REGULATORY AND ENFORCEMENT ISSUES OF E-COMMERCE AND CYBER CRIME IN INDIAN CONTEXT

by

Madan Mohan Oberoi

Department of Management Studies

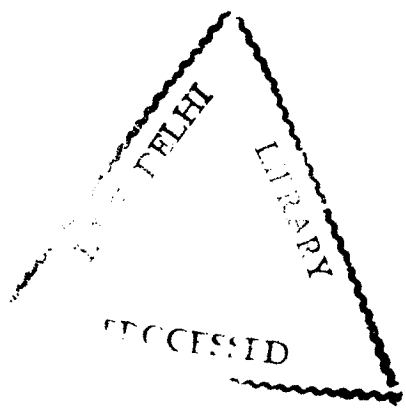
Submitted

in fulfillment of the requirements of the degree of Doctor of Philosophy

to the

Indian Institute of Technology, Delhi
Hauz Khas, New Delhi – 110016
India

April, 2002



Electronic commerce
E-commerce

CERTIFICATE

The Thesis entitled **Regulatory and Enforcement Issues of E-Commerce and Cyber Crime – in Indian Context**, being submitted by Mr. Madan Mohan Oberoi to the Indian Institute of Technology, Delhi, for the award of the degree of Doctor of Philosophy (Ph.D.) is a record of bonafide research work carried out by him. He has worked under our guidance and supervision, and has fulfilled the requirements for the submission of this thesis, which has attained the standard required for a Ph.D. degree of this institute. The results presented in this thesis have not been submitted elsewhere for the award of any degree or diploma.

(D.K. Banwet)
Professor
Department of Management Studies
Indian Institute of Technology
New Delhi.

(Surendra S. Yadav)
Professor
Department of Management Studies
Indian Institute of Technology
New Delhi.

ACKNOWLEDGEMENTS

It is my proud privilege to have worked with Professor D.K. Banwet and Dr. Surendra S. Yadav. I am deeply indebted to them for their initiation, constructive criticism and enlightening discussions. Their supervisory efforts and affectionate guidance have always served as a beacon light in my progress.

I am deeply obliged to all faculty members of the Department of Management Studies, IIT Delhi, who helped me in this research effort. I am especially grateful for the support and timely advice offered by Professor P.K Jain, Professor Sushil, Dr. M.P Gupta, Dr. Ravi Shankar and Dr. Kiran Momaya.

I am grateful to the members of the Expert Group, who spared their valuable time for providing useful insights and critical data to tackle this research effort.

I would like to express my gratitude to all the respondents of the survey, who took out time from their busy schedules to provide data for this research.

I would also like to express my sincere thanks to Dr. B.S Nagi for his help in data analysis and interpretation.

But for the constant support, help and advice of Dr. Neeraj and Dr. Pankaj, this research would not have seen the light of day, I express heartfelt thanks to them.

Words fail me at this juncture while expressing my profound sense of reverence and affection to my parents for their inspiration and constant encouragement. My wife

Monisha and daughter Manya deserve a special mention for their love, moral support and understanding.

Last but not the least, I am grateful to all my friends, well wishers and all those wonderful people who directly or indirectly contributed to this study.

Date: (Madan Mohan Oberoi)

ABSTRACT

The study aims to evolve a framework for developing regulatory enforcement policy related to e-commerce / cyber crime. It makes an attempt to identify and critically discuss various regulatory and enforcement issues concerning e-commerce and cyber crimes. The broad objectives of this study include comparative analysis of different cyber laws; examining the impact of various factors on growth of e-commerce and cyber crime; analysis of policy implications of electronic money; analysis of legal, social, economic, political and strategic policy implications of electronic commerce; identification of problems faced by law enforcement agencies in tackling cyber crime and steps to be taken to remove them.

A reasonably comprehensive survey of literature was done. It has been organized under five broad heads namely, e-commerce, cryptography concepts & issues, electronic money, cyber laws and cyber crime. Review of literature helped in identifying the issues. The important issues included uniform global cyber laws, security of electronic records, privacy of personal information, investigation of cyber crimes, intrinsic value of e-money, systemic and other risks of e-commerce and so on.

The principles of flexible systems methodology have been used for study design. The entire study design was divided in three parts namely exploratory, empirical and analysis & synthesis.

A matrix of cyber laws was prepared on 43 dimensions, using 12 cyber laws. Options Field Methodology was used to generate list of options for all 43 dimensions. Four case studies were also used. Indian IT Act was analyzed using options fields generated and the case studies.

The policy implications arising out of various issues concerning e- money were analyzed. The implications were analyzed from the point of view of four actors namely, government, banks, consumers, and law enforcement agencies. The major policy issues were identified as power to issue e-money, intrinsic value of e-money, systemic and other risks, control of monetary aggregates, liability of stolen / compromised e-cash.

Factors influencing growth of e-commerce and cyber crime were studied. Idea engineering workshop generated 40 variables influencing them. These were grouped in 10 broad factors using Interpretive Structural Modeling (ISM). An Interpretive Structural Model was also prepared for modeling the influence of these broad factors.

Exhaustive lists of legal, social, economic, political and strategic policy implications of E-Commerce were prepared from survey findings. These were analyzed in SAP paradigm from the point of view of the following major actors: Government, Enforcement Agencies, Judiciary, Legislature, and Business Organizations.

A survey was also conducted to find the perception of users (Business organizations, policy making bodies of government and enforcement agencies) of e-commerce about various regulatory / enforcement issues. The survey findings were also used to identify the problems being faced by enforcement agencies in investigating cyber crimes and solutions thereof.

The research study concluded with the discussion of significant contributions of the research, limitations of the work and scope for further research in the area.

TABLE OF CONTENTS

Abstract	**iii**
List of figures	**xi**
List of tables	**xiii**
List of appendices	**xviii**
Abbreviations	**xix**

Chapter 1		
Introduction to the Study		
1.1	Electronic Commerce	3
1.2	Cyber Crime	5
1.3	E-Commerce and Cyber Crime	7
1.4	Need of this Study	9
1.5	Aim & Objectives of the Study	12
1.6	Scope of the Study	13
1.7	Methodology of the study	13
1.8	Organization of the Thesis	15
1.9	Concluding Remarks	16

Chapter 2			
Literature Review			
2.1	Introduction		20
2.2	Basis of Present Review		20
2.3	E-Commerce		21
	2.3.1	Definition of E-Commerce	21
	2.3.2	Scope and Status of E-Commerce	23
	2.3.3	Secure E-Commerce	29
2.4	Cryptography Concepts and Issues		33
2.5	Electronic Money		43
2.6	Cyber Laws		47
2.7	Cyber Crime		52
2.8	Current State of Research		57
2.9	Limitations of Existing Approaches and Further Directions		59
2.10	Concluding Remarks		60

Chapter 3			
Study Design			
3.1	Introduction		63
3.2	Research Design		63
3.3	Flexible Research Design		64
3.4	Problem Conceptualization for the Present Study		66
	3.4.1	Issue Generation	66
	3.4.2	Issue Classification	69
	3.4.3	Classification Of Objectives	71
	3.4.4	Conceptual Model of the Research Problem	72
3.5	Fuzzy Clustering		76
3.6	Matching the attributes with the Techniques		78
3.7	Selection		81
3.8	Integration and Innovation		81
3.9	Implementation		85
3.10	Concluding Remarks		86

Chapter 4			
Cyber Laws			
4.1	Introduction		90
4.2	Methodology Used		91
	4.2.1	Options Field Methodology	91
	4.2.2	Study Design	94
4.3	Development of Options Field		97
	4.3.1	Purpose of the Act / Law	99
	4.3.2	Sphere of Application	100
	4.3.3	Interpretation	101
	4.3.4	Definition of Data Message / Electronic Record	101
	4.3.5	Definition of Electronic Data Interchange	102
	4.3.6	Definition of Originator, Addressee, Intermediary of Data Message	102
	4.3.7	Definition of Information System	103
	4.3.8	Definition of Asymmetric Cryptosystem and related terms of Public Key Infrastructure (PKI)	104
	4.3.9	Definition of Digital Signature	105
	4.3.10	Definition of Electronic Signature	106
	4.3.11	Definition of Security Procedure	106

	4.3.12	Definition of Trustworthy System	107
	4.3.13	Provisions to satisfy Legal requirements of Information to be in Writing	107
	4.3.14	Provisions to satisfy Legal requirements of Signatures	109
	4.3.15	Provisions to satisfy Legal requirements of information to be retained in Original Form	109
	4.3.16	Admissibility and evidential weight of data	110
	4.3.17	Provisions to satisfy Legal requirements of production of Document / information	111
	4.3.18	Provisions to satisfy Legal requirements of retention of Data Messages	112
	4.3.19	Formation and validity of contracts	113
	4.3.20	Recognition by parties of data messages	113
	4.3.21	Attribution of data messages	114
	4.3.22	Time and Place of dispatch and receipt of data	115
	4.3.23	Liability of Network Service providers	116
	4.3.24	Secure Electronic Record and Secure Electronic Signature	116
	4.3.25	Secure Digital Signatures / Acceptable Technologies	117
	4.3.26	Government Use Of Electronic Records & Sign	118
	4.3.27	Contents of a certificate	119
	4.3.28	Licensure and qualifications of Certification Authorities (CAs)	120
	4.3.29	Recognition of repositories	121
	4.3.30	Contents of a certification authority disclosure Record	122
	4.3.31	Duties of Certification Authorities (CAs)	123
	4.3.32	Duties of Subscribers	126
	4.3.33	General Duties Relating to Digital Signatures	128
	4.3.34	Regulation of Certification Authorities (CAs)	128
	4.3.35	Functions and Other Powers of Controller / Division	130
	4.3.36	Liability and Recommended reliance limits	132
	4.3.37	Protection of Personal Data	133
	4.3.38	Performance audits and investigations	134
	4.3.39	Offences & Penalties	135
	4.3.40	Investigation	136
	4.3.41	Adjudication	138
	4.3.42	Presumptions in adjudicating disputes	139
	4.3.43	Cyber Appellate Tribunal	140
4.4	Case Study Analysis		141
4.5	Information Technology Act of India		147
	4.5.1	Cyber Crime and Information Technology Act of India	150

	4.5.2	Investigation of Cyber Crimes and Information Technology Act of India	152
4.6	Concluding Remarks		156

Chapter 5			
Electronic Money			
5.1	Introduction		159
5.2	Methodology Used		160
5.3	Electronic Money		161
5.4	Policy Implications of Electronic Money		167
	5.4.1	Actors	168
	5.4.2	Government (Situation)	169
	5.4.3	Banks (Situation)	170
	5.4.4	Consumers (Situation)	174
	5.4.5	Law Enforcement Agencies (Situation)	177
	5.4.6	Policy Options	181
5.5	Analysis and Integration		188
5.6	Concluding Remarks		190

Chapter 6			
Growth of E-Commerce and Cyber Crime			
6.1	Introduction		193
6.2	Methodology Used		194
	6.2.1	Idea Engineering	195
	6.2.2	Interpretive Structural Modeling (ISM)	196
6.3	Variables affecting Growth of E-Commerce & Cyber Crime		202
6.4	Structuring of Variables affecting Growth of E-Commerce and Cyber Crime		204
6.5	Impact of various Factors on Growth of E-Commerce and Cyber Crime		209
6.6	Results and Discussion		213
6.7	Concluding Remarks		215

Chapter 7			
Implications of E-Commerce			
7.1	Introduction		218
7.2	Methodology Used		220
7.3	Legal / Security / Regulatory / Enforcement Implications of E-commerce		221
7.4	Social / Political Implications of E-Commerce		227
7.5	Economic / Strategic Policy Implications of E-Commerce		230
7.6	Concluding Remarks		236

Chapter 8			
Survey Findings and Analysis			
8.1	Introduction		239
8.2	Outline of the Survey		239
8.3	Background of Respondents		241
8.4	Growth of E-Commerce and Cyber Crime		244
	8.4.1	Factor Analysis for variables influencing growth of E-Commerce and Cyber Crime	247
	8.4.2	t-test of factors influencing growth of E-Commerce and Cyber Crime with background variables of respondents	253
8.5	Present status of factors influencing growth of E-Commerce in India		258
	8.5.1	Factor Analysis for present status of factors influencing growth of E-Commerce in India	260
	8.5.2	t-test of present status of factors influencing growth of E-Commerce in India with background variables of respondents	261
8.6	Comfort level of users of e-commerce for different transactions		264
8.7	Problems faced by Enforcement Agencies and the steps that should be taken to improve their capabilities		271
8.8	Opinion of Respondents about other regulatory / enforcement issues		274
	8.8.1	Opinion about Investigation Powers of Police	290
8.9	Correlates and Determinants		293
8.10	Concluding Remarks		304

Chapter 9			
Summary and Conclusion			
9.1	Introduction		307
9.2	Summary of the Learnings and Major Recommendations		307
9.3	Significant Research Contributions		312
	9.3.1	At Conceptual Level	312
	9.3.2	At Empirical Level	312
	9.3.3	At Methodological Level	313
9.4	Limitations of the Present Research		313
9.5	Suggestions for Further Research		314
9.6	Concluding Remarks		314

References	**316**
Appendices	
Curriculum Vitae	