

**Legal Issues of Electronic Commerce: A Survey of The
Emerging International and Indian Approaches to
Regulation of On-line Businesses**

Dissertation Submitted to
Jawaharlal Nehru University
In Partial fulfillment of the requirements for
the Award of the Degree of

Master of Philosophy

By
BIJU T.M.



International Legal Studies Division
Center for Studies in Diplomacy,
International Law and Economics,
School of International Studies,
Jawaharlal Nehru University,
New Delhi- 110067

2000



जवाहरलाल नेहरू विश्वविद्यालय
JAWAHARLAL NEHRU UNIVERSITY

NEW DELHI - 110 067

Centre for Studies in Diplomacy
International Law and Economics
School of International Studies.

July 21, 2000


CERTIFICATE

This is to certify that the dissertation entitled
**“Legal Issues of Electronic Commerce: A Survey of the
Emerging International and Indian Approaches to
Regulation of On-line Businesses”** submitted by **Biju T.M.**
in partial fulfillment of the requirements for the award of
the Degree of **Master of Philosophy** of this university has
not been submitted for any other degree of this university or
any other university and is his own work.

We recommend that this dissertation be placed
before the examiners for evaluation.


Prof. K.D. Kapoor

CHAIRPERSON


Prof. V. S. Mani

SUPERVISOR

To...

**Papa, Mummy,
Manju, Cinju & Ammamachi**

CONTENTS

	Page No.
Acknowledgements	i
List of Abbreviations	ii-iii
Glossary of Terms	iv-viii
Cases	ix-xii
Chapter I : Introduction	1-11
Chapter II : Principal Legal Issues	12-122
Chapter III : International Response to Regulating E-Commerce	123-154
Chapter IV : Indian Response to Regulating E-Commerce	155-171
Chapter V : Conclusion	172-181
Selected Bibliography	182-191

ACKNOWLEDGEMENT

The completion of this dissertation has been one of a learning experience, the values of which cannot be measure quantitatively. The efforts put up by me would not have been fruitful, if it were not for the people around me at all times.

No amount of gratitude can be sufficient for the valuable suggestions, patient hearings and persuasive guidance of Prof. V.S. Mani, which has gone a long way in shaping this dissertation. It is his generosity in granting excuses that made this dissertation possible.

I would like to express my sincere thanks to Prof. B.S. Chimmii, Prof.Y.K. Tyagi and Dr. Frank Bierman for their guidance during the course work and continuing support during my stay in the department.

Special thanks to Dr. Venayak Rao, Diplomacy Division and Dr. Girishankar, KLALC for their constant encouragement in my academic pursuit, in the field of technology law.

I am deeply indebted to Dr. R.C. Tripathi, Director, IPR Cell, Ministry of Information Technology (MIT), for providing me with research materials and also allowing me to use the MIT library.

I owe my gratitude to the librarians and staff of JNU, ISIL, INSDOC, UN, ACL, National Law School, Cochin University and MIT for their co-operation.

I am indebted to my friends and colleagues for their valuable suggestions and help. Special thanks to Prakash, Manu, Joshi, Pradeep, Ajish, Prabhakar and Manoj. Thank you Anbu for allowing me to use your computer. Words fail to mention the help provided by Abraham, Gopan, Shiju and Vimu, as they stood like guardian angels around me during the moments of crisis.

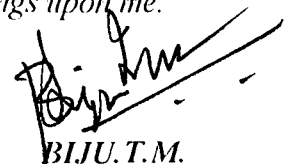
No amount of words will be able to express my gratitude towards my parents, who despite their financial troubles allow me to pursue my higher studies. I am grateful to Manju, Cinju and Sabi for their emotional support. I am indebted to Suma for her constant encouragement.

I specially thank Amar Singh for the timely execution of the work. His patience deserves a mention.

In the end, let me thank the Almighty for showering his abundant blessings upon me.

J.N.U.

21 July 2000



BIJU.T.M.

LIST OF ABBEVIATIONS

- EFT** = Electronic Fund Transfer
- B2B** = Business to Business
- C2C** = Customer to Customer
- G2G** = Government to Government
- B2G** = Business to Government
- G2C** = Government to Consumer
- EDI** = Electronic Data Exchange
- WWW** = World Wide Web
- IP** = Intellectual Property
- IPRs** = Intellectual Property Rights
- HTML** = Hyper Text Markup Language
- IMG** = Inline Links
- DMCA** = Digital Millennium Copyright Act, 1998
- OCILLA** = Online Copyright Infringement Liability Limitation Act, 1998
- SSL** = Secure Socket Layer
- SET** = Secure Electronic Transaction
- E-Cash** = Electronic Cash
- CPM** = Cost per Thousand Page Impression
- ASA** = Advertising Standards Authority
- ICC** = International Chamber of Commerce
- DPA** = U.K. Data Protection Act, 1998
- LINX** = London Internet Exchange List
- WIPO** = World Intellectual Property Organisation
- WTO** = World Trade Organisation
- UNCITRAL** = United Nations Commission on International Trade Laws
- DNS** = Domain Name System
- RAM** = Random Access Memory
- Kbps** = Kilo bytes per second
- AeBN** = Australian electronic Business Network
- VAN** = Value Added Networks
- URL** = Uniform Resource Locator
- OSP** = Online Service Provider

ISP = Internet Service Provider

TLDs = Top Level Domains

GTLDs = Generic Top Level Domains

ccTLDs = Country Code Top Level Domains

EU = European Union

ICANN = Internet Corporation for Assigned Names and Numbers

TRIPS = Trade Related Intellectual Property Rights

RTC = Religious Technology Center

CRAT = Cyber Regulation Appellate Tribunal

CRAC = Cyber Regulation Advisory Committee

E-commerce = Electronic Commerce

USA = United States of America

UK = United Kingdom

LIST OF ABBREVIATIONS AND GLOSSARY OF TERMS

Access provider	A company that sells Internet connection. Known variously as Internet access or service providers (IAPs or ISPs), e.g. Demon, CompuServe or America online.
Asymmetric cryptography	A remote computer, with publicly accessible file archives, that accepts 'anonymous' as the log-in name and e-mail address as the password.
Authentication	Authentication is the process of validating the identity of someone or something.
Bandwidth	The term used to describe the amount of data which can be sent over a telecommunications link to the Net. The higher the bandwidth, the faster data can flow.
BBS	Bulletin Board System. A computer system accessible by modem. Members can dial in and leave messages, send e-mail, play games, and trade files with other users.
Cryptographic algorithm	A cryptographic algorithm is a mathematical function that takes intelligible information (plain text) as input and changes it into unintelligible cipher text.
Cyberspace	A term coined by science fiction writer William Gibson, referring to the virtual world which exists within the marriage of computers, telecommunication networks, and digital media.
Database	A computerized filing system for storing, arranging and retrieving information.
DES	The Data Encryption Standard. A block algorithm that has been endorsed by both the U.S. National Institute for Standards and Technology (NIST) and the American National Standards Institute (ANSI) as providing adequate security for unclassified sensitive information.
Digital certificates	A digital certificate indicates the ownership of a public key by an individual or other entity. It allows verification of the claim that a given public key does in fact belong to from using a phoney key to impersonate someone else. In their simplest form digital certificates contain a public key and a name. More sophisticated versions also contain an expiration date, the name of the certifying authority that issues

the certificate, a serial number, and the digital signature of the certificate issuer. The most widely accepted format for certificated is defined by the X.509 international standard. Therefore certificated can be read or written by any application complying with X.509.

Digital Signature

A digital signature verifies the contents of a message and the identity of the signatory. It also provides a way of ensuring that a document was in fact sent by a particular sender. This feature is known as non-repudiation. So long as a secure cryptographic hash function is used to generate the digital signature, there is no way to extract someone's digital signature from one document and attach it to another, nor is it possible to alter a signed message in any way. The slightest change in a signed document will cause the digital signature verification process to fail.

Browser

A software programme, such as Netscape Communications or Microsoft's Internet Explorer, that allows you to read and **download** Web documents.

Bulletin board

One computer running software allowing multiple people to access the same information and to post information. Virtually all **bulletin boards** are text and graphics only, although they could become capable of displaying audiovisual works.

Chat room

A section of an online service where interactive textual communication occurs amongst a collection of people.

Click

People click on a mouse button to instruct the cursor on screen to activate something.

Cryptography

Cryptography is the science of keeping communications private. A central element of cryptography is encryption, which is the transformation of data into an unintelligible form. Encryption and decryption (the reverse of encryption) using computers require the use of some information, usually called a key. Some encryption systems use the same key to encrypt and decrypt (**Symmetric cryptography**), while others rely upon the two parties having different, but mathematically related keys (**Asymmetric cryptography**).

Host	Your host is the computer you contact to get on to the Net.
HTML	Hypertext mark-up language. The language used to create documents on the www.
HTTP	hypertext transfer protocol is the standard method of transferring HTML documents between browsers and Web servers .
Hypertext	Text where any word or phrase may be linked to another point in the same or another document. These links trigger other documents to be displayed.
Internet	A cooperatively run global collection of computer networks with a common addressing scheme: the TCP/IP protocols.
Intellectual Property	The legal rights which result from intellectual activity in the literary, artistic, industrial and scientific fields.
Intranet	The deployment of Internet technology inside an organisation which uses the Internet protocols. An intranet needs no connection to the global public Internet.
I.P.	Internet protocol. The most important protocol on which the Internet is based. It defines how packets of data get from source to destination.
Domain	A part of the Internet name that specifies certain details about the host such as its location and whether it is part of a commercial, governmental, or educational entity. The address is written as a series of names separated by full stops.
Download	The transfer of a file from one computer to another.
E-commerce	A broad term describing business activities with associated technical data that are conducted electronically.
E-mail	E-mail is a way of sending messages electronically to other people from your P.C.
E-mail address	The unique private Internet address to which your e-mail is sent. Takes the form of <u>user@host</u> .
Encryption	The mathematical processing of securing text or data by making it unintelligible to all but the intended

recipient Encryption is based on two components – a **Cryptographic algorithm** and a key.

Firewall	A collection of hardware and/or software components or a system that sits between the Internet and a network through which all traffic from inside to outside, and vice-versa, must pass through and which ensures that only authorised traffic, as defined by the local security policy, is allowed to pass through it. The firewall itself has to be immune to penetration.
Key generation	The creation of a key or a distinct pair of Public and Private keys.
Link	A connection between two items of hypertext .
Online	A network connection to another computer.
Packet	A unit of data. In data transfer, information is broken into packets, which then travel independently through the Net. An Internet packet contains the source and destination addresses, an identifier and the data segment.
ISDN	Integrated services network. A digital telephone network. ISDN can dramatically speed up transfer of information over the Internet or over a remote LAN connection, especially rich media like graphics, audio or video or applications. Typically an domestic ISDN line runs 128kb per second although far higher speeds are possible with commercial links.
ISP	Internet service provider. A company that sells access to the Internet and other online services.
Robot	A ‘crawler’ program that trawls the Web to update search databases such as InfoSeek and Lycos.
RSA	RSA is an Asymmetric cryptography cryptosystem for both encryption and authentication invented in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman. RSA’s system uses a matched pair of encryption and decryption keys, each performing a one-way transformation of data.
Search engine	A computer program that utilises key word identification to find websites and establish hypertext links to them.

Server	A central computer which provides multiple users simultaneous access to data and services.
SPAM	An inappropriate attempt to use a mailing list, or USENET or other networked communications facility as if it was a broadcast medium (which it is not) by sending the same message to a large number of people who did not ask for it. The term comes from a Monty Python sketch, which featured the word "spam" repeated over and over.
SET	The Secure Electronic Transactions (SET) protocol is being developed by a consortium including VISA, Mastercard, Microsoft, Netscape, IBM and others. It aims to establish a single technical standard for protecting credit card purchases made over the Internet.
SSL	Secure Sockets Layer: A protocol designed by Netscape Communications to enable encrypted, authenticated communications across the Internet. SSL is used mostly (but not exclusively) in communications between web browsers and web servers. URL's that begin with 'https' (rather than 'http') indicate that an SSL connection will be used.
Symmetric cryptography	An encryption/decryption system in which knowledge of the encryption key is equivalent to knowledge of the decryption key.
TCP/IP	Transmission control protocol/Internet protocol. The protocols that drive the Internet, regulating how information is transferred between computers.
URL	Uniform resource locator. The standard addressing system for the World Wide Web.
Web	The World Wide Web or WWW the generic terms for a network of graphic/hypermedia documents on the Internet that are interconnected through hypertext links.
Website	A collection of Web pages about a particular subject or organisation.
Web server	A computer on the Internet that stores Web pages and sends them to Web browsers .

Adams v. Lindsell. [(1818) 1 B & Aid. 681].

Adams v. Richardson & Staling Ltd. [(1969) 1.W.L.R. 1645].

Advent system Ltd. v. Unisys Corporation. [(1991) 925. F.2d 670, U.S. CA, Third Circle, LEXIS 2396].

Anheuser-Busch Inc v. Balducci Publications. [28 F 3d.769 8th cir 1994].

AOL v. LCDN. [(10 Nov 1998) (US District Court for the Eastern District of Virginia)].

Barclays Bank v. RBS Advanta [(1996) RPC307]

Bazak International co. v. Mast Industries Inc. [73 N.Y. 2d III, 7 UCC Rep. Serv. 2d 1380 (1989)].

Beatty v. First exploration Fund 1987 *and* Co. Ltd. partnership, [25 B.C.L.R. 2d 377 (1988)].

Beta Computers (Europe) Ltd v. Adobe Systems. [(Europe) Ltd. 1996 S.L.T. 604].

British Sugar v. James Robertson. [(1996) R PC 281].

British Telecommunications plc v. AT&T Communications (U.K.) Ltd. [18 December, 1996, unreported].

Brookfield Communications Inc v. West Court Entertainment Corporation. [<http://www.vcilp.org/Fed-ct/circuit/9th/opinions/9856918.htm>].

Byrne v. Van Tienhoven. [(1880) 5 CPD.44].

Carlil v. Carbollic Smoke Ball Co Ltd. [(1892) 2 Q B. 484].

Centaur communications (830 F.2d).

Clyburn v. All State. [826 F.Supp. 955 (D.S.C. 1993)].

Data Concepts Inc v. Digital Consulting Inc. [97-5802, 1998 Fed App. 0214P, 47 USPQ 2d 1672 (6th cir 5 November 1998)].

Derby & Co Ltd v Weldon. [(No. 9) (1991) 1 W.L.R. 652].

Deutsche Genossenschaftsbank v. Burnhope. [(1996), Lloyd's Rep. 113]

Dickinson v. Dodds. [(1874) 2. Ch.D. 463].

Dilbert Hack Page" case. [<http://www.cs.princeton.edu/~dwallach/dilbert/>].

Direct Line Group Ltd v. Direct Line Estate Agency. [(1907) FSR 374]

Dr. Seuss.[109 F 3d at 1405].

Duluth News-Tribune v. Mesabi Publishing Co. [(84 F 3d 1093 8th cn 1996)].

E. I. Du Port De Nemours Co. [476 F.2d 1357, 177 U.S.P.Q. 563, 567 (C.C.P.A 1973)]

Edwards v. Sky Words Ltd. [(1964) 1 W.L.R. 349].

Euro Dynamic Systems v. General Automation Ltd. [(1988) Q.B.D, September 6, unreported].

Fedthouse v. Brindley. [(1862) 11 C.B.N.S. 869].

Feist Publications Inc v. Rural Telephone Services Co. [499 U.S. 340 (1991)].

Fisher v. Bell. [(1961) 2Q.B.394].

Fonovisa Inc v. Cherry. [37USPQ 2d 1590, 1594 (9th cir 1996).]

Frank Music Corporation v. CompuServe Inc. [93 Civ. 8153 JFK (S.D.N.Y. 1993)]

Futuredontics Inc v. Applied Anagramatics. [No. 97-56711, 1998 US App (9th cir, 23 July 1998), case No. CV. 97-6991, ABC (manx), 1998 US dist (CD. cal. 30 January 1998)].

Goodman v. J. Eban Ltd. [(1954) 1. Q. 13. 550].

Grainger & Sons v. Gough. [(1896) AC. 325].

Harrods Ltd. v. U.K. Network Services Ltd. [High Court, Ch D. December 9, 1996].

Hasbro, v. Internet Entertainment group Inc. [No. C 96-3381 cw 1996 U.S. Dist. LEXIS 17020 (N.D. cal. Oct. 29, 1996)].

Household Fire Insurance Co. Ltd v. Grant. [(1879) 4 Ex. D. 216].

Howley v. Whopple. [(U.S.) 48. NH. 487 (1869)].

Hyde v. Wrench. [(1840) 3 Beav. 334].

Insituform Technologies Inc v. National Envirotech Group L.L.C. [Civil Action No. 97-2064 (E.D. La)].

Interfoto Picture Library Ltd v. Stiletto Visual Programmes Ltd. [(1989) Q.B.433, (1988), 1 All E.R. 348].

Intermatic Inc. v. Dennis Toeppen. [947 F. Supp. 1227 (ND 111 1996)].

J. Evans & Sons (Portsmouth) Ltd v. Andera Merzario Ltd. [(1976) 1 L.W.R. 1078].

Kohlmeyer & Co v. Bowen. [126 Ga. App. 700 192 S.E.2d. 400 (1972)].

Lane v. First Nat Bank of Boston. [687 F. supp. (DC Mass 1988)]

Luttges v. Sherwood. [(1895) 11 T.L.R. 233].

MAI Systems Corporation v. Peak Computer Inc. [991 F. 2d. 511 (9th cir. 1993)].

Malarkey Taylor v. Cellular Telecommunications Industry Association. [929 F. Supp. 473 (D.D.C.1996)].

Maritz Inc. v. Cybergold. [1996 US Dist Lexis 14977, 29 August 1996].

Mc Donalds Hamburgers Ltd v. Burger king U.K. [(1987) FSR 112].

Merchantile Union Guarantee Co v. Ball. [(1937) 3 All E.R.].

Metzke v. The May Department Stores. Co.[34 USPQ 2d. 1844, 1847 (WD Pa 1995)].

Microstar v. Forongen. [942 F. supp. 1312 (S.P. Cal 1996)].

Midway Manufacturing Co v. Arctic International Inc. [547 F. Supp. 999,216 U.S.P.Q. 413, (N.D. ill 1982)].

Miller v. Universal City Studios Inc. [650 F. 2d 1365, 1369 (5th cir 1981)];

Minnesota v. Granite Gate Resorts. [568 N.W. 2d. 715].

Mobil Oil Corporation v. Pegasus Petroleum Corporation. [818 F 2d 254,257-58 (2d cir 1987) 24].

MTV Networks v. Adam Currey. [867 F. supp. 202 (S.D.N.Y. 1994)].

Niton Corp. v. Radiation Monitoring Devices Inc. [(no. civ. A, 98-11629-REQ, 1998 WL 812685)].

Norman v. Ricketts. [(1886) 3 T.L.R. 182].

One in a Million Case. [(1998) FSR 265; (1998) Tr LR 333].

Oppedahl & Larson v. Advanced Concepts. [Civ. Act. No. 97-Z-1592, 1998 U.S. Dist. LEXIS 18359 (D.Colo. Feb. 6,1998), 1997 U.S. Dist. LEXIS 23105 (D.Colo. Dec. 19, 1997), 1997 U.S. Dist. LEXIS 23108 (D. Colo. Dec. 19, 1997)].

Panavision International LP v. Toeppen. [245 F. supp 1296, 1996 US Dist. LEXIS 19628 (CD cal. 1996), aff'd 1998 US App. LEXIS 7557, 98 Daily Journal DAR 3929 (9th cir. April 17, 1998)].

Parker v. South Eastern Railway Co. [(1877) 2 CPD 416].

Pharmaceutical Society of Great Britain v. Boot Cash Chemists (Southern) Ltd. [(1951) 2 Q. B. 795].

Pitman Training Ltd & PTC Oxford Ltd. v. Network Solutions U.K. Ltd & Pearson Professional Ltd. [No CH 1997 F 1984, (1997) FSR 797 (ch 22 May 1997)].

Playboy Enterprises Inc (PEI) v. Frena. [839 F. supp. 1552 (M.D. Fla 1993)].

Playboy Enterprises Inc v. Asia Focus International, Inc. [No. 97-734-A, 1998 U.S. Dist. LEXIS 10359 (E.D. Va. Feb. 2, 1998) (Mag. J.), adopted by 1998 U.S. Dist. LEXIS 10459 (E.D. Va. Apr. 10,1998)].

Playboy Enterprises Inc v. Calvin Designer Label. [985 F. Supp. 1220 (N.D. cal 1997)].

Playboy Enterprises Inc v. Webb World Inc. [986 F supp. 1171 (N.D. tax 1997)].

Playboy Enterprises. Inc v. Welles. [7 F. Supp. 2d 1098 (S.D. cal) aff'd, No. 98-55911, 1998, U.S. App. LEXIS 27739 (9th cir .oct.27,1998)].

Playboy v. Chukleberry Publishing. [937 F. Supp. 1032, 39 U.S.P.Q.2d. 1746 (S.D.N.Y. 1996)].

Polaroid Corporation v. Polaroid Electronic Corporation. [(287 f 2d. 492)].

Prince Plc v. Prince Sports Group Inc. [(1998) FSR 21 (ch 1997)].

Princeton Review Management Corp. v. Stanley H. Kaplan Education Center Ltd. [94 civ. 1604 (MGC) (S.D.N.Y. filed March 9, 1994)].

Pro CD v. Zeidenberg. [1996 U.S. LEXIS 167 (WD. Wisc 1996)].

Quill Corporation v. North Dakota *ex rel* Heitkamp. [50A U.S. 298 (1992)].

Ramsgate Victoria Hotel Co. v. Montefiore. [(1866) L.R.I. Erch.109].

Re a Debtor (No. 2021 of 1995)

Rediff Communication Ltd v. Cyberbooth and another. [AIR 2000, Bombay 27].

Religion Technology Centre (RTC) v. F.A.C.T. Net Inc. [901 F. supp. 1519 (D. col. 1995)].

Religious Technology Center (RTC) v. Net.com On-line Communications Services Inc. [907 F. supp. 1361 (N.D. cal 1995)].

Religious Technology Center v. Lerma [40U.S. PQ. 2d. 1569 (E.D. va. 1996)].

Religious Technology Center v. Netcom On-line Communication Services Inc [907 F Supp. 1361 (N.D. cal 1995)].

Routledge v. Grant. [(1828) 4. Bing. 653].

Saphena Computing Ltd v. Allied Collection Agencies Ltd. [(1995) F.S.R. 616].

Schelde Delta Shipping BV v. Astarte Shipping Ltd (The Pamela). [(1995) 2 Lloyds page. 249],

Sega Enterprises Ltd v. MAPHIA. [948 F. Supp. 923, 41 U.S.P.Q.2d. 1765 (N.D. Cal 1996)].

SG2 v. Brokat

Shea v. Reno. [(930 F. Supp. 916) at 929 (S.D.N.Y. 1996)]

Shetland Times Ltd v. Dr. Jonathan Wills and Zet News Ltd [<http://www.jmls.edu/cyber/cases/shetldl.html>].

Smith v. Lucas. [(1881) 18 Ch.D. 531-542].

Sony Corporation v. Universal City Studios. [464 U.S 435, 104 sct 774, 785 (1984)].

Southern Bell Tel & Tel v. Associated Telephone Directory Publishers. [756 F.2d. 801, 809 (11th cir 1985)].

St. Albans City and District council v. International Computers Ltd. [(1996) 4 All E.R. 481, (1995) F.S.R. 686].

State Farm Mutual Auto. Ins. Co v. Brock Hurst. [453 f. 2d. 533 (10th civ.1972)].

