PREFACE

The main objective of the study is to facilitate healthy and effective growth of cyber legislations under a fast changing and highly technical environment. The statement of objects and reasons also recognizes that in the dynamic world of science and technology there is need to continuously explore the possibilities to combat cyber crime and simplify the laws governing internet and activities in cyber space. On a close examination of the Information Technology Act 2000 it would appear that this need has not been given due attention and the information technology law lacks perfectness and the main problem is that of identification of a cyber criminal and then comes the issue of jurisdiction. Furthermore the extradition of a cyber criminals seems to be a thing next to impossible as the definitions of various computer crimes differ from nation to nation. What is obscene is India may be an act of social and simple living in America.

In the absence of common international cyber laws and common definitions of cyber crimes enormous problems were being faced in locating and initiating legal action against such invisible and unidentifiable criminals.

Internet knows no jurisdiction in cyber space, so regulation is possible only after International
Harmonization and sincere efforts to liberalize the extradition treaties.

An attempt has accordingly been made in this work to examine as to 'what' and 'how' protection can be provided to a net user or any data / work saved in a computer system.

E-Governance is in its infancy stage but in near future it will govern the states. So every possible effort is being made through Information Technology Act 2000 to fill the possible loopholes that could destroy the complete administrative structure.

To examine the various aspects noted above, the present research study has been divided into seven chapters. The First chapter, as usual is devoted to introduction with special emphasis on historical development of internet and various definitions in context of cyber law and crime along with position of cyber law in U.S., U.K., and Australia and other relevant and connected matters.

The Second chapter deals with Nature classification and various forms of cyber crime which are committed through computers and in which computer is used as a tool.

The Third chapter explains the various common cyber crimes being committed all over the world and various global concerns which are raising various legal and social issues. Special emphasis has been laid on the laws
of U.S. and U.K. in regard to offences of Hacking, Spamming, Cyber-Defamation, Obscenity and Fixing the liability of Internet Service providers.

Chapter Four of this study is taking into consideration the most important issue related to cybercrime i.e. issue of jurisdiction. A sincere effort is being made to explore the subject, which has assumed importance in modern times due to development of technology and above all when internet has become a household thing and various global issues and problem have became just the local issues.

In chapter Five international initiatives takes by various organizations and nations to combat cybercrimes is being depicted. The various conventions and conferences that laid the foundation of today’s cyberlaws at global level give a picture of the development of cyberlaws all over the world. No nation has been able to combat the menace of cybercrime by enacting only one single act. To achieve the aim and objective of combating cybercrime help and coordination of different statutes has been taken to bring the offence within the realms of legal sphere.

Chapter Six which forms an integral part of this research specially refers to Information Technology Act 2000 which is the only Act enacted by the Government of India to regulate and control the activities performed in cyberspace. Though the Act is a first step towards the end of cybercrime it can’t be said to be a complete Act in itself as it lacks perfectness. A critical analysis of the related
statutory provisions of the Information Technology Act 2000 touching various issues concerning e-governance, hacking, defamation, privacy and role of ISP's has been given.

The Controversy over Domain names that arose in Rediff Communication Ltd. Vs. Cyberbooth and another, and the judgment delivered by Mumbai High court has also been discussed in the present research study at appropriate place.

The last chapter deals with conclusion and suggestions of the study. It is hoped that the suggestion given in the last chapter of the present work will be taken care of by the legislature and courts in order to provide adequate protection to the net users through the medium of information Technology Act 2000.

Dated: