IT act provide laws to protect **computer crimes**, charge **penalties** and **compensation** for the same. The bill proposes that if the computer crime involves a computer, computer system or computer network **located in India**, the law shall also apply to any contravention and offenses committed outside India by any person irrespective of his nationality. There are consequential amendment proposed in the Indian Evidence Act 1872, The Indian Penal Code 1860, The Banker's Book Evidence Act 1891 and The Reserve Bank of India Act 1934. For further study the web site http://www.mit.gov.in/itbillonline/it_framef.asp may be referenced.

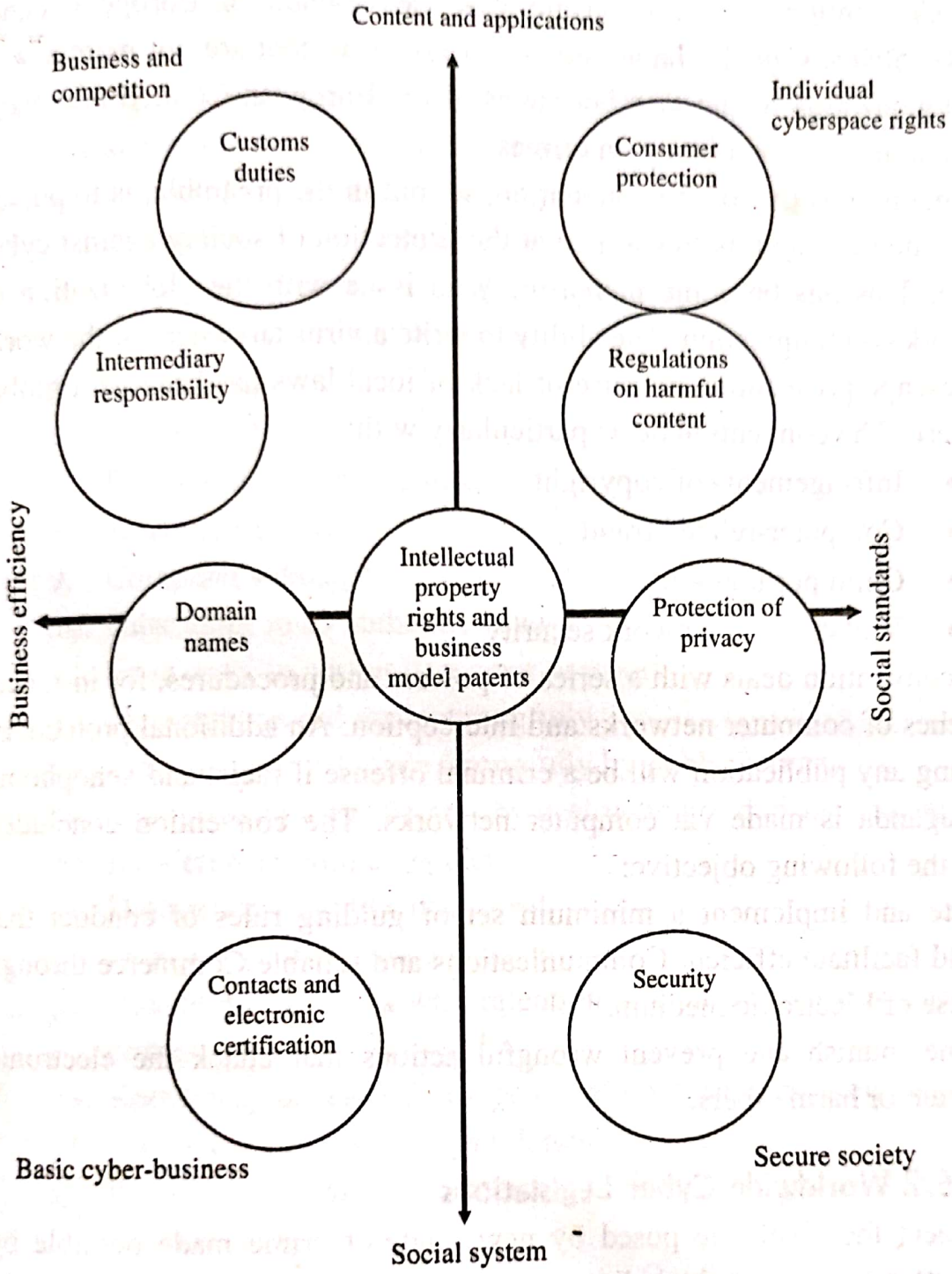
§ 1.6 Cyber laws

Law is a body of rules of action or conduct prescribed by controlling authority, and having binding legal force. That which must be obeyed and followed by citizens subject to sanctions or legal consequences is a law. The functions of law are:

- Keeping the peace
- Shaping moral standards
- Promoting social justice
- Maintaining the status quo
- Facilitating orderly change
- Facilitating planning
- Providing a basis for compromise
- Maximizing individual freedom

Flexibility of the law responds to cultural, technological, economic, and social changes. Laws that are no longer viable are often repealed, although it may take years for that to happen. Sometimes, because of error or misuse, the law does not reach a fair result.