Stern Electronic Inc v. Kaufman. [669 F 2nd 852, 213 U.S.P.Q. 443 (2nd cir 1982)].

Stewart v. Abend [495 U.S. 207,220 (1990)].

Telerate Systems v. Carco. [689 F. Supp 221, 232 (S.D.N.Y. 1986)].

Thornton v. Shoe Lane Parking. [(1971) 2. Q.B. 163, (1971) All. E.R. 686].

Ticket Master Corporation v. Microsoft Corporation. [Civ No. 97-3055 (DPP). (C.D. cal.1997)].

Tinn v. Hoffman & Co. [(1872) 29 L.T. 271].

Two Pesos Inc v. Taco Cabana Inc. [505 U.S. 763, 112 S.Ct. 2753, 23 U.S.P.Q .2d. 1081 (1992)].

U.S v. Thomas. [(1996) Nos. 94-6648/6649 FED. App. 0032P (6th cir)].

Vodafone Group plc v. Orange Personal Communications Services Ltd. [(1997) 5 EIPR D-134].

Wagamama Ltd v. City Centre Restaurants plc and others. [(1995) FSR 713, I bid, Page 53].

Washington Post Company v. Total News Inc. [Case No. 97. civ 190 (pkl) (S.D.N.Y. 1997)].

Watson v. Tom Growney Equip. Rac. [721 P.2d. 1302 (N. H. 1986)].

Yahoo! Inc v. Akash Arora. [1997 PTC (19) 201].

Introduction

In 1993 the world of commerce as we knew it ended.¹ In that year, commerce discovered the World Wide Web, the region of the Internet and the rush was on to establish a presence of any kind on the web. Electronic commerce [hereinafter referred to as e-commerce] is the future of trade. E-commerce has expanded from the closed world of transactions among known business parties to encompass a complex web of different activities involving a large number of individuals, many of whom will never meet each other. This has implications for economic and social life and its development is ushering in a new era of fast pace global communications and trade. E-commerce has the potential to change fundamentally the way in which commercial transactions, the business of government, the delivery of services and a host of other interactions are conducted. The greatest change here has been the reduction of the factors of distance and time. Now, for producers and consumers, geographical boundaries are no longer significant. The world is awake to business twenty-four hours a day, seven days a week and through the year.

Earlier, a customer had to go to the store, locate the desired product, followed by bargaining or otherwise, placing the order and finally receiving the supply. The entire process could range from a few hours to weeks, depending on the product, quantity, quality and source of purchase.² But the entire shopping paradigm has changed due to the recent advances in three areas, namely, computer technology, telecommunications technology and Information technology³. These three areas are changing life in such a way that was beyond human imagination a few decades ago. Everything in today's world is electronised whether it be EDI [EDI-Electronic Data Interchange], books (e books-electronic books), funds (EFT-Electronic Fund Transfer), cash [Electronic cash or e-cash], mail [electronic mail or e-mail], or commerce [Electronic commerce or e-commerce]. E-commerce seems to be heralding a new era, which could redefine traditional trade. This revolution, facilitated by the Internet, has been fast engulfing the global business scenario at a tremendous pace. The spectacular growth of Amazon.com, Yahoo!, e-bay etc have demonstrated how quickly business environs can be changed and gives a powerful indication of the changes that are in store⁴.

¹ Micheal Chissick and Alistair Kelman *Electronic Commerce: Law and Practice*, (London, 1999), p. 3.

² Prof. Sanjeev Gupta and Shamea Gupta, "E commerce & You", *Paradigm*, vol. 3, No.1, Jan – June, (1999) pp. 145-153, at p. 145.

³ Gupta and Gupta, n. 2, p.

⁴ Lyndon Cerejo, "All Things e", *The Sunday Review*, 21 May 2000, p.6.

DEFINITION

The definition of e-commerce varies considerably depending upon the mode of transaction among the parties. Generally, e-commerce refers to all forms of commercial transactions involving organisations and individuals that are based upon the processing and transmission of digitised data. E-commerce refers generally to all forms of transactions relating to commercial activities, including both organisations and individuals that are based upon the processing and transmission of digitised data, including text, sound and visual images⁵. It encompasses many diverse activities including electronic fund transfer, electronic share trading, electronic bill of lading, online servicing, public procurement, direct consumer marketing and after-sales service. It involves products (consumer goods, specialised medical equipments), services (information services, financial/medical/legal services), traditional activities (health care, education) and new activities (virtual malls)⁶.

“Electronic commerce is the sharing of information using a wide variety of different electronic technologies between organizations doing business with one another: customers, suppliers, banks, carriers and government agencies. E-commerce also refers to the procedure, policies and strategies required to support the incorporation of these electronic messages into the business environment.”⁷

E-commerce business can be broadly divided into six types. They are Business to Consumer (B2C), Business to Business (B2B), Consumer to Consumer (C2C), Government to Government (G2G), Business to Government (B2G), Government to Consumer (G2C).

(1) Business to Consumer (B2C)

Business, in this sector, directly sells to the end consumer. The advantage is that although the per-customer volume of the transaction is low, the number of customers serviced is large. Examples are sites like Amazon.com, Rediff.com etc which set up shops on the web, takes orders from the customer through the net and delivers the products to them within a specified time period.

⁵ URL: <http://www.oecd.org>.

⁶ European Commission 1997; URL: <http://www.europa.eu.int>.

⁷ Phyllis. K.Sokol, *From EDI to Electronic Commerce*, (New York, 1994), page 247.

(2) Business to Business (B2B)

It serves transactions between business entities. For example, Intel sells its chips to other business firms that makes digital devices, motherboard etc and not to end-users. It serves a limited number of people but the turnover of many business-to-business sites is many times that of the most famous business to consumer sites.⁸

(3) Consumer to Consumer (C2C)

This segment does not form a large part of web-based commerce. Here one end user can sell any material to another through the web. The examples of such business are the auction sites like e-bay where if you have something to sell, you can get it listed and others can bid for it.

(4) Government to Government (G2G)

This area involves the transaction between two governments. This sector has not been developed properly. An example of G2G transaction is that of Singapore. Singapore has announced that all the exports and imports from Singapore will be electronically based from the year 2001.

(5) Business to Government (B2G)

Here businesses directly sell to governments. This area is to develop as most of the electronic commerce transaction, presently takes place among private parties only.

(6) Government to Consumer (G2C)

Citizens can directly do business with the government. This segment can happen in both ways. The U.K. Government is April 1999 announced that basic dealings between the government and citizens will be by e-mail by 2008.⁹

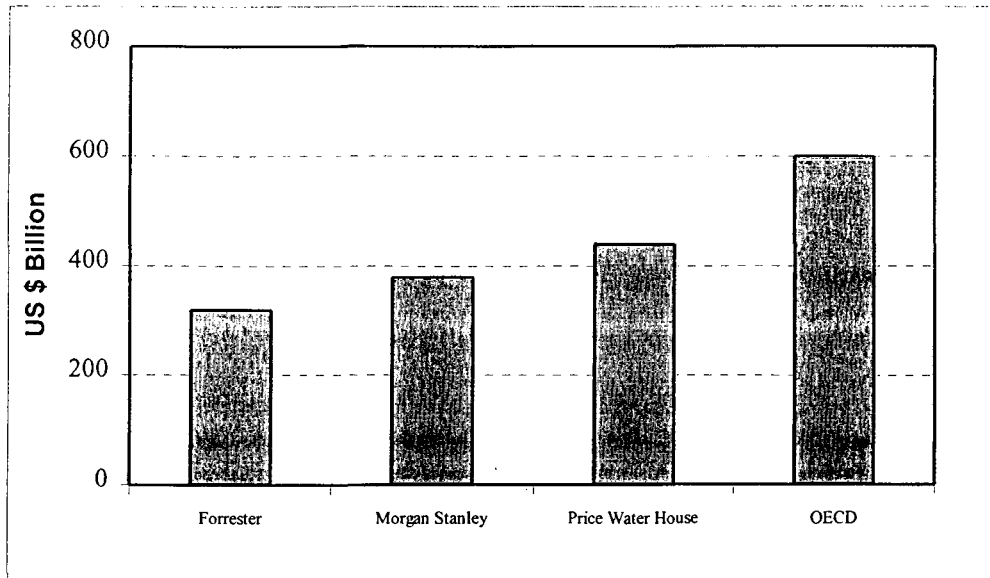
⁸ Forrester Research envisages that by 2003, online trade in the B2B sector will touch \$1.3 trillion, compared to just \$108 billion in B2B sector: Karnvir Mundry "To B2B or Not to B2B", *PC world*, February 2000, pp.102-106, at p.102.

⁹ <www.cabinet-office.gov.uk/moderngov/1999/whitepaper>.

IMPORTANCE OF STUDY

There are a number of reasons for the popularity of electronic commerce. Many of them suit the buyer and a lot suits the customer. The exponential growth of the e-commerce has been predicted in the recent studies conducted by various organisations.

Estimation of e-commerce revenue in 2001



Source: OECD, 1998

E-commerce primarily received the impetus for growth from factors like the globalisation of economy, commercialisation and privatisation of Internet, high labour cost and lesser available time, higher volumes of sales at lower profits, shorter product life cycles due to changes in technology, development of smart cards, Internet and the emergence of new field of Information technology¹⁰.

Electronic commerce will play a significant role in our economy in the years to come. Businesses will be able to improve efficiency, accuracy, reduce costs and provide faster, more reliable and more convenient services. With electronic interaction, companies are able to gather detailed information on the needs of each individual customer and automatically tailor products to those individual needs. E-commerce thus allows traditional supply chains to be shortened dramatically. Goods can be shipped directly to the end consumer by passing the warehouse and retail outlet. In case of products and services that can be delivered electronically like the software, the supply chain can be removed entirely. Middlemen will be reduced considerably.

¹⁰ Chissick and Kelman, n.1, p.1, Gupta and Gupta, n.2, p.146.

II. ADVANTAGES OF E-COMMERCE

For the consumer, the major advantage through e-commerce is the reduction in the price of articles and time saving. Through e-commerce, he can he can look for the lowest price offered for a particular product and competitive presence will lead to average price levels lower than those currently existing. Moreover e-commerce, Internet Banking and Interactive Banking allow the customers to monitor checking, savings, and credit and account availability, thus making the entire process of shopping on-line.

The virtue of having a Win-Win situation for both the customer and the supplier is another reason for the growth of e-commerce. This can be summed up by the following table: -

Opportunities for the buyer	Benefits for the customer
Global presence	Global choice
Improved competitiveness	Assured Quality of service
Mass customerisation	Personalised product & service
Shorter or elimination of supply chains	Rapid response to needs
Substantial cost savings	Substantial price reduction
Novel business opportunities	New products & services

Source: <http://www.cordis.lu/esprit/src/ecomint.htm>.

Doing business by e-commerce has many advantages over the traditional business, which has prompted many traditional business houses to establish their web presence also. This has been primarily due to the following reasons¹¹.

(1) Low set-up cost:

Anybody can easily set up a website. The starting point of most businesses is to develop a web page that contains basic information about the company, characteristics of

¹¹ These 14 reasons are compiled from Susan Singleton and Simon Halbster, *The Law, Business and the Internet*, (Great Britain, 1999), p.10; Chissick and Kelman, n.1, p.1; Gupta and Gupta, n.2, p.146.

the product including cost details. There is no need of large retail showrooms i.e. you do not have to start with heavy overhead costs.

(2) Faster and cheaper delivery of information:

Printed materials of business such as brochures, catalogues, new product information, etc can be reached to the customer as soon as they are put on the Internet i.e. advertising is fast and cheap.

(3) High degree of personalisation:

Getting information from customers about their likings and about their reaction against any product will help to adjust marketing strategy. Customer is the king.

(4) Improved customer services:

The web presence of a company acts as a customer service centre, which the customers can knock whenever they want. This helps the companies to assess the market response instantly and help further market penetration. The e-trader displays his products/services in the virtual market place, thus providing complete transparency to the customer.

(5) Global free market:

Nobody can easily dominate the global market because the presence on the Internet is easy not only for the global giants but even small organisations can participate actively at low costs and face upto stiff competition. Electronic commerce, the ultimate entrepreneurial vehicle, has a global audience used by artists in New Mexico to rug weavers in Morocco to basket makers in Botswana¹².

(6) Global access:

The worldwide web now has approximately 172 million¹³ users and is expected to double in the millennium. This massive audience is a positive reason for any business to go on line. The orders are going to pour from almost every part of the globe.

¹² Larry Irving, "No Heavy- Handed Regulation", *Telematics India*, Vol. , January 1998, p.70.

¹³ 172 million by the end of 2000, 223 by 2001, 282 by 2002, 300 by 2003, e Stats Report 1998, quoted in *Computer Today*, November 16-30,1999, p.58.

(7) Availability of Technology:

Since the same technology like that of web servers, browsers, search engines and Internet connectivity is used throughout the world, business can be easily conducted.

(8) Cheaper means of communication:

In some places, cost of making long distance telephone calls of extended duration can be very high. But the marginal cost of Internet based information comes less than international dialing.¹⁴

(9) Enhanced business to business links:

Using EDI to link suppliers to producers and seller gives companies a fuller picture of supply and demand and saves time and money by shortening the ordering cycle.

(10) Tough competition:

With more and more business entering the web export market everyday, your business has global competition. Along with a good hold of actual market, a strong web presence is required to have advantage over the competitors. E-commerce will be a great leveller. It is not a question of big companies competing with the small, but it is the race between fast versus slow.

(11) Multiple opportunities:

By use of e-commerce, multiple activities like selling, renting, purchasing etc can be performed. In fact a whole variety of transactions can be provided all under one roof.

(12) Lesser cost for the product:

The products being directly transported to the customers, the price added to the products like retailers commission, agents' commission, reduction in operating costs etc

¹⁴ For eg: Beamscope Canada Inc, transaction cost, got reduced from \$ 5, which is required to process a transaction via phone and fax to 50 cents for an online transaction; Mundrey, n. 8, p.102.

can be slashed to make the end product available to the customers almost near to the manufacturing cost.

(13) Speed and Accessibility:

E-mail can be delivered almost instantaneously and can be retrieved by the recipient from any where in the world, which makes it more advantageous than phone or fax.

(14) Environment friendly

Paperless world, being the basis of e-commerce, saves the destruction of trees, which makes the business practice environmentally perfect.

With electronic commerce, organisations are in the midst of a historic change – a transition from visible to electronic media¹⁵. Both the buyer and seller have nearly perfect information about goods and services being marketed. Entering and exiting market place are relatively easy for the buyer and seller. Buyers have substantial number of vendors to choose from and vendor will have greatly expanded market that is not geographically bound¹⁶.

For many businesses, there is no real choice as to whether or not to enter into e-commerce. Their competitors are doing so and to prevent their own customers from using the Internet to place orders or to find out about other businesses will result in a loss of sales. There is little to be gained by dwelling on perceived disadvantages. E-commerce is a reality, which businesses cannot ignore.

III. THE PROBLEM

E-commerce has created the largest possible market without maintaining a private network for sale, delivery and customer service. Clearly, the setting for e-commerce is different to that which existed for paper-based exchanges. Internet, the vehicle of e-commerce is inherently insecure and unreliable and so there is a need to safe, simple and secure mechanism for commercial transactions to make it more popular.

¹⁵ David O. Stephens, "Electronic Record Keeping Provision in International Laws", *Record Management Quarterly*, April 97, p. 72.

¹⁶ Robert A. Paterson, *Electronic Marketing and the consumers*, (New Delhi, 1997), p. 12.

This raises a number of legal issues and challenges, of both domestic and international significance.

There is a need for a well-defined legal and regulatory framework that is conducive to electronic commerce to facilitate e-commerce by removing the existing barriers. As global interaction is one of the main pillars of e-commerce, legal and regulatory framework must also have a global scope.

Anonymity, which is one of advantages of Internet, is also its main drawback. E-commerce poses threat of fraud, loss, insolvency, piracy and unchecked issues of electronic money. Laws are formulated to regulate the existing system. When a new situation arises, law has to bridge that gap too. The traditional business laws have now become obsolete with the advent of e-commerce. With the present legal system a wide variety of problems in cyberspace will remain unanswered.

Scientific and technological developments often give birth to certain issues, which are not addressed by the existing legal framework. In such a situation, laws are required to be remodelled so that they can properly fit into the newly created environment and thus prevent the law from becoming a stumbling block. This expected growth of e-commerce needs the support of a substantial legal regime specifying the rights, duties and obligations of all players like the buyer, the seller, the service provider, the bank etc, so that e-commerce can flourish according to its potential.

Daniel Greenwood, Deputy General Counsel for the Commonwealth of Massachusetts, U.S.A., sums up these tensions in this way:

“... When our civilisation had transition to the industrial age, our legal system did not adapt by the mere addition of a new word of “industrial law”. Rather, nearly every area of law was transformed by, and helped to create, the new economic, social and political realities associated with the industrial revolution and our subsequent industrial civilisation. Similarly, the pervasive information revolution will relegate many currently familiar concepts to irrelevant historical curiosities”¹⁷.

¹⁷ Electronic Signature and Records: Legal, Policy and Technical consideration, Appendix G to the statement by the legislative and policy working group of American Bar Association.
URL:<www.abanet.org/scitech/ec/isc/statecls.html>.

SCOPE OF STUDY

There are some technical and business related problems, which are required to be addressed when a topic like e-commerce is dealt with. But in the present research, emphasis has been given on some of the legal issues, which are likely to come up in case of e-commerce transactions. The principal issues have been selected for discussion. They are those relating to Contracts, Intellectual Property Rights concentrating on Copyrights and Trademarks, Payments and Advertisements.

Since most legal developments have taken place in countries like U.S. and UK, these countries constitute the ready reference and benchmark for the study of legal issues surrounding e-commerce. The Indian position is also referred to wherever necessary.

OBJECTIVE OF THE STUDY

The study in general seeks to analyse the effect of e-commerce on the existing legal framework. Chapter II analyses the difference between contract formation through the On-line media and the Electronic Data Interchange (EDI), the methods of contract formation in cyberspace, the problems arising out of these electronic contracts, difficulties due to electronic signatures and On-line terms and conditions during contract formation etc.

The section on Intellectual Property is restricted to the study on Copyright and Trademark violations in cyberspace. It deals with the various new types of Copyright violations like linking, framing, caching etc and how the courts of various countries have tried to regulate this practice. The U.S. congress has passed Digital Millennium Copyright Act, 1998 (DMCA) to deal with the various copyright violations in cyberspace. Various provisions of DMCA are discussed here. This part also discusses copyright violations in video games, multimedia works, database rights, data protection in Europe. The Indian laws are referred wherever necessary.

Trademarks issues, which have come to the fore with the advent of Internet commerce is discussed in the next part. The conflict between domain name and trademarks is discussed with relevant case laws. The trademark infringement due to practices like linking, framing, use of Meta tags, are also addressed in this section.

The section of Payments deals with the new type of payment, the electronic money or e-money. This section discusses the different types of payment protocols and the various types of payment mechanisms in the digital era. The new problems due to introduction of e-money like the integrity problem, counterfeiting, privacy issues, seignorage loss, crimes and tax evasions have been discussed in detail.

The section on advertisements enumerates the different areas, which the e-merchant has to be cautious when his advertisements are being disseminated to the entire world. New legal issues that have emerged due to mass advertising, primarily due to the violations of privacy rights are analysed in this section. Trademark violations that often arise in this area are discussed with relevant case laws.

The third chapter discusses the international attempts to regulate e-commerce. This chapter is divided into two sections where the first section discuss the work done by International bodies like UNCITRAL, WIPO and WTO. The second part analyses the UNCITRAL Model Law, the EU E-Commerce Directive. The Singapore Electronic Commerce Transaction Act, 1998 is also discussed as the Information Technology Act, 2000 is based on the Singapore E-Commerce Act.

The fourth chapter discusses e-commerce in the Indian context. The growth of e-commerce in India is discussed at the outset. India has recently enacted the Information Technology Act, 2000, which is studied in detail. The chapter ends with a suggestion as to what are laws to be amended in India for the smooth functioning and flourishing of e-commerce in India.

The present work comes to an end with a brief concluding remarks containing recommendations, suggested policy, principles and a note on tasks ahead.

Principal Legal Issues

E-commerce has opened a Pandora's box of troubles. Commerce has almost settled rules and regulations for dealing with traditional commerce. But Internet commerce or e-commerce has opened possibilities for both for the consumer and the seller in ways which has never been thought before. The e-trader now has the whole world thrown open to him as markets. The consumer too receives new advantages that were not available to him like instant delivery, lesser cost, wide variety of choices etc. This chapter discusses the effect of e-commerce in the area of Contracts, Copyright, Trademarks, Payments and Advertising. The various issues that have come to the fora in these areas as a result of e-commerce is explained in detail under respective sections.

CONTRACTS

Contract formation across the Internet has initiated a great deal of debate primarily due to two reasons.¹ Firstly from an obscure academic beginning, the Internet has revolutionized global communication environment and hence commercial entities are attempting to develop new business models to exploit the potential the Internet holds as an international trading medium.² The essentiality for such a viable international commercialisation model is predictable and enforceable method of contracting. Secondly, and much more importantly, the functioning of the Internet can and do pose many problems when looking at contract formation.

Contracting on-line can take place in three different ways.³ The first method is through the exchange of e-mails, together with the attachments explaining the detailed terms and conditions of the contract. The second method, known as web contracts, where the e-trader maintains a website, where he advertises his goods/services and a prospective subscriber can find out the details of sale from the website and then order by filling up the electronic forms in the website. The third is where the parties trade under the framework of EDI agreement which usually consists of linking the businesses using dedicated bespoke software and private value added network. While B2B e-commerce consists of all the above-mentioned three methods, B2C sector primarily make use of the first and the second method.

¹ Lars Davies, 'Contract Formation on Internet Shattering a Few Myths', in Edwards and Waelde ed. *Law and the Internet –Regulating Cyberspace*, (Oxford, 1997), p.97.

² Ibid.

³ Mahony, Chia and Savage, "E-contract" in Stephen York and Kenchia ed. *E-trader: A Guide to law of Electronic Business*, (London, 1999), p.45.

E-Commerce and Electronic Data Interchange (EDI)

Commercial entities have been using EDI⁴ for quite sometime. It is often used where these entities exchange similar information and concludes agreements frequently and where the process can readily be mechanised. These agreements, 'many of which follow a 'model' format are mutually accepted as overriding contracts that specify all issues pertaining to the future business relationship: On-line contract formation, attribution of risk, operation procedures, security, over-technical aspects such as the standard format of the data fields'.⁵ The explicit nature of the EDI is evident from the low number of litigations by the contracting parties. It can be said that the EDI has been a legal success.

Although many of the legal principles that have been considered in the context of EDI will be common to e-commerce, the application of these principles to e-commerce contracts will have a different result because of the following vital distinctions between them:⁶

- (1) EDI assumes that the commercial entities use a highly structured form of messaging with pre-defined fields and contents; contracting over the Internet usually involves free form of communications.
- (2) EDI assumes ongoing relationship and usually the parties have signed an inter change agreement setting out the basis of exchange; Internet trading is likely to involve a casual buying of goods or services with little or prior contract between the parties and no necessity for a continuing relationship.
- (3) EDI frequently has little human involvement as the communicating computers may exchange information automatically. Trading over the Internet usually involves the conscious act of the buyer, at least, in ordering the goods and services.

⁴ Graham J.H.Smith, *Internet Law and Regulation*, (London, 1998), p.207.

⁵ Michael Chissick, & Alistair Kelman, *Electronic Commerce: Law and Practice*, (London, 1999), p.53.

⁶ J.H.Smith, n.4, p.208.

