://vjolt.student.virginia.edu>>.
4. Gareth Grainger. “Freedom of Expression and regulation of Information in Cyberspace: Issues concerning potential information cooperation principles for cyberspace”. speech given at UNESCO INTERNATIONAL CONGRESS, INFO Ethics '98, Monte Carlo, Monac. 1 Sept. 1998.
5. James Boyle. “In a Non Delegation Doctrine for the Digital Age”. Duke L.J. 5.50.
6. Lawrence Lessing. “Commentories – The Law of the Horse: what cyberspace might teach”. Harvard Law Review 113(1991):501. <<http://www.lessing.org/control/articles/works/finalhls.pdf>>.
7. Lawrence Lessing. “Code and Other Laws of Cyberspace”. 1999. 85-99.
8. Lawrence Lessing. “The Laws of Cyberspace”. essay presented at – Taiwan Net '98 Conference in Taipei, Mar. 1998. 24. Nov. 2006 <[http://www.lessing.org/content/articles/works/laws\\_cyberspacepath](http://www.lessing.org/content/articles/works/laws_cyberspacepath)>.
9. Martin Bangemann's. “New World Order for Global Communications – The Need for an International Charter”. Speech given at International Telecommunications Union, Geneva. 8 Sept. 1997.