The cyber law deals with cyber rules. There are two different types of cyber rules, and these can be plotted on two different axes. The first type (plotted on the vertical axis) deals with a matrix that shows whether the applicable rule supports the E-commerce infrastructure or covers content and applications. The other type (plotted on the horizontal axis) focuses on objectives and shows whether the rule alms at business efficiency or maintaining social standards and security. The figure below uses such a framework to categorize some of the issues concerning cyber rules.



Cyber Rules: The Rules Governing E-commerce

The very fast development of Internet technology has led to the growth of new forms of transnational crime globally. These crimes have may affect any country across the globe any time. Thus, there is a need for necessary legislation in all countries for the prevention of such crimes propagated through electronic medium. There is no territorial boundary to it, which is made up of the screens and passwords, separate the "Cyber world" from the "real world" of atoms.

The Convention on Cyber crime was the Council of Europe experts, United States, Canada, Japan, and other countries that are not members of the organization of the member states of the European Council organized the first international treaty on crimes.

The main objective of the convention, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cyber crime. This has be come increasingly an issue with the globalization of network communication. The ability to write a virus anywhere in the world and escape prosecution because of lack of local laws has become a global concern. The convention deals particularly with:

- Infringements of copyright
- Computer-related fraud
- Child pornography
- Violations of network security

The convention deals with a series of powers and procedures, for instance, searches of computer networks and interception. An additional protocol of making any publication will be a criminal offense if racist and xenophobic propaganda is made via computer networks. The convention concluded with the following objective:

Create and implement a minimum set of guiding rules of conduct that would facilitate efficient Communications and reliable Commerce through the use of Electronic medium.

Define, punish and prevent wrongful actions that attack the electronic medium or harm others.

§ 1.6.2 Worldwide Cyber Legislations

To meet the challenge posed by new kinds of crime made possible by computer technology including telecommunication, many countries have also reviewed their respective domestic criminal laws so as to prevent computer related crimes. Some of these countries are USA, Austria, Denmark, France Germany, Greece, Finland, Italy, Turkey, Sweden, Switzerland, Australia, Canada, India, Japan, Spain, Portugal, UK, Malaysia and Singapore.

However, no country has fully resolved all the issues such as legal, enforcement and prevention of crime. The legislations enacted by different countries cover only few of the classified computer related offences.

However, looking to the dynamic and fast changing technology, new types of offences may pop-up frequently. Some of the major types of offences against which many countries across the globe have enacted various Acts (mostly at preliminary levels) are as follows: -

1. Unlawful access to data in computers
2. Damaging data in computer etc.
3. Unauthorized access to computer and computer material
4. Committing mischief with data
5. Data spying
6. Computer fraud
7. Forgery of prohibitive data
8. Alteration of data
9. Computer sabotage
10. False entry in an authentic deed
11. False entry in permit license or passport
12. Electronic record made wrongfully
13. Electronic record made wrongfully by public servant
14. Interferences with business by destruction or damage of computer
15. Interferences with computer
16. Destruction of public document
17. Destruction of private document
18. Unauthorized access with intention to commit offences/ computer crimes
19. Knowingly access of computer without authorization related to national defense or foreign relation
20. Intentional access of computer without authorization to obtain financial information
21. Unauthorized access of computer of a Govt. Dept. or agency

§ 1.6.3 Cyber Crimes

"Computer or Cyber crimes are considered as illegal, unethical or unauthorized behavior of people relating to the automatic processing and transmission of data, use of Computer Systems and Networks".

Common types of Cyber Crimes may be broadly classified in the following groups:

1. Against Individuals:
   a. Against Person:

i. Harassment through e-mails.
ii. Cyber-stalking.
iii. Dissemination of obscene material on the Internet.
iv. Defamation.
v. Hacking/cracking.
vi. Indecent exposure.

b. Against property of an individual:
i. Computer vandalism.
ii. Transmitting virus.
iii. Internet intrusion.
iv. Unauthorized control over computer system.
v. Hacking /cracking.

2. Against Organizations:
a. Against Government, Private Firm, Company, Group of Individuals:
i. Hacking & Cracking.
ii. Possession of unauthorized information.
iii. Cyber terrorism against the government organization.
iv. Distribution of pirated software etc.

3. Against Society at large:
i. Pornography (specially child pornography).
ii. Polluting the youth through indecent exposure.
iii. Trafficking.

A steady increase in number of crimes in this area is expected which demands for greater attention of lawmakers. Only territorial laws applicable to online activities have no relevancy or perhaps even determinable geographic location? The law of the Internet has already emerged, and can continue to emerge with individual users and various governance issues cannot be resolved overnight. The cyber legal processes needs to be redefine in the new dynamic context. Finally, the Cyber Law defined as a thoughtful group conversation about core values and distinct benefits to the Society will persist. But it will not, could not, and should not be the same law as that applicable to physical, geographically defined territories.