- (4) EDI is likely to be carried out over a Value Added Network (VAN) with guarantees of services, quality and certainty as to the identity of carriers; the Internet cannot as yet provide either.
- (5) The trading partners in an EDI relationship are likely to be substantial commercial concern, whereas with the Internet, a commercial organisation will be more likely dealing with individuals.

This section does not purport to deal extensively with the contract law but to consider the application of some aspects of the Law of Contracts made over the Internet. It analyses on-line contract from its inception to completion and is classified into five parts, namely, subject matter of contracts, pre-contractual considerations, contract creation, writing and signature and on-line contract terms.

I On-line contracts

A contract is an agreement enforceable by law.⁷ Law allows contracts to be formed in any available manner-orally, by telephone, by written documents, by fax or by conduct of parties. 'The virtual or digital nature of the agreement theoretically presents no impediment to its recognition as some jurisdictions⁸ and UNCITRAL Model Law have offered specific legislations affirming their validity'.⁹

The UNCITRAL Model Law (Model law) states that in the context of contract formation, unless otherwise agreed by the parties, an offer and acceptance of an offer may be expressed by means of "data messages". Valid contracts can therefore, be formed where offer and acceptance are conveyed via Internet.

The Information Technology Act, 2000 (ITA)¹⁰ deals with the issues of validity of on-line contracts in the same way as the Model Law. Unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of "electronic records".

⁷ Section 2 (h), Indian Contract Act, 1872.

⁸ USA, UK, India, Japan, Germany, Ghana, Singapore, Malaysia, Canada, France, China, Brazil. 'E-Commerce: International Conclave', Seminar organised by FICCI on March 15, p. 28.

⁹ UNCITRAL Model Law 1996, Art 11(1), Chissick and Kelman, n.2, p.54.

¹⁰ Both the Houses of Parliament has passed the Act by voice vote. The government notification will be given on 15 August 2000.

Indian Contract Act, 1872, prescribes some contracts to be in writing. Therefore, it is possible that where the law does not prescribe contracts to be made in written form, contracts can be made in other forms. Oral contracts are valid thus and on-line contracts can also be subsumed under the rubric of other forms.

A. Types of on-line contracts

The subject matter of on-line contracts falls under three categories, namely goods, services and digitised services. The distinctions are important to on-line businesses when considering laws on consumer protection, implied terms and liability because many statutes define their scope based on whether a purchase is a good or a service.¹¹

1. Contracts for the sale of physical goods

Goods are defined as “all personal chattels other than things in action or money”.¹² This includes consumer goods such as toys, books, clothing etc. An electronic sale of goods usually involves ordering over the Internet and a shipment of the goods by post or courier to the purchaser. The goods supplied should be of promised type and quality.¹³ To determine this quality, the court considers whether the particular item was reasonably fit for its intended purpose, its price, defects and other relevant attributes.¹⁴

2. Contracts for supply of services and facilities

This would include on-line banking and other financial services, the giving of professional advice over the Internet and increasingly, the provision of voice telephony and potentially video conferencing. Service is where “the substance of the contract ... is that skill and labour have to be exercised”¹⁵ or where the contract between the supplier and consumer is unique in each case¹⁶. As to the quality of services expected, the provider of services needs only to perform the service with reasonable care and skill to the degree “expected of a professional man of ordinary competence and experience”.¹⁷

¹¹ Chissick and Kelman, n.5 p.54.

¹² Section 61 (1), Sales of Goods Act 1979 and Section 18, Supply of Goods and Service Act, 1982.

¹³ Section 14, Sales of Goods Act 1979.

¹⁴ Chissick and Kelman, n.5 p.54.

¹⁵ Robinson V. Graves (1935) 1 K.B. 579 at 587, quoted in Chissick and Kelman, n.5, p. 55.

¹⁶ As (in the United States) the case of contact lenses. Barbee v. Rogens. 425 SW2d 342 (1968), Ibid.

¹⁷ Chitty on Contracts, p. 13-24.

Law thus focuses more on the ability of the performer, not necessarily the end result of his/her actions.

3. *Contracts for the supply of digitised products*

These contracts involve the on-line supply of data such as software, text or multimedia products, often together with the granting of a licence of any copyright material comprising the products. The question concerning digitised services is whether they fall under the category of goods or services.¹⁸

In the Scottish case of *Beta computers (Europe) Ltd v. Adobe systems (Europe) Ltd*,¹⁹ the court regarded a contract for standard, non-customised software as *sui generis*. It observed:

“ It was not an order for the supply of disks as such. On the other hand, it was not an order for the supply of information as such. The subject of the contract was a complex product comprising the medium and the manifestation within it or on it of the intellectual property of the author”.²⁰

The UK Court of Appeal in *St. Albans City and District Council v. International Computers Ltd*,²¹ took the opposite view. Sir Iain Glidewell held that while a computer programme on a diskette clearly falls within the definition of ‘good’, computer programme *per se* did not:

“In both the U.K. Sale of Goods Act 1979, S. 61 and the U.K. Supply of Goods and Services Act 1982, S. 18, the definition of goods includes ‘all personal chattels other than things in action and money’. Clearly, a disk is within this definition. Equally clear, a programme, of itself, is not.”²²

This case has led to an illogical conclusion where identical digital products fell under different regimes merely because they were sold using a different medium. Computer programmes sold on a floppy diskette would be goods, whereas programmes transmitted directly via Internet or over the telecommunications system would constitute a service.

¹⁸ This is important to determine the terms implied to the contract and hence the standard of quality that these products will have to satisfy.

¹⁹ *Beta computers (Europe) Ltd V. Adobe systems (Europe) Ltd*. 1996 S.L.T. 604.

²⁰ I bid. at p. 608, quoted in Chissick and Kelman, n.5, p.56.

²¹ (1996) 4 All E.R. 481. First instance at (1995) F.S.R. 686.

²² (1996) 4 All E.R. at p. 493, quoted in Chissick and Kelman, n.5, p. 56.

This decision points out that the English courts will view digitised services as a dematerialised form of goods.²³

In *Advent system Ltd. V. Unisys Corporation*,²⁴ the US Court of Appeal for the Third Circuit reasoned that there were strong policy arguments for classifying mass-market software as goods. It remarked: -

“Computer programs are the product of intellectual process, but once implanted in a medium are widely distributed to computer owners. An analogy can be drawn to a compact disc recording of an orchestral retention. The music is produced by the artistry of musicians and in itself not a “good” but when transferred to a laser-readable disc becomes a readily merchantable commodity. Similarly when a Professor delivers a lecture, it is not a good, but, when transcribed as a book, it becomes a good.”²⁵

In *Howley v. Whopple*,²⁶ a US Court symbolically viewed the telegraph as a virtual pen of “copper wire a thousand miles long” and hence using a similar mental leap, Courts in future are likely to view digitised services as a virtual version of “goods” in order to maintain a consistent legal framework.²⁷

II Pre-Contract considerations

The culture of cyberspace encourages an attitude of ‘anything goes’ with the principal maxim being the *caveat emptor* (let the buyer beware). However, electronic commerce is just like any other form of commercial activity and is bound by the same regulations and legal principles regarding pre-contractual behaviour. Failure to observe these conditions can have a major impact on the performance and enforceability of subsequent contract.

The important pre-contractual considerations for on-line businesses are as follows:

A. Advertisement

In the context of goods and services, the advertising of which is regulated in other media, the advertiser will need to be aware of the extent to which the relevant regulations

²³ Chissick and kelman, n.5, p. 56.

²⁴ (1991), 925. F.2d 670, U.S. CA, Third circle, LEXIS 2396, cited in Chissick and Kelman, n.5, p. 56.

²⁵ Ibid at 675, quoted in Chissick and Kelman, n.5, p.56.

²⁶ *Heroley v. Whipple* (U.S.) 48. NH. 487 (1869), chissick and Kelman, n.5, p.57.

²⁷ Chissick and Kelman, n.5 p.57.

or restriction will apply to web pages or to goods or services offered via e-mail as they vary significantly among different jurisdictions.²⁸ The most common restriction relates to the identity of the recipient²⁹ or the information that must be imparted³⁰ or the industry specific rules.³¹ While advertising, the representations made have a significant impact in the formation of the contract. Hence pre-contractual claims or representations or terms must be carefully drafted.

Usually contracts are bilateral. However advertisements can create ‘unilateral’ contracts, where only the advertiser is bound by the terms.³² On-line advertisements need to be carefully drafted to ensure that customers and the courts interpret them as advertisements, not unilateral contracts. The advertisers can use disclaimers to emphasise that web advertisement is only an advertisement or an invitation to treat not an offer or unilateral contract.

(1) Express terms

One of the problems facing the e-trader is that sometimes the court may view the representations made prior to the contract creation as express terms³³ even though it was not detailed in the written contract. Such a scenario can occur in on-line contract as the court may find part of the contract in another e-mail or on a different web page despite their absence from the ‘actual’ contract written or otherwise. In addition, courts may also use, in the interest of justice, some statutory law³⁴ or the concept of collateral contracts to hold the on-line merchant liable.

²⁸ For example Germany has strict rules against comparative advertising in contrast to both U.K. and U.S. Example cited by Allan Williams, in International Conclave on e-commerce, conducted by FICCI, 28 February 2000, New Delhi.

²⁹ Age Restriction on advertising of alcohol or tobacco.

³⁰ Advertising of financial services, credits of shares.

³¹ Relating to tobacco, gambling, bookmaking etc.

³² *Carlil v. Carbolic Smoke Ball co. Ltd.* (1892) 2 Q B. 484.

³³ In *J. Evans & son (Portsmouth) Ltd v. Andera Merzario Ltd* (1976) 1 L.W.R. 1078 at 1083 the court held that “the court is entitled to look at and should look at all the evidences from start to finish in order to see what the bargain was struck between the parties” cited in Chissick and Kelman, n.5, p.59.

³⁴ Misrepresentation Act, 1967.

The moral to be learned is that if an on-line customer enters into a contract due to some misrepresentation made by electronic commerce business, the courts have many ways of holding the electronic commerce business responsible.³⁵

(2) Misrepresentations

Irrespective of their incorporation into the final contract, certain statements of either party made prior to the formation of a contract may constitute representations³⁶ which, if untrue can give right to damages and/or rescission, by the party to whom the representation is made. Thus untrue statements made in the web page or in an e-mail or else where in cyberspace about the quality of goods or services, may amount to misrepresentations.³⁷

A victim of misrepresentation may affirm the contract or seek remedy in courts and obtain damages and/or rescission of contract depending on whether the misrepresentation was made fraudulently, negligently or innocently.

B. Verifying identity of the customer

On-line “trader” does not want to sell goods or service to everyone on the Internet. Trade embargoes may block sales to particular countries³⁸ while local laws may prohibit sale of certain goods or content like tobacco, pornography etc. to minors. Although technical developments (e.g. Digital Signatures, Smart Cards etc.) may provide effective solutions in the future, presently the on-line businesses will have to resort to indirect methods for verifying identity and blocking web access from unwanted jurisdiction.

There are a host of reasons why on-line traders should regulate access to their sites and exclude users from unwanted jurisdictions. The consequences of carelessness in this area are not only potential embarrassment or difficult to-enforce contracts, but also possible civil and/or criminal liability.

³⁵ Chissick and Kelman, n.5, p.59, Section 36 of Monopolies and Restrictive Trade Practice Act (MRTP), 1969, will deal with unfair trade practices like this.

³⁶ A representation is a statement of fact (and not, generally opinion), which induces the recipient to enter into the contract concerned.

³⁷ Section 36 of MRTP Act, 1969 deals with this in India.

³⁸ Sales to countries like Iraq, Cuba, etc can be withheld due to trade embargos. For details see, Susan Singleton and Simon Halberstam, *Business, The Internet and the Law*, (Great Britain, 1999), p.165.

(1) Jurisdiction

There are a number of reasons why businesses will often want to limit the countries or jurisdictions with which they want to transact. They include export/import restrictions, commercial embarrassment, consumer protection legislation, illegal or regulated activity, on-line contract considerations and minors.

(a) Export/Import restrictions

An e-trader may restrict the sales to certain jurisdictions because certain products of dual use technology³⁹ are subjected to export restrictions to certain countries. Some jurisdictions have import restriction as certain items.⁴⁰ Hence the e-merchant may exclude these products from the respective jurisdictions.

(b) Commercial embarrassment

Even if not subjected to government regulations, some businesses may choose to avoid dealing with particular countries, for public relations reasons. Some businesses are unhappy about selling their goods to their competitors.⁴¹

(c) Consumer protection legislation

Many jurisdictions have consumer protection laws that imply mandatory terms into consumer contracts, some of which are surprisingly unfavourable to foreign merchants. On-line businesses wishing to avoid draconian legislations or foreign lawsuits may wish to refuse purchaser from some jurisdictions.

(d) Illegal or regulated activity

Some on-line content or activities such as financial services, gambling or pornography may be legal in some areas and illegal or subject to heavy regulation in others. Even without purposely directing activity towards a particular jurisdiction, some

³⁹ Encryption software for example is restricted in USA under Arms Export control Act [22U.S.C section 2751 (1994)] and International Traffic in Arms Regulations [22 U.S.C. 2778 (a) (1) (1994)] Daniel and Rua, " Cryptobabble: How Encryption Export Disputes are Shaping Free Speech for the New Millennium", *North Carolina J. of International Law and Commerce Regulations*, vol. 24, (1998) pp.138-139.

⁴⁰ There are import prohibition in Japan on Contraceptive pills. Cited in Singleton and Halbstern, n.38, p. 166.

⁴¹ Singleton and Halbstern, n.37, p. 156.

long arm statutes (often found in the United States) may seek to bring a website owner into a foreign court. Cases like *Minnesota v. Granite Gate Resorts*,⁴² *U.S v. Thomas*⁴³ can be cited as examples.

(e) On-line contract considerations

On-line advertisements need to be carefully constructed so that they are only invitations to treat, not offers. This gives the on-line business the option to accept or refuse dealing with particular customer after obtaining their specific details (location, age etc.) without raising the spectre of breach of contract.

(f) Minors

Minors (anyone under the age of 18) present two interesting problems to on-line merchants. First, the sale of certain goods and materials to minors, such as tobacco, alcohol and pornography, is unlawful. Second under English law, contracts made by minors for things other than necessities (food, clothing, shelter, etc.) are voidable⁴⁴ against the minor, but they are enforceable against the merchant.⁴⁵ Consequently, if litigation arises, it would cause formidable problems to an e-merchant to prove in his defence that the goods were necessities. The merchant who sells music CDs, on-line could always be at the receiving end. Furthermore, if a minor purchased goods from a merchant based in another jurisdiction, the risk of litigation becomes almost insignificant. What will happen when a child using a parent's credit or debit card without permission makes a contract? Such a situation results in two possibilities. Parents can incur the liability and okay the transaction. Secondly, if they are not willing, then the credit card or debit Card Company may sue the child for cheating.



X: (c



⁴² *Minnesota v. Granite Gate Resorts* 568 N.W. 2d. 715. A number of Minnesota residents accessed a Nevada website advertising a forthcoming international Internet gambling sites. Consequently, a Minnesota court claimed personal jurisdiction, stating that the defendants had "purposefully availed themselves of the privilege of conducting activities in (Minnesota). It should be noted that Granite Gate involved merely advertising, not even actual gambling activities. Cited in Chissick and Kelman, n.5, p. 61.

⁴³ [(1996) Nos. 94-6648/6649 FED. App. 0032P (6th cir)]. A Federal court in Tennessee claimed jurisdiction, applied local obscenity standards and convicted a website owner based in California even though there was a disclaimer to that effect. Cited in Chissick and Kelman, n.5, p. 61.

⁴⁴ *Merchandise Union Guarantee co v. Ball (1937) 3 All E.R.*. Cited in Chissick and Kelman, n.5, p.64.

⁴⁵ Section 2, Minors contract Act, 1987, which repealed the Infants Relief Act 1874.

TH- 7995

The e-trader can try to find out the jurisdiction of the customers using web server checks and site disclaimers. Although IP address contains the country of origin of the customer, it can be masked.⁴⁶ A web server can perform a simple check as a preliminary verifications although sever checks are not always fool proof, but they would be taken into account by any court when determining whether the e-trader was intending to sell its goods/services in the relevant localities. Site disclaimers can discourage unwanted customers by explicitly defining the intended audience. But, the disclaimers must be consistent with the site owner's claims.⁴⁷ Moreover even for using site disclaimers, there are some prescribed methods in various jurisdictions⁴⁸ and violating them will also cause serious trouble to e-trader.

(III) CONTRACT CREATION

Under both the English and the Indian law, the formation of a contract comprises of four elements: offer, acceptance, consideration and an intention to create legal obligation.

A. What constitutes an offer?

English law states that if a reasonable person would interpret a particular action or communication as an offer, it is an offer whether the party intended it or not.⁴⁹ Careless on-line statements can result in making unintentional offers to the world engendering unwanted binding legal contracts.⁵⁰ To protect from making unintentional offers, the on-line merchants should make it clear that the advertisement was only an invitation to treat.⁵¹

⁴⁶ IP addresses can be masked through a technique called 'weaving' where a user connect the website via a number of other computer, creating layers which hide his original location.

⁴⁷ In *Granite Gate case*, there was site disclaimer "consult with local authorities regarding restrictions". Even then the court held the company liable as it found that their subsequent action were a "clear effort to reach and seek potential profit from business consumers." *Minnesota v. Granite Gate Resorts* (568 N.W. 2d. 715)

⁴⁸ For e.g.: The French law states that a disclaimer to any customer in France should be in French language. Example cited by Allan Williams, at International Conclave on e-commerce, organised by FICCI, 28 February 2000, New Delhi.

⁴⁹ Chitty on contracts, 2-002.

⁵⁰ A typical example is, when Argos, the UK retailer, in September 1999, advertised to sell a 21 inch television which costed £299 for £2.99 on its website. Before the mistake was found out, in received orders worth £1million. Argos negated the contracts stating that it was only an invitation to offer. Quoted by Mahony, Chia, and Savage, n.3, p.45.

⁵¹ Chissick and Kelman, n.5, p. 67.

English law holds that shop displays and price lists are invitation to treat. In *Pharmaceutical Society of Great Britain v. Boots Cash Chemists (Southern) Ltd*,⁵² the British court held: -

“It is a well established principle that the mere exposure of goods for sale by a shopkeeper indicates to the public that he is willing to treat but does not amount to an offer to sell.... The customer is informed that he may himself pick up an article and bring it to the shopkeeper with a view to buying it and if, but only if, the shopkeeper then expresses his willingness to sell the contract for sale is completed.”⁵³

Similarly in *Fisher v. Bell*,⁵⁴ the UK court said: -

“It is clear that according to the ordinary law of contract, the display of an article with a price on it in a shop window is merely an invitation to treat. It is in no sense an offer for sale, the acceptance of which constitute a contract.”⁵⁵

A similar principle could be applied to electronic mail price lists: that websites are the electronic analogue of shop windows and catalogues, advertising the description of products and their prices. These analogies are still conjecture, since no case law has yet verified websites as invitation to treat.⁵⁶ In order to minimise the risk of an unfavourable decision, websites and e-mail solicitations should contain disclaimers explicitly stating them to be invitation to treat and not offers.

Construing the advertisements as invitations to treat is always legally good for the e-merchant for three reasons:⁵⁷

- (a) By retaining the power to accept or refuse, the e-businesses can refuse undesirable customers and jurisdictions without committing a breach of contract.
- (b) On-line merchants cannot accurately assess the number of replies he will receive in response to a solicitation⁵⁸.

⁵² *Pharmaceutical society of Great Britain v. Books cash chemists (Southern) Ltd* (1951) 2 Q. B. 795. Ibid.

⁵³ Ibid. at p. 801. Quoted in M. Chissick and Kelman, n.5, p. 67.

⁵⁴ *Fisher v. Bell* (1961) 2Q.B.394.

⁵⁵ Ibid. at P 399, quoted Chissick and Kelman, n. 5, p. 67.

⁵⁶ Chissick and Kelman, n. 5, p.67.

⁵⁷ Chissick and Kelman, n. 5, p. 68.

⁵⁸ One of the primary reasons why court introduced the principle of invitation is treat was to protect traditional businesses from supply shortages. In *Grainger & Sons v. Gough*, (1896) AC. 325 at 334, the court reasoned that “the transmission of price-list does not amount to an offer to supply

(c) Electronic mail can frequently become garbled due to transmission problems such as incompatible formats, changes in languages or keyboard sets or even firewalls. If the error cannot be traced, then the e-merchant becomes liable for contract breach. Hence ensuring that websites are invitation to treat and requiring the customer to make offer reduces this risk.

According to the Indian Contract Act 1872, the communication of an offer is complete when it comes to the knowledge of the person to whom it is made.⁵⁹ Therefore, in case of on-line contract, an on-line offer will be validly made only when the offer reaches the person to whom it is made.

Under the Model Law, the offer will be made at the time when the data message enters any information system designated by the offeree for the purpose, or, if no system is designated for the purpose, when the data message enters the information system of the offeree, or, if any information system has been designated, and the data message is sent to some other information system, when the offeree retrieves such data message.⁶⁰

(B) What amounts to acceptance of an offer?

In cyberspace, acceptance is a contentious issue because the offeror and offeree are distanced in time and space. Also whether it amounts to an offer depends on the character of an advertisement. If it is assumed that the website is an invitation to treat and that the customer response is an offer, it is the e-trader who accepts and forms the contract.

The primary issue in the context of acceptance in e-commerce transaction is whether the merchant's web server or computer accepts the offer and creates a contract. English law and most other legal systems, have a tradition of attributing the actions of machine to the person who instructs it to execute a particular routine.⁶¹

an unlimited quantity..... If it were so, the merchant might find himself involved in any number of contractual obligations to supply wine of a particular description which he would be quite unable to carry out, his stock of wine of that description being necessarily limited. Ibid.

⁵⁹ Section 4, Indian Contract Act, 1872.

⁶⁰ Article 11, UNICTRAL Model Law 1996.

⁶¹ Chissick and Kelman, n.5, p. 69.

In *Thornton v. Shoe Lane Parking*,⁶² the British court ruled that a customer contracted with a carpark machine when he fed in his money and received the claim ticket. As Denning, L.J., suggested,

“The customer was committed at the very moment when he put his money into the machine. The contract was concluded at that time. It can be translated into offer and acceptance, in this way: the offer is made when the proprietor of the machine holds it out as being ready to receive the money. The acceptance takes place when the customer puts his money into the slot.”⁶³

In a US case, *State Farm Mutual Auto. Ins. Co v. Brock Hurst*,⁶⁴ the court ruled that since the computer only operated as programmed by the insurance company, the latter was bound by the contract formed.

Based on these two precedents, it can be said that web-automated contracts are valid and hence need to be carefully constructed to prevent the creation of unwanted contracts. A properly constructed website should not allow the customer to alter the terms in the contract.⁶⁵ The customer should be presented with a contract of adhesion and can only click a button to send the offer.

According to the Indian Contract Act, 1872, when the person to whom the offer is made signifies his assent to it, the offer is considered accepted. The acceptance is binding on the offeror when the acceptance is outside the control of the offeree and binding on the offeree when the offeror receives the acceptance.⁶⁶

According to the Model Law, the acceptance is binding on the acceptor the moment it is out of his control, and on the offeror when he receives it.⁶⁷ This differs from the position under the Indian Contract Act.

⁶² (1971), All. E.R. 686, Ibid.

⁶³ Ibid. at P.689. Quoted in Chissick and Kelman, n. 5, p. 70.

⁶⁴ 453 f. 2d. 533 (10th civ.1972). Ibid.

⁶⁵ Use of technical solutions such as Hash Functions, Digital Signature can ensure message integrity and prevent this problem.

⁶⁶ Section Indian Contract Act 1872.

⁶⁷ Article 11, UNICTRAL Model Law, 1996.

1. Valid methods of acceptance

Acceptance is an unconditional agreement to the offer. Acceptance must be made in the manner specifically required by the offeror, but if no specification of the method for acceptance is made in the originating offer, acceptance may be any manner and by any medium reasonable in circumstances.⁶⁸ Determining what constitutes a reasonable response involves considerations of the speed and reliability of the medium, a prior course of dealing between the parties and usage of trade.⁶⁹ Accepting an offer by the same means by which it was originally communicated (or by a faster and more reliable method) should be sufficient,⁷⁰ unless the terms of the offer explicitly insist on a specified method. Contracts can even be accepted by a 'click-wrap'.⁷¹ Although English Courts have not yet dealt with click-wrap agreements, a United States District Court held them to be enforceable in America. Probably English courts will also recognise 'click-wrap' contracts.

Acceptance cannot be assumed from silence.⁷² For on-line contracts, since a product supplier will rigidly and elaborately specify all the terms in the offer, silence may be construed as acceptance because one might reasonably assume that the supplier will accept his own terms. As always, the best method of removing this risk is for a supplier to specify in the contract how he will communicate an acceptance.

2. Contract Creation

The instant of acceptance is the instant of contract creation. The location of acceptance plays a role in the law, jurisdiction and implied terms, which will apply to the contract. In the light of the postal rule⁷³ and the receipt rule,⁷⁴ where will electronic mail

⁶⁸ Raymond. T. Nimmer, "Electronic Contracting: Legal Issues", *Journal of computer and Information Technology*, vol. XIV, (1996), p. 215.

⁶⁹ Ibid.

⁷⁰ *Tinn v. Hoffman & co.* (1872) 29 L.T. 271, Chesire 51 quoted in Chissick and Kelman n. 5, p. 71.

⁷¹ Click-wrap contracts are those contracts which are entered into by clicking the 'I agree' or 'I Accept' columns provided in the website.

⁷² *Fedthouse v. Brindley* (1862) 11 C.B.N.S. 869, cited by Chissick and Kelman n. 5, p. 71.

⁷³ Postal rule was established in *Adams v. Lindsell* (1818) 1 B & Aid. 681. The rule states that when an acceptance is sent through the post, the contract is completed at the moment the letter accepting the offer is posted, even though it never reaches the destination. This rule places an unfair burden on the offeror primarily due to two reasons.

1. The offeror alone selects the method of communicating an acceptance. Hence the risk also should fall on him.
2. After the offeree post the letter, he cannot change his terms and conditions of acceptance. Hence the contract becomes complete at that point.

and web contracts be formed? What will be the time of receipt⁷⁵? No case law has decided this question yet, but looking at the attributes of both rules of communications may indicate what the courts might decide, if such a dispute should arise, as it inevitably will in the coming years.

(a) Electronic Mail

E-mails seem most suited for postal rule for at least three reasons.⁷⁶ Firstly, electronic mail is not instantaneous and the sender does not normally receive any immediate or continuous feedback concerning the delivery of the message.⁷⁷ Secondly, once the offeree clicks the 'send' button, his control over the message is terminated. Thirdly, the same issues of uncertainty for sending messages through the post apply to e-mail as well.

If electronic mail acceptance falls under the postal rule, on-line contracts would form at the instant the offeree sends the message. The place of formation of the contract depends on whether the solicitation by the merchant is an "offer or "invitation to offer."

On the other hand, reasons also exist for arguing that electronic mail acceptances are subject to the receipt rule.⁷⁸ Electronic mail is not as reliable as the post. In cyberspace, electronic mails can get lost, become garbled and are often rejected by firewalls.⁷⁹ Reduced reliability and increased risk of non-delivery place an undue burden on the offeror.

⁷⁴ Receipt rule is used in contract formation when parties form contract through continuous communication like telephone, telex etc. the contract is formed when the offeror hears the acceptance.

⁷⁵ In *Schelde Delta shipping BV v. Astarte Shipping Ltd (The Damelu)*. [(1995) 2 Lloyds page. 249], the court held that if an acceptance is sent outside of normal business terms, the time of receipt will be the time is which it is expected to the read is until the opening of business the next day. (In the present case, the court held that time of receipt is on Monday morning after the weekend), quoted in Chissick and Kelman, n. 5, p.73.

⁷⁶ Chissick and Kelman, n. 5, p. 73.

⁷⁷ After sending e-mail and receiving confirmation, sometimes we can find that the e-mail has been returned with the statement that 'the server could not be found' or 'the web page cannot be found.'

⁷⁸ Chissick and Kelman, n. 5, p. 73-74.

⁷⁹ Under the Postal rule, if the e-mail acceptance is lost in the post, the contract is still binding. (*Household Fire Insurance Co. Ltd v. Grant* (1879) 4 Ex. D. 216). Mahony, Chia and Masen, n. 3, p. 48, Chissick and Kelman, n. 5, p. 74.

If electronic mail does fall under the receipt rule, then the contract would form at the offeror's location.⁸⁰ However, a receipt rule for electronic mail raises a number of other thorny issues.⁸¹ But in determining the precise time of recipient the courts will likely to follow *Schelde Delta Shipping B.V. v. Astarta Shipping Ltd (the Pamela)*.⁸² When communication was sent by telex, fax etc. the question arises regarding the time of formation of the contract. Is it when the fax or telex is expected to be read or the actual time of receipt? The court in this case held that if an acceptance is sent outside the normal business hours, receipt is not effective until the opening of business the next day (or in the case of *Schelde*, on Monday morning after the weekend).

If the supplier wishes to retain the option of acceptance/refusal (the price lists being invitations to treat), the customer must necessarily be the offeror. Under the receipt rule, this arrangement necessitates that the contract forms in the customer's jurisdiction, where the customer receives the merchants' acceptance. On-line merchants thus face the unwelcome prospect of forming and enforcing contracts in scattered jurisdictions throughout the world.

Selecting and applying one of the existing acceptance rules to e-mail acceptances will continue to pose problems because e-mail has attributes found both in posting messages and in more instantaneous forms of communications. If and when disputes arise on this subject, the courts will have a difficult choice to make.

(b) Website Contracts

The World Wide Web (WWW) exhibits the features of method of instantaneous communication (interactive and in real time), the sender has almost immediate feedback and errors, faults are readily apparent on the face of the message. As a result, the receipt rule will probably apply to Web contracts. If the electronic commerce business retains

⁸⁰ The receipt here must logically mean that the offeror has been able to read the message, not simply that the offeror's computer has received the message. The receipt should be intelligible to the offeror. It should be in this form prescribed by the offeror, if such a form has been prescribed.

⁸¹ The issues like

- (a) Where does the receipt actually take place? Is it receipt when the acceptance arrives at the offeror. Mail server or when it is downloaded onto the computers or when the offeror reads it?
- (b) Whether a person has a 'continuous Internet connection' or a 'dial up' connection may also affect the time and location of receipt.

⁸² (1995) 2 Lloyd's Rep. 249, quoted in Chissick and Kelman, n. 5, p. 73.

the right to contract, the acceptance is effective until it reaches the customer, thus creating the contract in customers' jurisdiction, which is not welcomed by the on-line merchants.

Under English law, the receipt or postal rule only applies if the offer does not specify an explicit method of acceptance. Therefore e-trader can specify in the website catalogue that it is an invitation to offer and acceptance is effective once sent (postal rule). This arrangement would succeed in retaining the on-line traders' right to accept or refuse the customers offer, while ensuring that the contract is formed in the trader's jurisdiction.

Whether or not the court will decide that such favourable terms for the on-line electronic commerce businesses are unfair is an open question. It is likely to be contextual. In addition many jurisdictions have mandatory consumer protection laws that may run against this type of construction in consumer contracts.

3. Revocation of offer

Terms usually included in an offer determine the time during which the offer is effective. If the period of validity is not specified, the courts will imply that the offer lapses after a reasonable period. Determination of this reasonable period depends on factors such as the subject matter of the contract and the method of communication used by the parties.⁸³ In addition to the automatic lapsing of an offer, the offeror may revoke it at any time until the moment of acceptance, irrespective of any terms that specify the period in which the offer is valid.⁸⁴ A revocation must be received (receipt rule) before it is effective.⁸⁵

⁸³ *Ramsgate Victoria Hotel co. v. Montefiore* (1866) L.R.I. Erch.109, Chissick and Kelman, n. 5, p. 77.

⁸⁴ *Routledge v. Grant* (1828) 4. Bing. 653, *Dickinson v. Dodds* (1874) 2. ch.D. 463, Chissick and Kelman, n. 5, p.77.

⁸⁵ *Byrne v. Van Tienhoven.* (1880) 5 CPD.44, Ibid.

The e-trader should also mention valid methods for revocation of acceptance. Section 5 of the Indian Contract Act, 1872, states that a revocation of offer can be made at any time before the acceptance becomes binding on the offeror. Therefore, any revocation of offer has to be made before the acceptance is put into transmission to the offeror, after which the acceptance becomes binding on the offeror.

Under the provisions of the Model Law, the offeror is bound by an acceptance when he is in receipt of it. Therefore, if a revocation of the offer enters an information system outside the control of the offeror before he is in receipt of the acceptance, the revocation is binding on the offeror and no valid acceptance can be said to have been made.

4. Counter offer and Battle of Forms

Since an acceptance must be an unequivocal assent to all terms, if the “acceptance” contains additional or modified terms, it is a counter offer⁸⁶ and no contract is hence formed.⁸⁷ This counter offer scenario cannot happen in standardised web contracts but can certainly occur during electronic mail negotiation. Disputes involving “Battle of Forms”⁸⁸ can thus occur. Consequently, on-line business should protect them by prudently refraining from any action that might implicitly indicate acceptance of the other party’s terms and conditions.⁸⁹ Failing to observe this counter may result in being inadvertently bound to unfavourable terms.

C. Consideration

Consideration is often defined as the exchange of something of value but can include a detriment to the promisee or a benefit to the promisor. Consideration poses no threat to on-line contracts and electronic commerce.⁹⁰ The goods, services or digitised services provided by the on-line merchant and the payment given by the customer fully satisfy the requirement for consideration.

⁸⁶ In *Hyde v. Wrench* (1840) 3 Beav. 334, the court held that counteroffer necessarily means the rejection of the original offer. Ibid

⁸⁷ Mahony, Chia and Savage, n. 3, p. 46.

⁸⁸ Two parties trying to make a contract, where each party is trying to hold on to his own terms and conditions, which form the agreement, the situation arising is known as Battle of forms.

⁸⁹ Singleton and Halbstern, n. 38, p. 156, Mahony, Chia and Mason, n. 3, pp. 45-46.

⁹⁰ Different methods in which consideration can be made is mentioned in detail in the section on Payments.

Regarding contractual issues of payment, on-line vendors and customers should keep two legal principles in mind.⁹¹

In *Luttges v. Sherwood*,⁹² the UK court had held long ago that cash lost in the post constituted non-payment.⁹³ Applying this rule to cyberspace, digital cash that becomes ‘lost’ enroute the on-line merchant does not constitute payment either. If there is a fault in the line or server connection and subsequently the digital cash disappears, the customer is burdened with the loss. Besides an unscrupulous merchant could theoretically even keep the cash and deny ever having received it. In the future, customers in cyberspace may want two systems, anonymous digital cash for small transactions and privacy and traceable digital cash for larger transactions and accountability.⁹⁴

In *Norman v. Ricketts*,⁹⁵ the UK court had, on the other hand, suggested that if the contractual terms described a method of payment and the sender observed the specified procedures, the sender would not have liability for lost payment in traditional transactions. For the on-line merchant, the precedent gives a good reason to exercise caution in specifying payment method. Instead he can add a standard term, which denies liability for lost numbers and digital cash. Let the customer sent the payment at his/her own risk.

D. Intention to create legal relations

The final and core element of contract formation, namely, the intent to create legal relation, is also easily satisfied because in the context of electronic commerce, which typically involves commercial contracts, intent will normally be presumed to exist. The terms of the offer and acceptance will determine the commencement, duration and termination of the legal relations, as also the applicable disputes settlement methods, competent fora and procedures. The onus of proving otherwise “is on the party who asserts that no legal effect is intended, and the onus is a heavy one.”⁹⁶

⁹¹ Chissick and Kelman, n. 5, p. 99.

⁹² (1895) 11 T.L.R. 233, quoted in Chissick and Kelman, n. 5, p.99.

⁹³ Hence sending of payment is not like sending of an acceptance; the postal rule does not apply.

⁹⁴ Electronic Payment Mechanisms are dealt elsewhere in this chapter.

⁹⁵ (1886) 3 T.L.R. 182, quoted in Chissick and Kelman, n. 5, p. 99.

⁹⁶ *Edwards v. Sky words Ltd* (1964) 1 W.L.R. 349, at 355, cited in Chissick and Kelman, n. 5, p. 79.

IV. REQUIREMENTS OF WRITING & SIGNATURE

In most cases, English and Indian laws do not require a contract in written form or with signature. Only a few types of contract are specifically required by statute to be signed and in writing.⁹⁷ In the context of global electronic commerce, on-line businesses may need to comply with foreign requirements to ensure enforceability of their contracts. For example, in the United States, writing and signature are currently required for, *inter alia*, contracts for the sale of goods over \$ 500 and contract lasting over a year.⁹⁸

A. Writing

The Legislatures and Courts in different jurisdictions have been giving a liberal interpretation to the requirement of writing and signature to include digital version of both of these. For example, Civil Evidence Act, 1995⁹⁹, the Copyright, Designs and Patent Act, 1988¹⁰⁰ etc. define writing to include the digital form also. The UK court in *Derby & Co. Ltd. v Weldon*¹⁰¹ held that computer databases (files) are valid documents for purposes of recovery.

“ The data base, so far as it contains information capable of being retrieved and converted into readable form, is a document with in the meaning of R.S.C. ord. 24 of which discovery must be given.”¹⁰²

The United States has similarly attempted to construe writing to include digital form. The Uniform Commercial Code defines writing as “printing, typewriting or any other intentional reduction to tangible form.”¹⁰³ Similarly, other technological media such as

⁹⁷ For example, contracts for assignment of a Copyright [sec. 90 (3) of the Copyright, Designs and Patent Act, 1988], Regulated Consumer Credit Agreements [sec. 61 of Consumer Credit Act, 1974]; Contracts for Marine Insurance [sec. 22 of the Marine Insurance Act, 1906]; Contracts for the Sale or Disposition of Interests in Land [sec. 2 (1) of Law of Property (Miscellaneous provision) Act, 1989]; Contracts of Guarantee [sec. 4 of the Statute of Frauds, 1677], cited in Mahony, Chia and Mason, n. 3, p. 43.

⁹⁸ Jonathan Rosenoer, *Cyber Law: The Law of the Internet*, (New York, 1997), p. 237, Chissick and Kelman, n. 5, p. 81.

⁹⁹ The civil Evidence Act 1995 removed previous requirements that documents had to be original (in written form) in order to be admissible.

¹⁰⁰ Copyright, Designs and Patents Act, 1988, defines writing as including “any form of notation or code, whether by hand or otherwise and regardless of the method by which or medium in or on which, it is recorded.

¹⁰¹ (No. 9) (1991) 1 W.L.R. 652, cited in Chissick and Kelman, n. 5, p. 81.

¹⁰² Ibid at 654, quoted in Chissick and Kelman, n. 5, p. 81.

¹⁰³ U.S. Uniform commercial code S. 1-201 (46). Quoted in Rosenoer, n.98, p. 237.

telexes and faxes¹⁰⁴ were held to be writing in the U.S., culminating in this instructive opinion given in *Clyburn v. All State*:¹⁰⁵

“In today’s ‘paperless’ society of computer generated information, the court is not prepared, in the absence of some legislative provision or otherwise, to find that a computer floppy diskette would not constitute a ‘writing’ within the meaning of (the statute).”

B. Signature

A signature generally involves the writing of some name or identifying mark on the document accepting or authenticating it. The courts have also broadened the concept of signature. The English law definition of signature can be best summed up by referring to the decision in *‘Goodman v. J.Eban Ltd*,¹⁰⁶ where the court validated the use of a rubber stamp as a signature. Lord Evershed reasoned that:

“Where an Act of Parliament requires that any particular document be ‘signed’ by a person, then, *prima facie*, the requirement of the Act is satisfied, if the person himself places on the document an engraved representation of his signature by means of a rubber stamp..... the essential requirement of signing is the affixing in some way, whether by writing with a pen or pencil or by otherwise impressing upon the document, one’s name or signature “so as personally to authenticate the document.”

In *Re a Debtor* (No. 2021 of 1995) the court held that a faxed copy of a signature satisfied a relevant statutory requirement.¹⁰⁷ Laddie. J. held that:

“Once it is accepted that the close physical linkage of hand, pen and paper is not necessary for the form to be signed, it is difficult to see why some forms of non-human agency for impressing the mark on the paper should be acceptable while others are not.”

A signature represents the endorsement of a given document and whether it is written, typed or stamped makes no difference.¹⁰⁸ Courts consideration is largely based on the person’s intention to agree and to authenticate.

¹⁰⁴ *Bazak International co. v. Mast Industries Inc.* 73 N.Y. 2d III, 7 UCC Rep. Serv. 2d 1380 (1989). Chissick and Kelman, n.5, p.82.

¹⁰⁵ 826 F.Supp. 955 (D.S.C. 1993), quoted in Chissick and Kelman, n. 5, p. 82.

¹⁰⁶ (1954) 1. Q. 13. 550, cited in Ian Lloyd, ‘Legal Barriers to Electronic Contracts’ in Edwards and Waelde ed. *Law and the Internet: Regulating Cyberspace*, (Oxford, 1997), p. 141.

¹⁰⁷ *Ibid.*

1. Electronic Mail Signature and Web Signatures

How will the contracting parties sign on-line? Merely typing ones name at the end of an electronic mail will probably suffice, as long as there was an intention to authenticate. However, in the case of evidence, this does not equally weigh because a fraudster need only type another persons name or cut and paste over another signature file.¹⁰⁹ Web-based click wrap contracts, where clicking a button usually does acceptance. While actions like clicking a button can signify acceptance, they clearly do not satisfy definition of a signature being a name or an identifying mark.¹¹⁰ Furthermore, unlike in a traditional contract where all the terms are immediately visible, on-line documents often hide the contractual terms by providing a hyperlink. Thus recognising click-wrap contracts as signed contracts may create a system whereby people are unknowingly bound to serious contracts, a situation that the signature requirement was originally intended to prevent.

The United Nations Commission on International Trade Law (UNCITRAL)'s Model Law on Electronic commerce, 1996 has attempted to remove writing and signature requirements to promote electronic commerce. It first develops the concept of a 'data message', the electronic equivalent of a written document, which includes electronic mail, EDI,¹¹¹ telex etc. the Model Law reduces writing to its most essential legal property, i.e. permanence.¹¹² Articles 6 and 7, redefine the concepts of writing and signature to fit into the digital world.

Article 6 holds:

"Where the law requires information to be in writing, that requirement is met by a data message if the information contained there in is accessible so as to be usable for subsequent reference."¹¹³

¹⁰⁸ US cases have subscribed to a similar position, holding the validity of signature that are typed (*Watson v. Tom Growney Equip. Rac.* 721 P.2d. 1302 (N. H. 1986), represented by company letter heads. *Kohlmeyer & Co v. Bowen* 126 Ga. App. 700 192 S.E.2d. 400 (1972), and faxed (*Beatty v. First exploration Fund 1987 and Co. Limited partnership*, 25 B.C.L.R. 2d 377 (1988). Cited in Chissick and Kelman, n. 5, p. 83.

¹⁰⁹ Chissick and Kelman, n. 5, p. 83.

¹¹⁰ Chissick and Kelman, n.5, p. 84.

¹¹¹ Article 2(a), UNCITRAL Model Law on Electronic Commerce, 1996.

¹¹² Chissick and Kelman, n. 5, p. 85.

¹¹³ Article 6(1), UNCITRAL Model Law on Electronic commerce, 1996.

Similarly, the Model Law reduces signature to its essential property of endorsement or authentication.

“Where the law requires a signature of a person, that requirement is met relation to a data message if:

- (a) A method is used to identify that person and to indicate that persons approval of the information contained in the data message; and
- (b) That method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreements.¹¹⁴

The Model Law also verifies the enforceability of on-line contracts, providing that both offer and acceptance may be in the form of a data message and that contracts “shall not be denied validity or enforceability on the sole ground that a data message was used for the purpose”.¹¹⁵

One should note that most of the English precedents applicable to writing and signature are from the period before the advent of the computer and Internet. Whether the courts will extend their principles into digital age remains to be seen. Nevertheless, UNICTRAL’s Model Law represents a good base line and may hold some influence with the court, should a dispute over on-line contracts arise.

V. TERMS & CONDITIONS OF ON-LINE CONTRACTS

Most on-line contracts are not formed after lengthy discussion and negotiations over specific terms and clauses. Rather, they are generally standard form contracts called “contracts of adhesion”. Besides key issues, such as price and type/quality of goods or services, the terms in these contracts are not negotiated but are offered on a “take-it-or-leave-it” basis. The standard terms are pre-drafted by the trader to protect his interests, and the customer receives them only at the time of purchase, usually with neither time nor the desire to scrutinise them. Due to the global nature of electronic commerce, for contract formation the standard terms mentioned in the website should be reasonable and

¹¹⁴ Ibid Article 7(1).

¹¹⁵ Ibid Article 11 (1).

should not contradict statutory provisions existing in the country of business.¹¹⁶ Although complete review of this topic is not possible here, because many of the issues require detailed analysis, clauses like method of contract formation, choice of law, limitation of liability, jurisdiction etc. is discussed here.

A. Displaying contract terms on-line

The basic requirement is that the terms and conditions must be made known to the parties before they enter into an agreement.¹¹⁷ The terms and conditions in standard form contract will have no effect unless the customer is given 'notice' of them before the contract is formed.¹¹⁸ Merely displaying the terms somewhere may not be sufficient. For more onerous conditions, such as ones that deprive the customer of legal rights and remedies, English and Indian laws demand an even greater effort by the merchant to give notice. In *Thornton v. Shoe Lane Parking*¹¹⁹, which dealt with an exemption of liability for personal or bodily injury, Lord Denning M.R., held that:

“It [the exemption] is so wide and so destructive of rights that the court should not hold any man bound by it unless it drawn to his attention in the most explicit way In order to give sufficient notice, it would need to be printed in red ink with a red hand pointing to it -- or something equally startling.”¹²⁰

1. World Wide Web

On-line merchants have various means by which they can inform the customer of their standard terms and conditions.¹²¹ The structure of any website must be set so that the user has to at least see the terms before he has the chance to accept the offer.¹²² The different methods and their respective legal weightage are scrutinised below.

¹¹⁶ For e.g. Unfair Contract Terms Act, 1977 requires that the exclusion clauses in a contract should be research to in order to be enforceable.

¹¹⁷ Lars Davies, n. 1, p. 115.

¹¹⁸ Chitty on Contracts, 12-009.

¹¹⁹ (1971) 2. Q.B. 163, cited in Chissick and Kelman, n. 5, p. 87.

¹²⁰ Ibid at 170.

¹²¹ This is one of the problems affecting e-merchant. Too many legal clauses will make him safe but the website will be unattractive. He will have to balance legal requirements with the resulting attractiveness of their websites.

¹²² Lars Davies, n. 1, p. 116.

(a) Reference statement without hyperlink

Merchants could include a statement, such as “this contract is subject to company’s standard terms and conditions” at the bottom of the order form. While this small statement may be commercially attractive, it may fail the test of reasonable notice. For reasonable notice, the terms and conditions must not only be within the notice of the customer, but also be accessible to him for his perusal.

(b) Reference Statement with hyperlink

Reference statement could be linked to a page containing the standard terms and conditions. This technique is popular as it achieves some legal credibility without substantial digression from the commercial aspects. Legally this may satisfy the reasonable notice requirement for “usual terms”¹²³ but exclusion/limitations of liability clauses and other unusual terms should be incorporated on the order page or otherwise brought clearly to the customer’s attention.¹²⁴

Just because the terms are some how accessible does not mean that the user is induced to examine them. For example, in the U.S. case of *Microstar v. Forongen*¹²⁵ the court admonished the merchant for putting the restrictive terms in a separate, non-cross-referenced file that the customer did not necessarily have to view. For more onerous terms, such as long-term financial commitments, the hyperlink method is likely to be inadequate, if one applies Lord Denning’s example of using “red ink with a red hand pointing at it.” In *Interfoto Picture Library Ltd. v. Stiletto Visual Programmes Ltd.*,¹²⁶ the court ruled that the vendor had a duty to draw attention to particularly special surprising or onerous terms using boldface type or a separately attached note.¹²⁷

Hence e-commerce businesses using the hyperlinks to display terms should transfer the surprising terms and exclusion/limitation clauses off the “legal page” onto the actual order form.

¹²³ In *Parker v. South Eastern Railway co* [(1877) 2 CPD 416], a notice of ‘see back’ on the front of a railway ticket with terms and conditions on the back was held to be sufficient notice. This “see back” notice is strikingly similar to the hyperlink at the bottom of a web page. The case cited in Chissick and Kelman, n. 5, p. 88.

¹²⁴ Mahony, Chia and Manson, n. 3, p. 51.

¹²⁵ 942 F. supp. 1312 (S.P. Cal 1996). cited in Chissick and Kelman, n.5, p. 88.

¹²⁶ (1989) Q.B.433, (1988) 1. All E.R. 348, Ibid.

¹²⁷ In this case, the surprising term was a particularly harsh penalty clause for the late return of photographs.

(c) Display term at bottom of page

Instead of hyperlink the standard terms and conditions, the merchant could stream the whole text at the bottom of the order form or web page. Since the terms are capriciously displayed, this method has a greater legal weight in terms of notice.¹²⁸

(d) Dialogue box

The creation of a dialogue box forces the user to scroll through the terms and conditions before clicking “I Agree” or “I Accept” or “Submit”. The customer is not just given the opportunity to review the terms; indeed he/she is forced to review them and to agree through a positive action (i.e. click). The customer clearly realises that the contract is subject to certain terms and conditions.

2. Electronic Mail

To provide notice requirements in e-mail contracts, the e-trader should include the standard terms and conditions at the bottom of the e-mail offer (or invitation to treat). As seen already, terms such as “this contract is subject to the company’s standard terms and conditions” will not suffice. Similar is the case with placing terms in attachments¹²⁹ or hyperlinks.¹³⁰

B. Express, Implied and Mandatory terms

Properly drafted and displayed to the customer, expressly stated standard terms and conditions are useful devices for protecting the electronic commerce merchant’s best interests. Just as in the case of “traditional contracts”, on-line contracts are subjected to express, implied and mandatory terms. A proper understanding of their distinctive and the issues they raise is essential to any on-line merchant who wishes to construct enforceable on-line contracts to their advantage.

¹²⁸ But it can easily make the web page visually unattractive.

¹²⁹ Firewalls often remove electronic mail attachments, and thus the terms may not even accompany the electronic mail.

¹³⁰ Hyperlinks assume that the electronic mail program will support them and that the user has access to the World Wide Web, which will not be the case if a text only connection is being used.

1. Express terms

Express terms directly and explicitly specify on what terms the merchant wishes to conduct the business. Express terms can also specifically override any undesirable implied terms, protecting the merchant from unwanted liability or responsibility.¹³¹ As the e-trader is in the position to draft standard terms and conditions, he appears to have an inherent legal advantage. As a result, poorly drafted and ambiguous terms and conditions could result in judicial interpretation unfavourable to the on-line merchant. In case of vague or ambiguous terms, English law requires the courts to interpret the terms against the party who drafted them.¹³² The customer will receive the benefit of doubt. When courts interpret written contractual term, they focus almost exclusively on the outward appearances and meanings conveyed, not the actual underlying intention of the parties.¹³³ The House of Lords confirmed this doctrine in *Deutsche Genossenschaftsbank v. Burnhope*¹³⁴, stating:

“... The methodology is not to probe the real intention of the parties but to ascertain the contractual meaning of the relevant contextual language. Intention is determined by reference to expressed rather than actual intention.”¹³⁵

Express terms are also subjected to legal restrictions¹³⁶

2. Implied terms

Since the commercial world of cyberspace is not even a decade old, it has obviously not had the opportunity to develop well-recognised practices and customers. Also since the Internet environment is constantly changing, new and novel industry practices continually arise. What is the practice today may not be prevalent tomorrow. Many problems may arise when applying the traditional rules to cyberspace.¹³⁷ The

¹³¹ Mahony, Chia and Manson, n. 3, p. 58.

¹³² *Adams v. Richardson & Staling Ltd* (1969) 1.W.L.R. 1645. cited in Chissick and Kelman, n.5, p. 90.

¹³³ *Smith v. Lueas.* (1881) 18 Ch.D. 531-542. Ibid.

¹³⁴ (1996), Lloyd's Rep. 113, cited in Chissick and Kelman, n. 5, p. 90.

¹³⁵ Ibid at 122.

¹³⁶ For example, In England they are subject to Unfair Contract Terms Act, 1977.

¹³⁷ This is particularly true for digitized services. The question like whether software has to satisfy the implied requirement of satisfactory quality is yet to be answered completely. In *St Albans City and District Council v. International Computer Ltd* (1996) 4 All ER. 481, the court answered in affirmative. But the court was dealing with bespoke software and damages arising from it. What about commercial software downloaded as a digitized service? This is yet to be judicially considered.

environment is too new and untested for on-line merchants to rely on implied contractual terms. In almost all areas, either industry practice has not yet been well developed or accepted or the applicability of traditional customs and practices is unknown. The courts therefore have very little on which to base decisions except for the express terms found in the standard terms and conditions and perhaps, their own common sense. Consequently whenever any doubt exists, the electronic commerce business should wisely state its intentions in express terms.

3. Mandatory terms

Despite the apparent legal advantage given to electronic commerce businesses as the drafters of standard terms and conditions, they certainly do not have complete freedom. Parliament has imposed mandatory implied terms, which cannot be excluded, varied or limited in case of consumer protection legislation.¹³⁸ Many of the terms have arisen through the recent progress in consumer protection and almost all are felt to be so fundamental that to exclude them would be unfair or unreasonable.¹³⁹

Contract formation terms for formation of contracts

We have already identified above a few problem areas in respect of offer acceptance and formation of contracts. One of the principle areas requiring express term in an on-line contract is how the contract itself is formed. The “contract formation” clause of standard terms and conditions may encompass the entire contract formation process, including the following issues¹⁴⁰: -

- (1) What constitutes an offer, as opposed to an invitation to treat?
- (2) Whether counter offers are allowed, prohibition against customer-changed offer terms where there is automated computer acceptance.
- (3) If the merchant is making an offer, how long is an offer valid, what constitutes revocation of an offer and when is a revocation effective?

¹³⁸ Lars, Davies, n. 1, p. 117.

¹³⁹ For example one cannot avoid the mandatory terms found in the Unfair Contract Terms Act, 1977, like restriction of liability for personal injury or death resulting from negligence.

¹⁴⁰ Chissick and Kelman, n.5, p. 93.

- (4) What constitutes acceptance: how, by what method and exactly when an acceptance is effective (postal or receipt rule)? When can an acceptance be withdrawn?

D. Limitations & Exclusion of Liabilities

Using their standard terms and condition, electronic commerce businesses will try to exclude as much liability for errors and negligence as possible and limit or cap what cannot be excluded.

E. Warranties

Under the U.K. Sale of Goods Act 1979, any contracts for sale of goods has an implied warranty of “satisfactory quality” which takes into consideration the description price, and all other relevant circumstance of the sale.¹⁴¹ In contrast to goods, contracts for services have an implied term that the supplier will perform the service with reasonable care and skill. The essential difference between classifying a product as good or a service hinges on this distinction between satisfactory quality and performance with reasonable care and skill.¹⁴² For most part in electronic commerce, the traditional distinction between goods and services and the warranties those contracts imply will remain exactly the same.¹⁴³

However, one area that continues to pose problems for measurement of quality is digitised services particularly software. Regardless of whether software is judged to be a good or a service, determining standard for software quality poses a considerable challenge for the Courts especially in cases concerning bugs in software. In *Saphena Computing Ltd. v. Allied Collection Agencies Ltd.*,¹⁴⁴ the court held that software containing bugs were not a breach of satisfactory quality. The supplier was merely required to fix those bugs in due course. In *Euro Dynamic Systems v. General*

¹⁴¹ Sales of Goods Act 1979, section 14 (2A).

¹⁴² Supply of Goods and Service Act, 1982, see 13.

¹⁴³ Chissick and Kelman, n.5, p. 97. He reasons that “In order to maintain customer satisfaction and loyalty, most on-line businesses offer generous return and refund policies, just like their high street counterparts”. The on-line merchants have to follow the traditional statues like. The Unfair Contracts Terms Act 1977, the distance-selling directive, which makes the sentence a true one.

¹⁴⁴ (1995) F.S.R. 616, cited in Chissick and Kelman, n. 5, p. 98.

Automation Ltd,¹⁴⁵ the British court replicated the above position. But the court did not follow this leniency in *St. Albans v. ICL*,¹⁴⁶ where it awarded the plaintiff approximately £1 million in damages stemming from the consequences of a programming error that breached the requirement of satisfactory quality.

The U.S. Courts appear to measure software quality on case-by-case basis. The above cases involved bespoke software where the parties knew the level of quality expected and the purpose anticipated. The packaged software and other digitised services will be quite different in this respect. In due course, however, one might expect a legal distinction between personal use and business use, since errors in business application software can result in claims for greater damages. One might see digitised service providers in future restricting programmes for personal use only, or charging a premium for business use in order to cover the added, liability risk. If a premium is collected, that “business” version will naturally be held to a higher and more stringent standard.

This section has mentioned elaborately the important issues associated with on-line contract formation. One of the key areas not discussed was the problem that can arise when employees are allowed to enter into contract formation on behalf of the e-business. In order to remove the bureaucratic procedures in business and to save time, the employees will be sometimes authorised to enter into contracts on behalf of the enterprise. The question arising now is whether the employer will be liable for unauthorised contracts being entered into by his employee. Both under the English law and the United States law,¹⁴⁷ if an employee has the apparent authority to conclude a contract, the employer will normally be held liable, regardless of whether or not the employee had the authority to do so or not.

Hence to protect himself from the consequences of an unauthorised action of an employee, an employer is advised to take care of the following, measures:¹⁴⁸

- (1) The employer needs to establish clear policies stipulating what employees can do with Internet connections.

¹⁴⁵ (1988) Q.B.D, September 6, unreported, Ibid.

¹⁴⁶ (1996) 4 All E.R. 481, Ibid.

¹⁴⁷ 3 Am. Jur. 2d Agency section 71 (1986); Restatement (second) of Agency, section 8A (1958), quoted in Chissick and Kelman, n. 5, p. 66.

¹⁴⁸ Chissick and Kelman, n.5, p.66.

- (2) The authority may be established through providing symbols of authority like “signature tags” at the bottom of e-mails and other order forms.
- (3) The e-merchant should circulate among vendors a document setting out the true extent of the contractual authority granted to employees.
- (4) Employees should be educated and trained regarding the risk of business transaction.

COPYRIGHT

While there is sufficient body of law in India dealing with Intellectual Property (IP) there has been very little active development in the area of Internet related Intellectual property law. The main thrust of this part of the chapter will be the various approaches that the Indian legal system can adopt in resolving disputes involving intellectual property rights pertaining to cyberspace and thereby complement a comprehensive codification of cyberspace law. Also, it seeks to bring to focus the various legal issues that have emerged as a corollary to cyberspace dispute in the United States, the U.K. and Europe in this field. This would, hopefully, be a useful reference point for the emerging Indian law, as it is in these domains that one witnesses a profusion of computer and cyberspace related transactions.

Copyright law

Copyright is often referred to as a bundle of rights.¹⁴⁹ Under the United States copyright Act, the owner of the copyrighted work acquires certain rights *vis-à-vis* his work, including the exclusive right to

- (1) Reproduce the work.
- (2) Distribute the work.
- (3) Publicly perform the work.
- (4) Display the work.
- (5) Make any derivative work.¹⁵⁰

Sometimes different persons may own these rights. Accordingly it is important for the e-merchant to know;

- (1) Who owns all the rights or has all the required licences?
- (2) What right one has and is prepared to give a licence to?
- (3) What can one do if someone infringes one's rights?

¹⁴⁹ H.R. Rep. No 1476, 94 th Cong. 2d Sess 61 (1976). *Stewart v. Abend* [495 U.S. 207,220 (1990)]. Don W. Martens and Stacey R. Halpern, 'Intellectual Property Law in Cyberspace', Paper presented at International Chamber of Commerce Seminar on Cyber Law, New Delhi, 29 April 1997.

¹⁵⁰ U.S.C. sec 106.

No intent to infringe, needs to be proved for establishment of a direct copyright infringement. Moreover, a person can be held liable for the infringing conduct of another under either a vicarious or contributory principle.¹⁵¹ A party may be liable for contributory infringement if he/she has the knowledge of the infringing activities of another and induces or causes or materially contributes to that infringing conduct.¹⁵² In the case of vicarious infringement the wrongdoers are identified, if he/she supervises and controls the direct infringement and benefits from the infringement.¹⁵³

The Problem

The phenomenal growth of the Internet continues to create various new problems for the intellectual property community and subsequently leads to numerous lawsuits with seemingly conflicting decisions regarding copyright infringement in cyberspace. The intangible, digital nature of the cybertechnology makes the copyright infringement i.e. digital copies being downloaded, copied and instantly distributed all over the world, possible in a matter of seconds. This causes a great deal of concern for various jurisdictions as to how copyright checks can be implemented in this context. Gross violations occur in the cyberspace due to the misconception that everything on the web is in public domain and therefore its use would not violate or infringe copyrights. This view is further strengthened by another misconception that the law only protects those materials that display the proper copyright notice upon publication.¹⁵⁴

The fundamental issue of IPR that an e-merchant confronts in his dealings is the one pertaining to copyright. The copyright in the context is applicable to:

- (a) the text, graphics, computer programs and scripts, music files, animation and video clips which the e-merchant uses in his Web page,
- (b) the digital products that are electronically delivered by the e-merchant e.g.: information, software, articles, e-books, music, films, videos etc.,

¹⁵¹ *Sony Corporation v. Universal City Studios*, [464 U.S 435, 104 sct 774, 785 (1984)]. Ibid.

¹⁵² *Metzke v. The May Department Stores. Co.*[34 USPQ 2d. 1844, 1847 (WD Pa 1995)]; *Fonovisa Inc v. Cherry* [37USPQ 2d 1590, 1594 (9th cir 1996)]. Ibid.

¹⁵³ Ibid.

¹⁵⁴ Rahul Matthan; *Law Relating to Computers and the Internet*, (New Delhi, 2000), p. 300.

- (c) the 'works' carried on the physical goods supplied by the e-merchant and in any accompanying instruction manuals, software and packaging etc.¹⁵⁵

Works made by unknown authors whose identity cannot be ascertained by reasonable enquiry is also protected by copyright.¹⁵⁶ It is essential for the e-merchant to review carefully any material he uses, to make sure that it has the necessary rights before incorporating them in its website or its products.

It may be noted that other forms of reproductions are also indirectly protected by copyright. In case of an artistic work, the construction of a three dimensional copy from a two-dimensional work or a two dimensional copy from a three-dimensional work can be liable for legal action, if the e-merchant does not procure prior permission. In case of films, TV broadcasts or cable programmes, the infringement clause can be restored if the e-merchant unauthorisedly uses a substantial part of any image that forms a part of the programme. Even the uploading of still images and photographs from a programme onto a website needs the copyright owner's permission.¹⁵⁷

In cyberspace, it has to be noted that one act can often infringe more than one exclusive right of the copyright owner. For example, if the operator of site A makes an unauthorised copy of an article copyrighted and places it in site A's website, several of the copyright owner's exclusive rights may stand infringed. These may include the right to reproduce the work, the right to distribute the work and the right to display the work. In addition to these, if site A alters, albeit even slightly the contents of the work, it may become an infringement of the copyright owner's exclusive right to make derivative works.

A peculiar situation arises when site A simply hyperlinks to another site which has posted an unauthorised copy of the work. In this instance one can invoke copyright infringement liability, but who is the one to be held liable for the infringing conduct: the person who posted the work on the Internet; the company that runs or operates the website; or the company that acts as the access provider to the website?

¹⁵⁵ Harry Cohen and Kenchia, "E-Rights" in Stephen York and Kenchia (ed.) *"E-commerce: A guide to the law of electronic business"*, Butterworths, London, 1999 page 138.

¹⁵⁶ Ibid at 142.

¹⁵⁷ Ibid at a 144.

Depending on the particular circumstances, the answer to these questions can be in the affirmative.

The range of liability for copyright infringements in cyberspace can be categorised as follows:¹⁵⁸

- (1) Liability due to the posting or uploading of materials on the website.
- (2) Linking.
- (3) Inline links and Framing.
- (4) Caching.
- (5) Archiving.

(I) Liability due to the posting or uploading of materials on the Website

The decisions pertaining to this mode of infringement have been context specific. The court on the basis of the facts and circumstances of the individual cases has arrived at varying conclusions. Some courts have found liability where a person merely creates and manages a Bulletin Board Service (BBS) on to which infringing materials are posted by others without the knowledge of the BBS operator,¹⁵⁹ while others have required something more than mere creations of the forum in order to impose liability.¹⁶⁰ Also there have been instances where courts declined to find liability evoking the defence of fair use.¹⁶¹ Some of the case law that illustrates these varying judgments has been enumerated below.

***Playboy Enterprises Inc (PEI) v. Frena*¹⁶²**

Frena was operating a computer BBS to which subscribers uploaded and downloaded graphic files scanned from playboy's copyrighted magazines. PEI brought a copyright infringement action against Frena. The U.S. District Court found Frena liable even though he himself did not participate in downloading or uploading of files or even have the knowledge of the existence of files. The court held that

¹⁵⁸ Martens and Halpern, n. 149, pp. 3-24.

¹⁵⁹ *Playboy Enterprises Inc v. Frena*, [839 F. supp 1552 (M.D. Fla 1993)]. Ibid at p. 6.

¹⁶⁰ *Religious Technology Center v. Netcom on-line Communication Services Inc* [907 F Supp. 1361 (N.D. cal 1995)]. Ibid.

¹⁶¹ *Religious Technology Center v. F.A.C.T. NET, Inc.*, [901 F. supp 1519 (p.col. 1995)]; *Religious Technology Center v. Lerma* [40U.S. PQ. 2d. 1569 (E.D. va. 1996)]. Ibid at p. 12.

¹⁶² 839 F. supp. 1552 (M.D. Fla 1993).

Frena's intent was irrelevant and concluded that Frena was liable for supplying a product containing unauthorised copies of copyrighted works.

Religious Technology Center (RTC) v. Net.com On-line Communications Services Inc.¹⁶³

Netcom, the Internet Services Provider (ISP) Erlich, a Netcom subscriber and Klemesrud (BBS operator) were sued by RTC alleging copyright infringement. It was alleged that Erlich's posting RTC's copyrighted material on the bulletin board was illegal. The court held that Netcom and Klemesrud were not liable, as-

- (1) Neither of them had performed any affirmative conduct except for providing access to the Internet and thereby to the newsgroups on the BBS.¹⁶⁴
- (2) Since screening all the transmitted materials, is well nigh impossible, it can be concluded that Netcom lacked control over the information posted on the BBS.¹⁶⁵
- (3) Direct copyright infringement needs the presence of some element of volition or causation. This condition did not exist in the present case because Netcom was merely creating, storing, and transmitting copies of materials posted by third parties.¹⁶⁶
- (4) Also, Netcom was not vicariously liable for Erlich's conduct as it was receiving only a fixed fee and not a share of Erlich's profits.¹⁶⁷

Sega Enterprises Ltd v. MAPHIA¹⁶⁸

Sega sued the BBS operator who solicited the uploading and downloading of sega's copyrighted works on to the BBS. A permanent injunction was granted against the defendant. The court reasoned that the operator had provided direction and encouraged infringement knowingly. Also, he derived a profit *vis-à-vis* the subscribers from this arrangement.

¹⁶³ 907 F. supp. 1361 (N.D. cal 1995), cited in Martens and Halpern, n. 149, p. 6.

¹⁶⁴ Ibid at 1373.

¹⁶⁵ Ibid at 1372.

¹⁶⁶ Ibid at 1373.

¹⁶⁷ Ibid at 1374.

¹⁶⁸ 948 F. supp. 923 (N.D. cal 1996), citted in Martens and Halpern, n. 149, p. 8.

*Frank Music Corporation v. CompuServe Inc.*¹⁶⁹

The musical work publisher sued CompuServe for providing bulletin board service that allowed subscribers to upload and download copyrighted music. It was also alleged that CompuServe was a willing accomplice to the infringement in that it knew or should have known about the provision of these files. In defence CompuServe argued that it did not have any knowledge of the infringing materials and hence it was not liable; moreover the operation was done by a third party. The matter was settled with the payment of the required royalties to the music publishers for the music downloaded.¹⁷⁰

*Playboy Enterprises Inc v. Webb World Inc*¹⁷¹

Webb World operated a website ‘Neptics’ through which it offered adult images which could be downloaded by subscribers. PEI brought a copyright infringement action against the operator of the website infringement action against the operator of the website and two other persons alleging that some of Playboys copyrighted materials were unauthorisidely sold to the site’s subscribers. Unlike in the earlier case of *RTC v. Netcom*, the court held that Webb World was not an “information conduit” as was Netcom.¹⁷² The court reasoned that

- (1) Webb World was not an Internet service or Internet access provider and it was paid to make the images available.
- (2) Although Webb World may have had no control over subscribers who post images, it did have control over the images that Webb world itself placed on its website.

The Court granted partial summary judgment for direct infringement. The court upheld the Playboy’s claim of vicarious infringement¹⁷³ against the site’s operator because it found that the two operators had the right and ability to control what occurred on the site and had a financial interest in the site. The court held that

¹⁶⁹ 93 Civ. 8153 JFK (S.D.N.Y. 1993), quoted in Martens and Halpern, n. 149, p. 9.

¹⁷⁰ *Wall Street Journal*, Nov. 8, 1995, at p. B 11.

¹⁷¹ 986 F supp. 1171 (N.D. tax 1997). cited in Martens and Halpern, n. 149, p. 9.

¹⁷² *Ibid* at 1175.

¹⁷³ *Ibid* at 1177.

vicarious copyright infringement arose where a defendant “has a direct financial interest in the infringing activity and the right and ability to supervise the activity”.¹⁷⁴

From this case it can be deduced that guidelines regarding the types of materials allowable on a site and the liability for the violation of those very guidelines should be explicitly posted on the website by the provider, the operator and the managers of the website. Also precise policies for removing possible infringing of contents should be provided.

(II) LINKING

The web is a system of hypertext links, which enables the browser to skip from one document to another by clicking on a high-lightened part of the document.¹⁷⁵ These links are established with the help of Hypertext Mark Up Language (HTML) which allows the connecting of one website to another.¹⁷⁶ When the link is clicked, the users browser establishes a connection directly to the targeted site. The procurement of the target page from the new site is in a way problematic because it would appear though the user had typed in the URL on his screen to go directly to the site. Through hyperlinks, a user can move seamlessly between documents, regardless of their location.¹⁷⁷

The web has flourished precisely because a web page author can create links, which point to documents on any other site, whether or not he has the authority to look into various independent websites. In this context, it is often asked as to whether the proprietor of a site has any right to control linkages to his site. This is not necessarily, and primarily, a question of copyright. There could be the issue of trademark or passing off question or as is evident in some countries, the question of moral rights and unfair competition aspects.

To explicate further, let us take the following situation. When site A contains a hyperlink to site B, the link itself is generally the URL or title of sites B’s site.¹⁷⁸ A URL is comparable to an address or a telephone, which is not protectable under U.S.

¹⁷⁴ Ibid at 1176 at 1177.

¹⁷⁵ C. Shipley & M. Fish, *How the World Wide Web works*, (New York, 1996), pp. 27-33.

¹⁷⁶ Microsoft Press Computer Dictionary at [238, 240 (3rd ed. 1997)].

¹⁷⁷ *Shea v. Reno*, [(930 F. supp. 916) at 929 (S.D.N.Y. 1996)]. cited in Martens and Halpern, n. 149, p. 14.

copyright law.¹⁷⁹ So the reproduction of site B's URL on site A is not an infringement. Similarly, if the hyperlink on site A in site B's name, instead of its URL, the hyperlink would still not give rise to copyright protection, since short titles or phrases are typically non copyrightable.¹⁸⁰

However, there have been a few recent judgements, which bring us to the conclusion that linking in certain circumstances may result in copyright infringement.

MAI Systems Corporation v. Peak Computer, Inc¹⁸¹

This is a case that could be broadly interpreted to impose copyright liability with respect to hyperlinks. When an Internet user clicks on a hyperlink found on site A, which takes him/her to site B, the user's computer will copy site B to the computers memory. In such a case, site A could be found liable for contributory infringement. However since the user would create a copy of site B on his/her RAM (Random Access Memory). Whether it is linked to site B from site A has arguably given consent to the copying.

Shetland Times Ltd v. Dr. Jonathan Wills and Zet News Ltd¹⁸²

Shetland Times and Shetland News, are web-based newspapers. The Shetland Times homepage consisted of Newspaper's "frontpage" which listed a number of news headlines and these headlines were in turn linked to the corresponding articles. The front page of the Shetland News website consisted of reproduction of the headlines appearing on the Shetland Times website and these headings were directly linked to the corresponding articles in the Shetland Times. Hence, when the viewer clicked on the Shetland News headings, he was directly taken to the Shetland Times articles by bypassing the homepage. The Scottish Court held that there is a gross copyright violation as copyrighted articles were unauthorisedly sent through the defendant's site. The court added that the conduct of Shetland News also violated the various clauses of Scottish Copyright Designs and Patent Act because the hyperlinks allowed the visitors to bypass the Shetland Times homepage, on which its sponsors

¹⁷⁸ Shipley and Fish n. 175, at pp. 34-35.

¹⁷⁹ 17. U.S.C. section 102 (b); *Feist Publications Inc v. Rural Telephone services co.* [499 U.S. 340 (1991)]. cited in Martens and Halpern, n. 149, p. 16.

¹⁸⁰ 17. U.S.C. section 103, 17. U.S.C. section 101.

¹⁸¹ 991 F. 2d. 511 (9th cir. 1993). cited in Martens and Halpern, n. 149, p. 15.

advertised. The Court determined that the Shetland News's reproduction of the headlines on the Shetland Times site also constituted copyright infringement due to the length of the headlines.

Under the U.S. law it is not clear as to whether the process of hyper linking to an internal page would create liability for copyright infringement unless the text of the headlines which the Shetland News used as hyperlinks was independently copyrightable. In such a situation, it may give rise to trademark infringement liability and liability for passing off or misappropriation.

(III) INLINE LINKS & FRAMING

Inline links (IMG) cause an image from any location within a site (site A) or from another site (Site B) to be "seen" by the viewer of site A, as if the materials were located on site A, from where the viewer is accessing.¹⁸³ If an IMG link retrieves an image from file stored on site B, it will be incorporated into site A without any acknowledgement that the image come from site B.¹⁸⁴

"Dilbert Hack Page" case¹⁸⁵

Dan Wallach created a webpage named Dilbert Hack Page in his website which had an inline link to the daily Dilbert comic strip United Media, the company which controlled the copyrights to the Dilbert comic ship protested against this unauthorised usage. The IMG allowed a user of Wallach's site to retrieve the comic strip, thereby make it appear to be included in the text of Wallach's Web site. United Media argued that since such a conduct may be considered as a derivative work under the U.S. Law, Wallach's inclusion of the comic strip in his website may be regarded as violative of U.S. copyright law. It was also argued that since any visitor to Wallach's site could copy the image, he could be made liable for contributory infringement.

¹⁸² A copy of Court's opinion can be found at <<http://www.jmls.edu/cyber/cases/shetldl.html>>.

¹⁸³ Microsoft Press Computer Dictionary, (3rd Edn) at p. 25.

¹⁸⁴ Under traditional hypertext link, when materials from site B appears on the screen, the URL for site B appear along with it, at the top of the Frame, with a warning that viewer will be taken outside the present website.

¹⁸⁵ The correspondence between the parties can be found at <<http://www.cs.princeton.edu/~dwallach/dilbert>>.

The dispute was finally settled with Mr. Wallach removing his site from the Internet.

Framing involves a type of technology quite akin to an IMG link. Framing technology involves one website (site A) incorporating the contents from another site i.e. (site B) into a window or frame of its own in a manner wherein the framing site appear as the original site.¹⁸⁶ Each frame functions independently so that the information downloaded into that frame goes within the frame and does not go into the other frame or overlaps onto the frame itself.¹⁸⁷ When an user of Site A clicks on the hyperlink to site B, the page obtained from site B appears under the frame A. The user feels that the particular page was created by site A instead of site B or that site A is an authorised user or otherwise affiliated to site B. This misapprehension happens because the contents of site B gets reduced to fit into the frame of site A. The URL of site B gets obscure and the contents gets placed along with the advertisements, logo, URL and menus of site A.

It has to be understood that it is the advertisement obligations of site B that remains unfulfilled during such a transfer. Advertiser may buy space on a website based on the expectation that their advertisement will appear in a certain location or slot, be of a certain size or duration or be free of the “clutter” of competing advertisements. The framing activity by passes and defeats all/any of those expectations.¹⁸⁸ Hence a suit can be filed against the framing site based on legal clauses pertaining to violations like trademark dilution, trademark infringement, false designation of origin, false representations and false advertising, deceptive acts and practices, copyright infringements, and tortious interference with advertising contracts.

Washington Post Company v. Total News Inc.¹⁸⁹

The plaintiff's website was 'framed' by the defendant. When a browser of Total News site clicked on one of the linkers the text of the files of the plaintiff's

¹⁸⁶ Microsoft Press Computer Dictionary, (3rd Edn) at 207.

¹⁸⁷ Ibid.

¹⁸⁸ Graham J.H. Smith, *Internet law & Regulations*, (London, 1997), p. 29.

¹⁸⁹ Case No. 97. civ 190 (pkl) (S.D.N.Y. 1997). In this case, the Washington Post CNN, Times Mirros, Dow Jones, Time-Warner, and Reuters filed a lawsuit against Total News alleging nine cause of action in District court of New York.

website appeared but portions of plaintiff website were hidden under defendant's frame. Plaintiff's URL did not appear at the top of the screen. The parties finally agreed for an out of court settlement.¹⁹⁰

Even if the parties had not settled the case, the copyright liability would have existed because

- (1) The frames gave the impression that the defendant created the work (copyright infringement for unauthorised copying.
- (2) Defendant's site might be considered as a derivative work.

***Futuredantics Inc v. Applied Anagramatics*¹⁹¹**

The defendant framed the contents in the plaintiff's website. But the U.S. Ninth circuit court did not grant injunctive relief as it found that the plaintiff has failed to show that it was or would be injured by the Defendant's conduct.

Prevention of unauthorised linking

A few methods for avoiding linking are

- (1) The website creators can notify on the site the link creators should obtain a prior permission before creating links.
- (2) The direct passage to the internal page by bypassing homepage via links can be blocked using effective passwords.
- (3) Creation of software which intercepts and re-routes links to homepage of the linked site.
- (4) Using search engines to locate the sites, which are directly linked to the site so that such users can be warned individually.

¹⁹⁰ A copy of the stipulation, the order of settlement and Dismissal can be found at <<http://www.ljx.com/internet/totalse.html>>.

¹⁹¹ No. 97-56711, 1998 US App (9th cir, 23 July 1998), case No. CV. 97-6991, ABC (manx), 1998 US dist (CD. cal. 30 January 1998).

Ways for avoiding liability for linking

- (1) Obtaining prior permission before the creation of a hypertext link or frames.
- (2) Linking to the homepage instead of directly going to the internal pages.
- (3) Providing disclaimers, which specifically state that the linked sites are neither affiliated with, nor endorsed by the linking site.
- (4) Site operators can include a statement with external hyperlinks informing the user that the links will take the user away from the site.

(IV) Caching

Caching is a function performed by computers to enable Internet to function more efficiently by reducing the load on the communications link. It generally involves the storage of frequently accessed materials in the computer's memory cache, which can quickly retrieve the materials.¹⁹² The Internet involves several types of caching which are fundamental to the operation of World Wide Web.¹⁹³

The first type of caching involves the copying of document that is currently displayed on the screen of an Internet users personal computer while he/she is browsing the web. The second type is where a personal computer not only makes a copy of the documents that are currently being displayed, but also temporarily retains copies of documents which are reviewed by the user in the past. When the computer receives a request for the documents, which were previously viewed, it will bring up the cached copy rather than retrieve the documents from the Internet. In both the types of caching, the computers memory detects the documents, when it is switched off.

The third type of caching is the one causing concerns to the e-merchants. In this case, instead of storing the materials on the personal computer, the documents are stored by an Internet Service Provider (ISP) or by the operator on the website. Hence when the user requests a web page, ISP checks if the documents are already stored in his machine and if he has stored it, the server sends this cached copy of the documents to the browser. This can create a few problems

¹⁹² Microsoft Press Computer Dictionary, at p. 72.

¹⁹³ Smith, n.188, p. 50.

Firstly, the users may not be viewing the current copy of the requested website (the user may not even know that the copy is obsolete). Secondly, caching can cause damage to a sites reputation and finally caching may reduce advertising.¹⁹⁴

(V) ARCHIVING

Archiving is the process of downloading and storing the materials of one website in another so that the second website can provide its users with the materials of the first website in its own website without having to hyperlink to the former to retrieve the materials. Hence when the user clicks on the hyperlinks, instead of going to that site, the user will be taken to another area of the same site, where the materials are stored. This may lead to copyright infringement,¹⁹⁵ trademark infringement¹⁹⁶ and unfair competitions, false designation of origin, passing off etc.

There are many problems arising due to archiving Firstly, since the URL at the top of the screen may not change, the user can erroneously assume that the site B was created by site A or site A is afflicted or associated with B. Secondly, the user may not be viewing the current copy of the information in display.¹⁹⁷ Thirdly the user is not sent to site B, the site B's web counter will not register a "hit". Also depending on the type of the programming found on site A, its web counter may register another hit.¹⁹⁸

VIDEO GAMES & COPYRIGHTS

A video game is a computer generated audiovisual scenario that can be stimulated to move. The player of the game can control one of the characters to perform a series of actions with the aim of arriving at a desired result. With regard to

¹⁹⁴ When the user views a cached copy, he is not taken to the original site and hence the ached site may not register a "hit". As industries advertise in sites registering more number of hits, caching will affect the ability of a site to obtain and retain advertisements.

¹⁹⁵ By storing materials on site A, it is making a copy of the material or reproducing the material. By making the material available to the public, site A is publicly displaying, publicly performing as well as distributing the material. By changing the URL and/or anything else on the page, site A is making a derivative work. Hence archiving constitutes copyright infringement.

¹⁹⁶ Because the materials cached may be outdated or altered, they may not be accurate and thus may infringe the goodwill made upon the trademark.

¹⁹⁷ Archiving is often done to provide materials no longer offered on site B. Hence most of the documents stored on site B might be outdated.

¹⁹⁸ This type of programming is now prohibited under the Digital Millennium Copyright Act, 1998. This area is discussed elsewhere in this chapter.

copyright infringement, the issue of liability arises when a person downloads or uploads a copyrighted video game into a website. While addressing this issue, the courts in U.S. have viewed computer games an audiovisual work.

*Stern Electronic Inc v. kaufman*¹⁹⁹

In the case, the U.S. Federal court held that the visual and audible aspects of game were original enough to be independently entitled to copyright protection even though, those aspects were generated by a computer programme, which was in itself entitled to protection.

This interpretation led to the criticism that a computer game was being reduced to the level of videotape or a music recording. But the U.S. court in *Midway Manufacturing Co v. Arctic International Inc*,²⁰⁰ held that not only the visual and audio aspects of the game is entitled to protection, the actual code that presents the player with all the options that are available to him are the creations of the software developer and therefore entitled to be protected as an original work. The court reasoned that

“The player of a video game does not have control over the sequence of images that appear on the videogame screen. He cannot create any sequence he wants out of the images stored on the games circuit boards. The most he can do is to choose one of the limited numbers of sequences the game allows him to choose.”

When a case of unauthorised downloading or uploading of videogames occurs, the infringer can be held liable for prosecution,

- (1) By a corporate, if the copyright of the videogames is held by a corporation.
- (2) If the copyright is held by different persons e.g. audio rights by one, visual display by another, higher graphics intensive programs by another, then the infringer is answerable to all these persons.

¹⁹⁹ 669 F 2nd 852, 213 U.S.P.Q. 443 (2nd cir 1982). Matthan, n. 154, p. 293.

²⁰⁰ 547 F. Supp. 999,216 U.S.P.Q. 413, (N.D. ill 1982). Ibid.

MULTIMEDIA WORKS & COPYRIGHT PROTECTION

Multimedia work involves the integration of several separate and distinct types of works, which are variedly combined using a computer. It includes information that is in the form of text, sounds, graphics, and even motion pictures clips. The copyright of such a work may or may not lie with a single person, in fact the author of the text, the music composer and the producer of the motion picture clip are all entitled to copyright for their individual composition. The software developer who has used his expertise to effectively integrate these individual components into a single cohesive product is also entitled for copyright protection.

The rapid technological developments have made it extremely easy for a software programmer to develop a multimedia work by choosing his pick from a whole range of audio-visual and graphical options that are available to him. However, since such competition can be violative of copyright protection of individual components that are chosen (e.g. Music, Pictures etc), it is required of him to actually apply for the right to use these individual copyrighted works. The multimedia programmer should be careful in choosing his images for his programmes. He should ensure that they are either properly licensed or that they fall in the public domain or else that it should be within the permissible limits of the “fair use” doctrine.

THE ‘FAIR USE’ DEFENCE

The fair use defence doctrine provides that a third party may use a copyrighted work without the copyright owner’s consent or authorisation provided that the use is fair.²⁰¹ Courts in their analysis of what exactly the fair use doctrine encapsulates have given various interpretations.

*Religious Technology Centre (RTC) v. F.A.C.T. Net Inc.*²⁰²

RTC sought action against F.A.C.T. NET²⁰³ to stop it from posting materials concerning RTC’s tax-exempt status and also regarding the charges that the RTC

²⁰¹ The fair use doctrine is set forth in 17 U.S.C. see 107, which provides four factors for determining fair use. They are (1) the purpose and character of the use, including whether such use is of a commercial nature or is for non-profit educational purposes. (2) the nature of the copyrighted work, (3) the amount and substantiality of the portion used in selection to the copyrighted work as a whole and (4) the effect of the use upon the potential market for or value of the copyrighted work.

engaged in psychological coercion of its members. The court held that the Defendant's use was fair use since its action was aimed at non-commercial criticism and that there was no harm to the church from such a copying endeavour since the members of the church would not consider the posting as a substitute for the church's work.²⁰⁴

Religious Technology Center (RTC) v. Lerma²⁰⁵

A copyright infringement suit was brought against Lerma for posting sixty-nine pages of RTC's material on the Internet. Lerma countered the allegation by claiming that RTC does not have a valid copyright and hence his use was a 'fair use'. The court ruled against Lerma on the following basis.

- (1) Even though the materials were factual in nature and publicly available, RTC still had a valid copyright.
- (2) The court held the act not a fair use because
 - (a) Materials were placed on the Internet without any comments or other changes.²⁰⁶
 - (b) The volume and completeness of the materials posted by Lerma were more than what was necessary to benefit and educate the public.

Religious Technology Center v. Netcom On-line Communications Services, Inc²⁰⁷

Here also, the issue of fair use doctrine was raised. The court upheld Netcom's claim that its use was a fair one because

- (1) The court noted that although, Netcom's use was commercial in nature, the purpose and character of the use in providing Internet access was different from the purpose and character of the RTC's use i.e. religious instruction.²⁰⁸

²⁰² 901 F. supp. 1519 (D. col. 1995) cited in Martens and Halpern, n. 149, p. 12.

²⁰³ F.A.C.T. NET Inc is a Colorado non-profit educational and charitable organization.

²⁰⁴ Ibid at 1525. Also see Smith, n. 188, p. 208.

²⁰⁵ 40 U.S.P.Q. 2d. 1569 (E.D. Va. 1996).cited in Martens and Helpem, n. 149, p. 13.

²⁰⁶ Ibid at 1576-77.

²⁰⁷ 907 F. supp. 1361 (N.D. cal. 1995). cited in Martens and Helpem, n. 149, p. 13.

²⁰⁸ Ibid, p. 1379.

(2) Netcom's copied no more of RTC's copyrighted materials than what was necessary to function as an ISP.²⁰⁹

There was a genuine issue of material fact as to whether Netcom's making available the RTC's copyrighted works would harm the market for that works.²¹⁰

THE U.S. DIGITAL MILLENNIUM COPYRIGHT ACT (DMCA)

The Digital Millennium Copyright Act (DMCA) enacted in October 1998 in United States tackles some of these issues and remove some of the uncertainty by its creation of 'safe harbours' for the innocent transmission, caching or storage of infringing materials by an On-line Service Provider (OSP). This section discusses the Impact of title II of the DMCA, entitled the Online Copyright Infringement Liability Limitations Act (OCILLA) and analyses the limitations of liability established by the OCILLA.

The OCILLA effectively limits liability for copyright infringement for certain conduct of an OSP by creating five 'Safe harbours'. The five safe harbours involve the following conduct: (1) data conduit activities. (2) Caching (3) Storage of information (4) information location tools: and (5) takedowns of allegedly infringing materials. Safe harbours (1), (3) and (5) are discussed under the heading "liability due to the posting or uploading of materials on the Internet", the safe harbour (2) is discussed under "liability due to caching" and 'safe harbour' (4) is discussed under 'Liability for linking'.

OCILLA

The OCILLA created a new section 512 to the copyright Act which provides for several limitations of liability for copyright infringement by an OSP due to innocent transmission, caching or storage of infringing material placed on the OSP's system by a third party. It imposes certain affirmative obligation upon an OSP to qualify for a 'safe harbour'²¹¹ the first being, whether the party can qualify as a 'service provider'.

²⁰⁹ Ibid, p. 1380.

²¹⁰ Ibid.

²¹¹ The OSP must (1) adopt and reasonably implement a policy for terminating subscribers who are repeat infringers and (2) accommodate and not interfere with 'standard technical measures' used by a copyright owner to identify and protect copyright works. [17. U.S.C. see 512 (i)].

These are two definitions for OSP, the first for the safe harbour concerning transitory communication (i.e. acting as a data conduit), a service provider is defined as “an entity offering the transmission, routing or providing of connections for digital on-line communications, between or among points specified by a user, of materials of the user’s choosing without modification to the content of the material as sent or received”.²¹² For the remaining form safe harbour, a ‘service provider’ is a ‘provider of on-line services or network access, or the operator of facilities therefore, and includes an entity described in the first edition.’²¹³

If a ‘copyright infringer’ qualifies an OSP and its conduct comes within one of the ‘safe harbours’, the OCILLA limits the OSP’s liability for copyright infringement.²¹⁴

LIABILITY DUE TO THE POSTING OR UPLOADING OF MATERIALS ON THE INTERNET

The cases before the enactment of OCILLA and the position of law were discussed earlier. Three safe harbours are discussed under this section

(a) Protection for transitory communications

Section 512 (a) of the OCILLA provides that where an OSP merely allows the transmission or providing connection or routing of digital information from one point to another or provides connections for the information, the OSP’s liability for copyright infringement may be limited if

- (1) A person other than the OSP initiated the transmission.
- (2) The transmission, routing, provision of connection or copying was carried out by an automatic technical process without any selection of materials by the OSP.

‘Standard technical measures’ “are defined as measures that the copyright owners use to identify or protect copyright works” [17 USC section 512 (i) (2)].

²¹² 17 U.S.C. section 512(K)(1)A.

²¹³ 17 U.S.C. section 512(K)(1)B. According to the House Judiciary Committee Report, this definition includes Internet access, e-mail, chat room and web page hosting services.

²¹⁴ 17 U.S.C. section 512(J)(1). Each of the ‘safe harbours’ providers complete bar to monetary damages and restricts the availability of injunctive relief.

- (3) The OSP did not select the recipients of the materials.
- (4) The copies of the materials made by the OSP are accessible to only the intended recipients and the OSP does not keep such copies for longer than reasonably necessary and
- (5) The OSP did not modify the content of the transmission.²¹⁵

If an OSP qualifies for this exemption, the OSP cannot be held liable for monetary damages for copyright infringement. While the OCILLA does permit injunctive relief, such relief is limited to orders to terminate the accounts of subscribers who are infringers and to take reasonable steps to block access to specific, identified on-line locations outside the U.S.²¹⁶

(b) Protection for storage of information on system or networks

Section 512 provides for a limitation of liability for an OSP where the OSP stores materials on its system at a user's request (such as a user's web page)²¹⁷. To qualify as a 'safe harbour' an OSP must:

- (1) Not actually know that the material is infringing or have information from which the infringing nature of the material is apparent.
- (2) Not have the right and ability to control the infringing activity or if it does, it must not receive a financial benefit directly attributable to the infringing activity.
- (3) Upon acquisition of knowledge or awareness as discussed in (1), expeditiously take down or block access to the materials.
- (4) Upon receipt of 'proper notice' from the copyright owner or agent, expeditiously take down or block access to the allegedly infringing materials²¹⁸ and

²¹⁵ 17 U.S.C. section 512(a).

²¹⁶ 17 U.S.C. section 512(j) (1) B.

²¹⁷ 17 U.S.C. section 512(C).

²¹⁸ An OSP is deemed to have received 'proper notice' of the 'claimed infringement' only if the OSP receives a written notice from the copyright owner or agent and which identifies the copyrighted work, the allegedly infringing materials and other information so that the OSP can

- (5) File with the Copyright Office a designation of an agent to receive infringement notices and make available the name and address of the agent on the OSP's website.²¹⁹

Where an OSP receives 'proper notice' and has removed or blocked access to materials, that OSP must take reasonable steps to notify the subscriber who posted the materials. If an OSP does not 'promptly' notify, the subscriber that the materials have been removed or blocked, the OSP may be found liable for removing or blocking access to the materials.²²⁰

In response to such notification, the subscriber may send a 'counter notification' to the OSP which indicates that the removal or blocking, of the material is due to a mistake or misidentification of the material.²²¹ If the counter notification complies with certain statutory requirements, the OSP must provide the copyright owner with a copy of the counter notification.²²² The copyright owner must then notify the OSP that a court action seeking to restrain the alleged infringement has been filed. If the OSP does not receive such notice from the copyright owner or agent, the OSP must replace or unblock the material within ten to fourteen days following the receipt of counter notification.²²³

(c) Protection for removing or blocking materials

If an OSP in good faith removes or disables materials, the OSP is exempt from liability provided that the OSP notifies the subscriber who posted the materials and complies with the other Safeguards discussed above.

(II) Protection for caching

An OSP's liability for copyright infringement may be limited, provided that

- (1) The OSP does not modify the content of the cached materials.

locate the materials, as well as contact information for the complaint. 17 U.S.C. section 512(C)(3).

²¹⁹ 17 U.S.C. section 512(C)(2).

²²⁰ 17 U.S.C. section 512(g).

²²¹ 17 U.S.C. section 512(g)(2)(B).

²²² 17 U.S.C. 512(g)(3).

²²³ 17 U.S.C. section 512(g)(2)(B).

- (2) The OSP must refresh (provides updated copies of cached materials) in accordance with generally accepted industry standard data communication protocol.
- (3) The OSP must not interfere with technology connected with the cached materials that returns information (such as the number of ‘hits’) to the person who posted the material provided that the technology meets certain standards.²²⁴
- (4) The OSP must comply with any user limiting conditions (such as a password or payment of a fee) imposed on the materials of the originating party.
- (5) If the OSP is notified that the materials have been removed, blocked or ordered to be removed or blocked from the original site, the OSP must promptly remove or block access to such cached materials.

If an OSP qualifies the first safe ‘harbour’ the OSP cannot be held liable for monetary damages for copyright infringement. Instead under this ‘safe harbour’ (as well as safe harbours 4 and 5) relief is limited to orders to terminate the account of infringing subscribers to remove infringing materials from the service providers network and other remedies that are the least burden same to the service provider among the range of comparably effective alternatives.²²⁵

(III) Protection for information location tools

Section 512 (d) provides for a limitation of liability for an OSP, where an OSP refers users to materials via a search engine, a hyperlink or a list of recommended sites.²²⁶ This ‘safe harbour’ requires an OSP to meet basically the same conditions as are discussed under section 512 (c). Safe harbour except that the notice must identify the link or reference instead of the materials.

²²⁴ 17 U.S.C. 512(b).

²²⁵ 17 U.S.C. section 512(j)(1)A.

²²⁶ 17 U.S.C. section 512(c)(d).

Moreover, liability for other types of linking such as inline (IMG) links and similar technology such as framing²²⁷ does not appear to be affected by the OCILLA.²²⁸

Avoiding copyright infringement liability and enforcing copyright rights

In the light of these cases and the enactment of the OCILLA, Service Providers, Operator and managers of website should post guide lines regarding the types of material allowable on their service or site and procedures for complying about violation of those guidelines, and should enact polices for removing allegedly infringing content as well as designate and register with the copyright office an agent to receive notification and establish take down procedures.

Like wise, copyright owners should actively police the Internet or use services, which will perform such tasks, and when encountering infringing materials should carefully comply with OCILLA's notification procedures.²²⁹ Furthermore, in the light of the potential for liability for misrepresentation, both copyright owners and subscribers should carefully consider their responses to notifications of infringement.²³⁰

It is important to note that merely because an OSP does not qualify for any of the OCILLA's safe harbours, the OSP is not necessarily liable for copyright infringement.²³¹ Instead, copyright infringement must still be demonstrated and the OSP may take advantage of any of the traditional defences to copyright infringement such as fair use.²³²

Despite the DMCA, copyright law in cyberspace is still an open frontier. Given that legal precedent is sparse, difficulties often arise in determining which legal theory supports an opposition to the conduct and where the boundaries of right and wrong should be drawn. Moreover, the international reach of cyberspace only exacerbates the difficulties, as the same conduct may be permitted by one sovereign

²²⁷ Mentioned elsewhere in this chapter sec. Footnote 49.

²²⁸ Supra note 46

²²⁹ The OCILLA also includes a procedure under which the copyright owners can obtain court orders for subpoenas copyright on OSP to identify information concerning the alleged infringing materials.

²³⁰ 17 U.S.C. section 512(f).

²³¹ 17 U.S.C. section 512(1).

state but prohibited by another. Nonetheless, given the explosive growth of cyberspace, copyright law will be forced to develop line protecting and limiting rights to at a much faster pace than it had to in the evolution of the copyright law with respect to more traditional media.

THE PROPOSED EUROPEAN COPYRIGHT DIRECTIVE

The Copyright Directive, which was presented by European Commission on 21 May 1999, aims to “establish a level playing field for copyright protection in the new environment”. It covers the reproduction rights, the communication to the public right, the distribution rights and legal protection of anti copying and rights management systems.

According to art 2 (b) of the Directive, the member states to provide right holders with fair compensation for copying by digital mean even where it is made for private, strictly personal and non-commercial use i.e. there is no fair dealing exceptions for research. The fair use exception is available only to illustration for teaching or scientific research, use by people with a disability, use of excerpts for reporting current events, quotations for criticism or review and use for public purposes. These rights together with rights provided under the rights management information means that in future all digital information’s can be tracked and charged for and strengthens the right owner’s position.

Member states will be required to comply with the directive by 30 June 2000.

Databases

One of the areas pertaining to intellectual property that has been enriched with the advancement of computer technology is the database. The modern understanding of the term database represents more than a mere collection of data. A data base today is, in addition to being a repository of data, a carefully structured and ordered filing cabinet, from which data retrieval is easy and can be performed by any user of the data base.²³³ The IP protection for database is a legally complicated issue. Very often

²³²

See page

²³³

Rahul Matthan, n. 154, p. 386.

it happens that the person who initially collected the information stands to lose his claims for IP rights owing to his negligence and laxity.

Legal Protection for Databases in the U.S.A.

Copyright, trade secret and contract law are the three channels through which one can protect his/her right over the database. The presence of loopholes in each of these protection mechanisms means that it is always better to go in for a combination of all these forms of legal protection for databases.

(a) Copyright protection for databases

The copyright law provides protection to the author of the work with reference to the form, creativity and style of his/her literary work. A pertinent question that arises here is as to how creative an author can be when dealing with a list of names and addresses. Though, considerable time, effort and money goes into the compilation of a database, it will be futile to ascribe beyond a point the quality of creativity. This is because, it is easy to distinguish raw data from the information presented in the database. In the 1980's the U.S. courts developed the doctrine of sweat-of-the-brow, to protect database creators. The doctrine holds that if considerable labour and effort had gone into the acquisition and selection of data, to make the compilation original, then it would be held valid for the purpose of securing copyright protection.²³⁴ This doctrine was widely criticised and in other courts of U.S.A, database disputes continued to be resolved using traditional concepts of creativity.²³⁵ This division of opinion was resolved by the Supreme Court of U.S. in the Feist case, which has come to be accepted as the uniform position in the U.S. legal arena.

Feist Publications Inc v. Rural Telephone Company²³⁶

Feist Publications, a company formed by Feist decided to make a telephone directory containing the listing from all the eleven telephone service areas in Kansas.

²³⁴ *Southern Bell Tel & Tel v. Associated Telephone Directory Publisher* [756 F.2d. 801, 809 (11th cir 1985)].

²³⁵ *Miller v. Universal City Studios Inc*, [650 F. 2d 1365, 1369 (5th cir 1981)]; *Lane v. First Nat Bank of Boston*, [687 F. supp. (DC Mass 1988)]. The court reasoned that grant of copyright protection to databases based merely on the "Sweat-of-the-authors-brow" would risk putting large areas of actual research material off limits and threaten the public's unrestrained access to information.

²³⁶ 499 U.S. 340, 111 SCT 1282, 113 LED 2d 358 (1991). cited in Matthan, n. 154, p. 386.

The license to use their directories was given by all companies except Rural Telephones. To have a complete listing Feist copied Rural's Directory but hired people to verify 5000 listings in Rural's Directory to check for false seedings.²³⁷ Out of the 47000 listings in Feist's Directory, 1300 were identical and 3600 were same as Rural's Directory. Rural sued Feist for copyright infringement. The trial court and the appellate court affirmed this claim. However, the Supreme Court of U.S. overruled these decisions and held that the essence of copyright is originality in the relation and arrangement of facts and hence Feist was not liable for copyright infringement. The court reasoned that the ultimate purpose of copyright law was not to maximise the financial return to individual authors, but to promote the dissemination of knowledge. Allowing second-comers of copy facts in preparation of another work, would therefore work to and in achieving the constitutional purpose of copyright law.

Pro CD v. Zeidenberg²³⁸

In this case, the plaintiff developed a database which was compiled from over 3,000 directories and consisting of over 95 million commercial and residential listings. The defendant developed a different programme to disseminate knowledge from this database. The court held the defendant not liable, taking the Feist's ratio into consideration.

Trade secret Protection for Databases

Trade secret is a form of knowledge that is exclusively developed/acquired by a person or a company through his or its own efforts for which there should be a right of IP protection. There are a number of databases that could easily be categorised as trade secrets. For e.g., compilation of consumer lists, consumer profiles and supplier lists are just some of the more common forms of databases that would commercially be thought of as trade secret of considerable value. The law relating to trade secrets in the U.S. is the Uniform Trade Secrets Act which in sec 1(4) defines trade secret as

“Information including a formula, pattern, compilation, program, device, method, technique or process that

²³⁷ Telephone companies used to mix fictitious listings, in order to catch persons who copy the listings of addresses from their directories. This process is known as 'seeing' or 'salting'.

²³⁸ 1996 U.S. LEXIS 167 (WD. Wisc 1996). Cited in Matthan, n. 154, p. 390.

(a) Derives independent economic value, actual or potential, not being generally known to, or not being readily ascertainable by proper means by other persons who can obtain economic value from its disclosure or use; and (b) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Databases being a compilation, which can deceive economic value, can in fact be given protection under the trademark secrets norms.

In **Telerate system v. Carco**,²³⁹ the U.S. court held that in order to be classified as a trade secret, the owner or compiler of the database must necessarily have made reasonable efforts to maintain the secrecy.

Contract Protection for Databases

The most practical solution to legal issues relating to protection of databases would be to ensure that all the persons who are given access to the database are required to bind themselves under a contract, to certain obligations in respect of the use of the database.²⁴⁰ The contract can in fact be made available in the form of a license agreement: Typically a license agreement gives the license a right to use the data in certain specified ways and it does not include the transfer of ownership or other IPRs by the license agreement, the user can be prohibited in a number of specified ways, all of which can be detailed in the license agreement and can be enforced through specific performance of contract.

Such an agreement is stronger than any statutory remedy, as this constitutes an agreement between the parties to behave in a specified manner, with respect of the use of the database, an agreement that is enforceable even when the provisions of law are silent or ambiguous.

DATABASE PROTECTION IN EUROPE

Unlike the U.S. legal system, which is still grappling with the classification of databases, in terms of the class of intellectual property within which databases falls, the European commission has been clear in its classifications. It has already issued a

²³⁹ 689 F. supp 221, 232 (S.D.N.Y. 1986). cited in Matthan, n. 154, p. 391.

²⁴⁰ Matthan, n. 154, p. 391.

directive in respect of the legal protection of databases that was adopted on 11 March, 1996²⁴¹.

The EU directive deals with the legal protection of databases²⁴² in any form. Database Directive is *sui generis* directive and is applicable within the European commission. The protection granted under the directive does not extend to the computer programs that are used in the making and operation of the databases. These computer programs have been specifically protected under the terms of software directive. The directive seeks to protect electronic and manual databases. However in the case of those databases, in which selection and arrangement of the contracts have been so structured so as to constitute the authors own intellectual creation, it is the copyright protection that has to be used.

Rights of the Authors²⁴³

The author has the exclusive right to carryout or to authorise

- (1) Temporary or permanent reproduction by any means and in any form, in whole or in part.
- (2) Translation, adaptation, arrangement and any other alteration.
- (3) Any form of distribution to the public of the database or copies thereof, an the understanding that the first sale of the copy of the database shall exhaust the right to control the resale of that copy within the community.
- (4) Any communication, display or performance to the public.
- (5) Any production, distribution, communication, display of performance to the public of the results of translation, adaptation arrangement or other alteration of the database.

The database directive permits the use of the database in certain circumstances without the express permission of the author. This includes

²⁴¹ Directive 96/9 EC of the European Parliament and of the Council.

²⁴² Database is defined as a “collection of independent works, data or other material, arranged in a systematic or methodical way and individually accessible by electronic or other means”. (Art 1(2) of EC Database Directive).

²⁴³ Creator of the database is referred to as author.

- (1) Reproduction of non-electronic database for private purposes.
- (2) Use of the database for the sole purpose of teaching or scientific research, provided there is due acknowledgement and provided that extent to use is justified by the non-commercial purposes that is being served.
- (3) Availing the database information for public security, administrative or judicial procedure.
- (4) Other exceptions to copyright granted under the national law.

The *Sui Generis* Extraction Right

The cardinal provision of the EU directive is the right offered to the author to prevent extraction²⁴⁴ and/or re-utilisation²⁴⁵ of his work. According to Art 7 (1) of directive.

“Member States shall provide for a right for the maker of the database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents, to prevent extraction and/or re-utilisation of the whole or substantially whole or of a part, evaluated qualitatively and/or quantitatively of the data base”.

It follows that, if proved that either quantitatively or qualitatively or both, a substantial investment in obtaining, verification or presentation of information contained in the database, the author can prevent the extraction and/or re-utilisation of the contents, such a right being an entirely new intellectual property right.

The database right will remain protected for a period of fifteen years from the first day of the year, following the year in which database was completed or made available to the public. However in case of substantial improvements, modification, deletions or alterations being made to the original text, as a result of which the

²⁴⁴ EU Directive defines ‘extraction’ as “permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any other means or in any form”. The definition therefore brings within its ambit digital copying, down loading, printing and all the other creations of the modern digital age.

²⁴⁵ Re-utilisation is defined by the Directive as “any term of making available to the public, all or a substantial part of the contents of a database, by the distribution of copies, by renting or by on-line or other forms of transmission.

database becomes a new investment, then the new data would qualify the database for another term of protection.

The EU law relating to databases represents a step in the right direction for at last two reasons. Firstly the efforts of database makers, which has been glossed over by IPR, got adequate protection. Secondly it initiates the action of a novel form of intellectual property Rights law, which is more effective and creator friendly.²⁴⁶

INDIAN LAW ON PROTECTION OF DATABASES

A brief preview of the Indian legal system with respect to IPR reveals that the Indian law has not yet caught up with the advancement in the west. This is particularly true in the case of granting protection to databases. The Indian database makers would have to rely on the protection available under the copyright laws in the country. The other suitable measures that could be used as a safe backup are the provisions that provides for protecting the database under trade secret law or contract law. If one involves the trade secret laws, the contents of the database would be treated as unique. Consequently a complainant can urge the court to recognise the tortious liability of a person who has misappropriated the information. In the case of contractual protection, the author of the database can exercise a greater degree of control over the licensed user.

²⁴⁶ The lack of any provision for compulsory licensing, which is present in all other intellectual property rights is absent in the EU Directive. There is enough potential for the creation of monopolies as a result of this license.

LAW OF TRADEMARKS

Trademarks disputes in cyberspace arise in many ways, the most important and widely debated area being that of cybersquatting. The first part of this presentation discusses the trademark law with respect to domain name disputes. This section ends with other trademark violations in the cyberspace like linking, framing, Meta tags etc.

Trademarks and Domain Names

Domain name is the gateway to the e-world.²⁴⁷ To establish a presence on the Internet, the first step by an entrepreneur is to choose a domain name. When you add to your company's names a ".com" domain name, actually you are setting a significant piece of cyberspace for your company.²⁴⁸ Having a domain name, makes, it easy for your customers, suppliers and other interested parties to contact the business by e-mail messages, the added advantage over the phone being that it may be difficult remember the telephone member of the company but it is easier to remember the domain name address, if they are associated with the company's name or its trademark or it's products.²⁴⁹

The domain name system (DNS) helps the Internet users to navigate across the Internet. This is done with the aid of two components namely the domain name and its corresponding Internet Protocol (IP) number. Domain name is a mnemonic term an internet user uses to instruct a computer to obtain the Internet Protocol address (IP) of the desired websites, the IP address being the numerical address code needed to communicate with a computer anywhere in the world hosting a website²⁵⁰ i.e. a domain name is basically an user friendly alias for an internet address.²⁵¹ The real IP

²⁴⁷ Kenchia, "E-world" in Stephen York and Kenchia ed, *E-commerce. A guide to law of electronic Business*, (London, 1999), p. 1.

²⁴⁸ Singleton and Halberstam, n. 38, p. 13.

²⁴⁹ Ibid p. 14; Kenchia, n. 247, p. 1

²⁵⁰ Charlotte Waelde, "Domain names and Trade marks: What's in a name?" in Edward and Waelde, ed., *Law and the Internet*, (oxford, 1997), p. 46, Kenchia n. 247, p. 1, Chisick and Kelman, n. 5, p. 17.

²⁵¹ Kenchia, n. 247, p. 1.

address is a string of number that is difficult to use and remember. For example 207.46.130.150²⁵² stands for www.microsoft.com.

The DNS operates on the basis of a hierarchy of names. At the top are Top-Level Domain (TLDs), which is divided into two levels: the Generic Top Level Domains and the Country Code Level Domains.

(1) Generic Top-Level Domains [gTLDS]

Generic top level domain names are seven in number of which three gTLDS have no restrictions for anyone to register names in them namely, .com (International Commercial Organization), .org (for miscellaneous organisations) and .net (network organizations). The remaining “restricted” or “closed” gTLDS are .edu (four-year, degree-granting colleges and universities), .int (International Treaty organisation), .gov (U.S. government) and .mil (U.S. military organizations).²⁵³

(2) Country code top-level domains. [ccTLDS]

ccTLDS bears a two-letter country code. Currently there are 243 ccTLDS. For example .uk. means a U.K. based internet domain name, .fr for France, .in for India, .ca for Canada.²⁵⁴ Each ccTLDS can have a second level domain name. i.e. for a U.K. company, there is .co and .ltd and .plc.

Domain name disputes

To facilitate the customer to locate the business easily, most of the businesses try to choose a domain name which incorporates either their corporate name or their main brand name or a name which describes the goods and services being offered, as the majority of the users will try to guess a domain name before resorting search engine.²⁵⁵ It is important for a business to ensure that its domain name is protected.

²⁵² IP address consists of four sets of number divided by dots or periods. Each individual number cannot be more than 255. In the cited IP address, 207 refers to the network, 46 and 130 to the Sub networks and 50 refers to the computer in which the file is located.

²⁵³ WIPO, *Final Report of Internet Domain Name Process*, April 30, 1999, para 6, available at <http://wipo2.wipo.int>.

²⁵⁴ Two letters denoting each country is derived from Standard 3166 of International Organization for Standardization (ISO 3166). Ibid, para 7.

²⁵⁵ Kenchia, n.247, p. 1.

Domain name disputes arise due to fact that domain name is unique and there may be multiple parties who wish to use the same domain name and are willing to fight over it. Conflicts arose where others have registered Internet domain names that are same as or similar to registered trademarks of other business/same business in same/different countries. Trademarks are national in scope and different businesses may be holding the same trademark in different geographical locations or they are doing different type of business with the same mark. Under the present DNS, only one of them can hold its trademarks in its domain name since domain name is unique.²⁵⁶

Domain name functions as a source identifier on the Internet. Ordinarily, source identifiers like addresses, were not protected under Intellectual property (i.e. trademark) per se. The use of domain name as source identifiers has burgeoned and courts have begun to attribute intellectual property rights to them while recognising that misuse of a domain name could significantly infringe, dilute or weaken valuable trademark rights²⁵⁷ i.e. use of a domain name by a person not entitled to the trademark, amounts to infringement.

Secondly the search engines can take you to the homepage of any site simply by typing a single identification word connected with the business.²⁵⁸ Often this single word used will be the trademark used by a business.

“Cybersquatting” which involves the use of a domain name by a person who neither has any trademark registration nor any inherent rights, arose primarily due to the registration policy of first-come-first-served. Most registrations were done with a malafide intention of holding the trademark owner to ransom.²⁵⁹ The domain name dispute happens in four ways.

²⁵⁶ For example, the name ITC is used by different companies like Indian Tobacco Company, Inter State Television Corporation, etc. But only one of them can register the domain name “www.itc.com”.

²⁵⁷ Framework for Global Electronic Commerce, President William J. Clinton, Vice President Albert Gore. In Washington D.C, July 1, 1997, p.

²⁵⁸ If one wants to visit homepage of Nike Ltd, the U.S based Sports Shoe company, only the word “nike” has to be typed for the search request. It will add the rest of the URL i.e. <http://www.nike.com.>.

²⁵⁹ Burger king, the famous U.K. Hamburger company had to be satisfied with the domain name ‘burger-king.co.uk’ as the domain name ‘burgerking.co.uk’ was registered by One in a Million Ltd. The subsequent letter demanding money ran as follows. “I confirm that I own the domain name burgerking.co.uk. I would be willing to sell the domain name for the sum of £ 25,000 plus VAT. In answer to your question regarding as to what we would do with the domain name should you decide not to purchase it-the domain name would be available for sale to any

Firstly, a third party intentionally registers a domain name with the knowledge that someone else will want it. The prime intention is to hold the business to ransom and demand financial reward for giving up the domain name.²⁶⁰

Secondly, dispute occurs where a domain name is registered by someone who knows it is the same as the trademark, belonging to someone else or very similar to such a trademark, but intends to use it for their own purposes. Visitors to the site may be surprised to find that the goods or services that are advertised are not those they would normally have associated with the mark that they know and understand.²⁶¹

Thirdly, disputes arise over “innocent registrations.”²⁶²

Fourthly, disputes which as known as “twins” or “string conflicts” involve cases where both parties have trademark registrations, either relating to same products in different countries or different products in the same country. If both the parties want to register a domain name, which is their trademark, then conflicts arise, which is almost irresolvable.²⁶³

Before going into the various domain name disputes, an examination on the grounds on which an action can be filed is important. Both in the U.S. and the U.K., an infringement of trademark is brought on the basis of two main grounds namely confusion and Dilution. Most of the disputes to date have involved instances of intentional pirating of domain names.

Doctrine of Confusion and Dilution in U.S.

The U.S. Lanham Act, 1984 defines a trademark as “any word, name, symbol or device or any combination used or intended to be used to indicate the source of

other interested party----- although you currently have burger-King. Co. UK, this would not be the most obvious first choice for any individual to use, should they be speculatively looking for you website”. Singleton and Halberstam, n. 38, Page 32.

²⁶⁰ ‘Macdonalds.com’ was registered by the Mr. Quinter, who transferred the rights in return to which Macdonalds Inc was forced to make donation for computer equipment for a primary school. Quoted in Waelde n. 250, p. 48.

²⁶¹ Teubner K Associates, a software company got confused, when their competitors registered “tuebner.com”, which is a common misspelling of Teubner, Ibid.

²⁶² A person may register a domain name, which might be the trademark of some business in another country without even knowing the existence of the said business.

²⁶³ Prince plc v. Prince Sports Group Inc. quoted in kenchia, n. 247, p. 6, Waelde, n.250, p. 51.

goods.²⁶⁴ The touchstone of liability under the act is “confusion.”²⁶⁵ The court in the case of *Maritz Inc v. Cybergold*²⁶⁶ considered domain name dispute alleging trademark violation based on “confusion.” Maritz Inc was providing an Internet service, which consisted of providing financial rewards for reading e-mails, who used an unregistered trademark “Gold mail”. Cybergold developed a similar service with the domain name “cybermail.com.” Which according to the plaintiff caused confusion with their URL “goldmail.com.” Negating the argument, the court reasoned that for confusion to be caused the use of allegedly infringing mark must create a likelihood of confusion, deception or mistake among an appreciable number of ordinary buyers as to the source or association between the two name²⁶⁷ or ‘create a likelihood that an appreciable number of ordinarily prudent purchases are likely to be misted or simply confused as to the source of goods in question.’²⁶⁸

In any trademark dispute, the factors pertinent to a finding of confusion was pronounced by the court in *Anheuser-Busch Inc v. Balducci Publications*²⁶⁹ which included, the strength of the trademark, the similarity between the marks, competitive proximity of the products, the intent to confuse the public, the evidence of actual confusion and the degree of care reasonably expected of the customer.

Doctrine of Trademark Dilution in U.S.

The ground of dilution “does not seek to protect ideas of origin, but the quality which the trademark embodies.”²⁷⁰ The cases mentioned below enumerates the number of different scenarios, which has been considered by the courts while deciding on dilution of trademark by using them as domain names by someone not connected with the mark.

In *Hasbro, v. Internet Entertainment group Inc*,²⁷¹ the court was convinced that Hasbro had been producing a game called ‘candy Land’ for children and that 94%

²⁶⁴ 15 U.S.C. s 1127.

²⁶⁵ *Polaroid corporation v. Polaroid Electronic corporation* (287 f 2d. 492), quoted in Waelde, n. 250, p. 49.

²⁶⁶ 1996 US Dist Lexis 14977, 29 August 1996. Ibid.

²⁶⁷ *Duluth News-Tribune v. Mesabi Publishing co* (84 F 3d 1093 8th cn 1996). Ibid.

²⁶⁸ *Centaur communications* 830 F.2d.Ibid.

²⁶⁹ 28 F 3d.769 8th cir 1994. Ibid.

²⁷⁰ Ibid at p. 55.

²⁷¹ No. C 96-3381 cw 1996 U.S. Dist. LEXIS 17020 (N.D. cal. Oct. 29, 1996). Quoted in Bajaj and Nag, *E-commerce, The cutting Edge of Business*, (New Delhi, 1999), p. 269.

of mothers were aware of this game. The defendants registered a domain name “candyland.com” featuring pornographic materials. The court held that the name “candy land” was diluted by the use by the Internet Entertainment Group. The court may well have been influenced in this case by the sexually explicit nature of the materials.

In *Panavision International LP v. Toeppen*,²⁷² the defendant registered “panavision.com” and attempted to sell the domain name back to Panavision. In the subsequent case alleging dilution of famous marks, the court held that registering a famous mark as a domain merely for the purpose of trading on the value of the mark by selling the name to the trademark owner violated dilution statutes.

Similarly, in *Intermatic Inc. v. Dennis Toeppen*,²⁷³ the court held that by attempting to licence or sell the mark by Toeppen caused the dilution of the distinctive quality of the mark by lessening Intermatic’s capacity to identify its goods to potential customers and destroying the marks advertising value.

This reasoning suggests that the court in the U.S. will find that there is dilution of trademark in all cases where there is an intention by the person who registered a domain name resembling a famous trademark to sell that domain name for financial award.²⁷⁴

Doctrine of Confusion and Dilution in U.K.

In *Harrods Ltd. v. U.K. Network Services Ltd.*,²⁷⁵ Harrods, the famous department store of London, alleged that the registering of “Harrods .com” by Michael Lawrie²⁷⁶ constituted “trademark infringement and passing off.” The court decided the case *exparte* in favour of Harrods and hence the first case on domain name dispute in U.K did not throw any light regarding the conflict between trademark and domain names.

²⁷² 245 F. supp 1296, 1996 US Dist. LEXIS 19628 (CD cal. 1996), *aff’d* 1998 US App. LEXIS 7557, 98 Daily Journal DAR 3929 (9th cir. April 17, 1998).

²⁷³ 947 F. Supp. 1227 (ND 111 1996).

²⁷⁴ Waelde, n. 250, p. 56.

²⁷⁵ High Court, Ch D. December 9, 1996. cited in, Waddle, n. 250, p. 50.

²⁷⁶ Michael Lawrie registered 54 other ‘famous marks’.

In *Pitman Training Ltd and PTC Oxford Ltd. v. Network U.K Ltd and Pearson Professional Ltd*,²⁷⁷ the case was filed on passing off as neither of them had a registered trademark. The domain name 'Pitman.co.uk' was registered by Pitman Publishing in February 1996. Due to some mistake of Nominet, the registration authority, Pitman training managed to register the same name in March 1996 and started using it from July 1996. Nominet transferred the name back to Publishing in April 1997. Pitman training argued that as they had used the name for a period of months, the general public would associate that name with their business and if it is reverted to Pitman publishing, it would amount to passing off. The court denied the passing off claim on the basis of the evidence presented.²⁷⁸

The U.K. Trademark Act, 1994 has not yet been analysed in detail in connection with trademark disputes in cyber space, but it will be useful to have an understanding of terrestrial trademark rights, which may be helpful in the battle in cyber space.²⁷⁹ Under the section 10(2) of the U.K. Trademark Act 1994, when a question of confusion and/or similarity of goods occurs, the following factors are to be taken into consideration, namely the users of goods and services, the uses of the goods and services, the physical nature of goods or acts of services, the trade chains through which the goods or services reach the market, whether in self service stores the goods are found together or apart and the extent to which goods and services are competitive²⁸⁰.

Trademark dilution in U.K.

Based on the judgement by *Laddie. J. in Wagamama Ltd v. City Centre Restaurants plc and others*,²⁸¹ it may be said that a trademark infringement by dilution is difficult to be established without proving that there has been an element of confusion within the meaning of section 10 (2) of the UK Trademarks Act. But in cases where a third party has used a company's name to make profit out of its goodwill, U.K. courts have taken strict measures against them.

²⁷⁷ No CH 1997 F 1984, (1997) FSR 797 (ch 22 May 1997), Kenchia, n. 247, p. 6.

²⁷⁸ During the period of use Pitman Training received only two e-mails.

²⁷⁹ Waelde n. 250, p. 52.

²⁸⁰ *British Sugar v. James Robertson* (1996) R PC 281. Ibid.

²⁸¹ (1995) FSR 713, I bid, p. 53.

In *Direct Line Group Ltd v. Direct Line Estate Agency*,²⁸² a trademark infringement action was brought against a number of companies using names such as YSL Limited, Virgin Jeans Limited and Nike Clothing Company Ltd.. Direct Line Group Limited objected to the use of names Direct Line Estate Agency Ltd and Direct Line Estates Ltd. Finding trademark dilution, Laddie J held that

“(The directors) have a track record of taking or being associated with the taking of famous trademarks belonging to third parties, either for the purpose of carrying on business which siphons off the goodwill belonging to other traders, or for the purpose of offering those marks back to their rightful proprietors, no doubt as a profit this court will view with extreme displeasure any attempt by traders to embark upon a scam designed to make illegitimate use of other company’s trademarks.”²⁸³

The above decision would approve a number of cases of the type brought in courts of US against registrants like Dennis Toeppan.

Famous and well-known marks and Domain Names

Famous names are given protection from trademark infringement through the U.S. Federal Trademark Dilution Act 1996 and section 56 of the U.K. Trademarks Act, 1994. Taking into consideration the omnipresent nature of the Internet, these laws can help the trademark owner in a domain name dispute.

In U.S., under the Federal Trademark Dilution Act, 1996, the only requirement to be proved is that the mark is famous, negating the requirements of likelihood of confusion to be established for proving infringement. The Federal Dilution Act, 15. U.S.C. see 1125 (c) prohibits the uses which diminish the ability of a “famous” marks to identify and distinguish goods or services associated with that mark even if there is no likelihood of confusion.

See 43(a) of Lanham Act provides that the owner of a famous mark shall be entitled to an injunction for user of the mark that cause dilution of the distinctive

²⁸² (1997) FSR 374, Singleton and Halberstern, n. 38, p. 33.

²⁸³ Waelde n.250, p. 57.

quality of the famous mark. The seven factors for determining whether a mark is famous, according to this section, are²⁸⁴

- (1) The degree of inherent or acquired distinctiveness of the mark.
- (2) The duration and extent of use of the mark.
- (3) The duration and extent of advertising.
- (4) The geographical extent of the trading area in which the mark is used.
- (5) The channels of trade.
- (6) The nature and extent of third party uses of same or similar marks and
- (7) Whether the mark is registered.

Some states also have anti-dilution statutes which long precede the Federal Dilution Act and which are not limited to “famous marks”.

In U.K., if the ‘mark’ is “well known”, then irrespective of whether it carries on business or has a goodwill in the U.K. the mark owner may stop a third party using a similar mark in relation to identical or similar goods, where that use is likely to cause confusion.²⁸⁵

Domain name disputes in U.K., U.S.A.

The international nature of these disputes was demonstrated in the Prince case. When two businesses have the same registered trademarks in different countries, the question arises as to who should own the domain name, which is the trademark itself.

In *Prince plc v. Prince Sports Group Inc*,²⁸⁶ was the first case in this area, where courts of the two different countries were involved. Prince plc, a U.K. IT Service Provider, registered the domain names “prince.com” and “prince.co.uk”. When U.S. sportswear company, who had several trademark registrations for “PRINCE” in both U.S. and U.K. decided to register, they found that Prince plc had already registered its domain name. Prince Sports instituted NSI Dispute policy and provided 30 days to Prince plc to ‘either relinquish the name or produce a valid trademark registration certificate or files a legal action in any court in U.S. or have its

²⁸⁴ Application of E.I. DuPont De Nemours Co., 476 F.2d 1357, 177 U.S.P.Q. 563, 567 (C.C.P.A.1973).

²⁸⁵ Waelde, n. 250, p. 57.

domain name put on hold.’ Prince plc filed a civil action in the U.K. High Court seeking a declaration that its registrations of “prince.com” did not infringe the trademark rights of the U.S. Company. Prince Sports Wear sued NSI and Prince plc in U.S. the ruling of the U.K. court left Prince plc in control of the domain name. But the Court did not get involved in the legal battle over domain name ownership as it would interfere with the U.S. law suit filed by Prince Sports Group. Hence the dispute is left to be ultimately resolved in the U.S. court.

In *One in a million case*,²⁸⁷ as already noted, the U.K. Court examined the passing off and trademarks issues. The plaintiffs filed a case against one-in-a-million Ltd, which had registered their trademark as a domain name and it had been done in order to make money out of them. The judge found that the defendant registered such famous names for the extraction of money and hence the registrations were not innocent and ordered the defendants to transfer the names to the plaintiffs. The judge made the U.K. legal position clear by stating:

“ Any person who deliberately registers a domain name on account of its similarity to the name, brand name or trademark of an unconnected commercial organisations must expect to find himself on the receiving end of an injunction to restrain the threat of passing off.”²⁸⁸

The Court of Appeal confirmed the High Court’s order and a leave to appeal to the House of Lords were refused, making the U.K. legal position clear.

U.S. Cases

The U.S. position remains settled in the Toeppan’s case. It is that cybersquatters shall lose in the subsequent dispute. The other important cases are noted below.

*MTV Networks v. Adam Currey.*²⁸⁹

Adam Currey, who had been employed as the video jockey on MTV, registered the site mtv.com, where he conducted a discussion on entertainment,

²⁸⁶ (1998) FSR 21 (ch 1997), Kehchia, n. 247, p. 6; Waelde, n. 250, p.51.

²⁸⁷ British Telecom, Virgin Atlantic, Sainsbury, Ladbrokes and Mark & Spencer v. one in a Million Ltd. Quoted in Singleton and Halberstam, n. 38, p. 34.

²⁸⁸ Singleton and Halberstam, n. 38, p. 33.

²⁸⁹ 867 F. supp. 202 (S.D.N.Y. 1994).

celebrities etc when MTV and Currey parted, he was asked to surrender the domain which he has registered in his own name. On his refusal, the parties moved the Court. Dispute was settled out of court with Curry handing back the name to MTV networks.

In *Princeton Review Management Corp. v. Stanley H. Kaplan Education Center Ltd*,²⁹⁰ the Princeton corporation who were the competitors of Kaplan Center, registered the domain name “kaplan.com” and the website produced messages derogating Kaplan Education Center and praising those of Princeton Review Corporation. In this case of cybersquatting, an agreement was reached out of court, transferring the name back to the Kaplan Education Center.

Data Concepts Inc v. Digital Consulting Inc²⁹¹

Data Concepts registered the domain name, DCI.com in 1993 but the same was the federal trademark of Digital Concepts, which they had registered in 1987. Digital proceeded against Network Solutions Inc (NSI) for transfer of domain name. In the case filed by Data Concepts, the Court found against them. However, this was revised by the 6th Circuit, urging that the Court should reconsider it. But 6th circuit also mentioned in the report that Digital has got the priority over the use of the mark.

SG2 v. Brokat²⁹²

Brokat, a German company registered ‘payline.com’. ‘Payline’ was the trademark of SG2, a French company, who in turn sued for trademark infringement. The President of the District Court of Nanterre considered that infringement was committed in France by the mere appearance of the word ‘payline’ on the screen. Brokat had distributed a brochure in a conference held in Paris, in which the domain name was printed. The court held that this also constituted trademark infringement.

²⁹⁰ 94 civ. 1604 (MGC) (S.D.N.Y. filed March 9, 1994).

²⁹¹ 97-5802, 1998 Fed App. 0214P, 47 USPQ 2d 1672 (6th cir 5 November 1998). Singleton and Halberston, n. 38, p. 38.

Indian position

Domain name disputes have also arisen in India, and the courts, taking into consideration the worldwide developments have also attributed trademark rights to domain names.²⁹³

In *Yahoo! Inc v. Akash Arora*,²⁹⁴ the defendants registered “yahooindia.com” and even copied the layout and format of the plaintiff’s website “yahoo.com.” The Delhi High Court considered the matter as a case of ‘passing off’ and held the defendant liable, reasoning that the domain name ‘yahoo’ has achieved a distinctiveness and is associated with the plaintiff company and that it should be entitled to protection. The court added that the use of a disclaimer would not suffice.

Similarly in *Rediff Communication Ltd v. Cyberbooth and another*,²⁹⁵ Rediff filed a suit for permanent injunction, restraining the defendants from using the domain name “radiff.com”, who were operating the website and providing the same services given by “rediff.com”. Having found that the adoption of the name Radiff was to deceive the consumers,²⁹⁶ the court held that once an intention to deceive was established the court will not make further enquiry about the likelihood of confusion. Issuing an injunction, the Court said:-

“Internet domain names are of importance and can be a valuable corporate asset. A domain name is more than an Internet address and is entitled to the equal protection as a trademark. With the advancement and progress in the technology, the services rendered in the Internet site have also come to be recognised and accepted and are being given protection so as to protect such provider of service from passing off the services rendered by others as his services.”²⁹⁷

In another case,²⁹⁸ Delhi High Court has ordered an injunction against an IT company, who registered the domain name, ‘bisleri.com’ in a case filed by Aqua Minerals Ltd who were the manufactures of mineral water branded ‘Bisleri’. The court held that

²⁹² It’s a French case decided on 13 November 1997, cited in Singelton and Halberstam, n. 38, p. 38.

²⁹³ In *Rediff Communication Ltd v. Cyberbooth and another*.(AIR 2000 Bom. 27), para 11, the Court held the same.

²⁹⁴ 1997 PTC (19) 201.

²⁹⁵ AIR 2000, Bom. 27.

²⁹⁶ The defendant argued that the name RADIFF was obtained by taking first three letters from ‘Radiant’ and first letters from ‘Information’ and ‘Free.’

²⁹⁷ Ibid at p. 30, para 11.

Bisleri is a very rare name and the defendants have got it registered only to obtain a monetary settlement.

Other Trademarks Violations: Linking, Framing, Meta tags

The evolution of Internet has lead to numerous problems involving trademarks. For example, outside the world of cyberspace, two companies can often use the same name and mark in different geographic locations without any problems because customers in either area may never be aware of the use in the other area. Internet being accessible worldwide, when both companies create a website, consumers from all over the world see both the websites and both the marks.²⁹⁹

Trademarks infringement

Under U.S. trademarks law, a trademark is defined as “any word, name symbol, or device or any combination thereof, used by a person or a company to identify its goods or services and distinguish them from the goods and services of others.”³⁰⁰ Under U.S. law both registered and unregistered trademarks are eligible for protection.³⁰¹

Two key elements for trademark protection under U.S. laws are use and distinctiveness.³⁰² Typically protectibility is analysed by classifying a term in one of four categories. (1) Arbitrary and fanciful (2) suggestive (3) descriptive or (4) generic.³⁰³ Trademarks falling into the first two categories are considered “inherently distinctive” and are protected from conception. Marks falling within the third category

²⁹⁸ Reported in *Times of India*, Delhi, 23 February 2000.

²⁹⁹ In addition, outside cyberspace two or more companies can use the same mark in the same geographic locations for different goods or services without any conflicts. An example of this is “Thrifty Dental Care” and ‘Thrifty Drug Store’. Although both the companies use the same mark, consumer are able to distinguish the user due to the difference in the goods and/or services. In cyberspace, such uses have produced a myriad of domain name lawsuits, which has been mentioned earlier.

³⁰⁰ 15 U.S.C. sec 1127.

³⁰¹ Same under Indian law but in UK only registered Trade Marks are protected.

³⁰² *Two Pesos Inc v. Taco cabana Inc*, 505 U.S. 763, 112 S.Ct. 2753, 23 U.S.P.Q .2d. 1081 (1992). Quoted in Loundy and Klett, “Trademark Law and Internet Address: Significant Cases in Selected Jurisdictions”. *The World Bulletin*, vol. 13 Sept.-Dec.1997, pp.78-120, p. 84.

³⁰³ Ibid.

are protectable when the mark has acquired distinctiveness.³⁰⁴ Generic terms are never protectable.³⁰⁵

To succeed in a claim of trademark infringement, the plaintiff must show that it has a protectable mark and that there is likelihood of confusion to the origin, affiliation, source and a sponsorship of the defendant goods or services.³⁰⁶

Likelihood of confusion is determined by a number of factors such as (1) the similarity of service, (2) the strength of plaintiff's mark,(3) the channels of distribution, (4) evidence of actual confusion, (5) the degree of care likely to be exercised by consumers, (6) the likelihood of expansion of products or services, (7) third party uses of the same or similar marks and (8) the intent of the defendant in adopting its mark.³⁰⁷

Traditional Trademarks Infringement in Cyberspace

Trademark infringement occurs in cyberspace when the trademark of one business is used by another in furtherance of their business objectives. More often the goodwill associated with the mark is used for promoting unauthorized goods. Few cases are discussed here to illustrate the trademark infringement in cyberspace.

In *Playboy v. Chukleberry Publishing*,³⁰⁸ an U.S. Court enforced an injunction against the defendant who was selling or distributing its PLAYMEN magazine in the United States. The defendant's website used the word "PLAYMEN" as its domain name.³⁰⁹ In addition, the defendant prominently displayed the designation. 'PLAYMEN' on its homepage and on each page of its website.³¹⁰ The court concluded that the defendants use of the designation PLAYMEN as a domain name and prominently displaying it on the website's homepage was the "electronic equivalent of a magazine cover and table of contents".³¹¹ It ruled that because the defendant's site offered services similar to those of the plaintiff, the defendant's conduct was violative of practices established under the trademark law.

³⁰⁴ Ibid.

³⁰⁵ Ibid.

³⁰⁶ 15 U.S.C. sec 114 (1); 14 U.S.C. sec 1125 (a).Ibid at p. 84.

³⁰⁷ *Forum Corp. of N. Am. v. Forum Ltd.*, [903 F. 2d. 434, 439 (7th Cir. 1990)]. Ibid at p. 85.

³⁰⁸ 937 F. Supp. 1032, 39 U.S.P.Q.2d. 1746 (S.D.N.Y. 1996).

³⁰⁹ Defendants domain name was <<http://www.playmen.it>>".

³¹⁰ Ibid at pp.1748-50.

The U.S. court enforced the U.S. injunction even through (1) defendant's website was based in Italy; (2) the defendant's name was acquired through an Italian domain name registration system; and (3) An Italian court had found that the plaintiffs PLAYBOY mark was not entitled to protection.³¹²

In *Playboy Enterprises Inc v. Frena*,³¹³ a case noted already, the U.S. Court held that the operator of a BBS which allowed subscribers to upload materials containing the words PLAYBOY and PLAYMATE infringed 'playboy's trademarks even if the BBS operator did not intend to use the marks. The court also held that the defendant's removal of Playboy's trademark from some of playboy's photographs constituted reverse passing off.³¹⁴

In *Sega v. MAPHIA*,³¹⁵ the U.S. Court determined that, among other things, defendant's electronic bulletin board from which visitors could download and upload video games infringed plaintiff's mark by using the SEGA trademark in games that were substantially similar to SEGA's games.³¹⁶

In *Malarkey Taylor v. Cellular Telecommunications Industry Association*,³¹⁷ the plaintiffs, a consulting firm for wireless cable television and satellite industries, provided on-line information called "Wireless Now" service. They had a U.S. Trademark Registration for the mark "Wireless Now". The plaintiffs were a member of the defendant organisation. At the defendant's 1996 trade show, also participated by the plaintiff, the defendant announced that its new website offered or on-line information called "Go Wireless Now!" At the trade show several parties inquired if the defendant was the sponsor of the plaintiff's service or if the plaintiff's service was being offered by the defendant. The defendant also received several e-mails and telephone calls inquiring of the affiliation between the plaintiff and the defendant. The plaintiff brought an action for trademark infringement. The U.S. Court used a traditional likelihood-of-confusion analysis and concluded that the two marks were similar in appearance and that the services were overlapping and might soon be

³¹¹ Ibid at p. 1751.

³¹² Ibid at pp. 1748-1751.

³¹³ 839 F. Supp. 1552 (M.D. Fla 1993).

³¹⁴ Ibid at p. 1562.

³¹⁵ 948 F. Supp. 923, 41 U.S.P.Q.2d. 1765 (N.D. Cal 1996).

³¹⁶ Ibid at pp. 938-940.

³¹⁷ 929 F. Supp. 473 (D.D.C.1996).

coterminous.³¹⁸ In further support of a finding of a likelihood-of-confusion, the court noted that the instances of actual confusion existed. It granted the preliminary injunction.

Several well-known companies have been involved in disputes concerning use of allegedly confusing marks on the website. In 1995, TOYS R US objected to the “ROADKILLS R US” website. Although the URL of the site was “rru.com” and does not infringe “TOYS R US” trademarks rights, they alleged that the solid use of the phrase “ROADKILLS R US” was likely to cause confusion.³¹⁹ Similarly, The Gap, Inc, which is the owner of Banana Republic objected to a company’s use of the name “BANANA REPUBLIC EMBROIDERY” on its website which did not originate in the United States. Again the dispute did not involve the domain name, which was <http://www.procaps.co.uk>, but the use of the BANANA REPUBLIC mark on the site.

Linking

Linking allows the user to go to a different spot on the same document, or to a different document stored on the same website or to a document located on a different computer.

A hyperlink from site A to site B could result in trademark infringement. For example, if site A uses site B’s mark as a hyperlink to site B’s website in a manner which leads visitors of site A to believe that there is some affiliation or sponsorship of site A by site B or suggests some connection or association between site A and site B, the use may be considered as infringement. Furthermore, if site A uses site B logo (a design or device mark instead of a word mark) visitors may be more likely to assume there is some relationship between the two sites, which might affect the commercial value of the sight negatively or positively depending on the linking site.

Ticket Master Corporation v. Microsoft Corporation³²⁰

In this U.S. case, Ticket Master alleged that the defendant’s website, which offered information about Seattle, provided a hyperlink that took the users to an internal page of Ticket Master’s website. Although the user could see Ticket Master’s

³¹⁸ Ibid at pp. 475-478.

³¹⁹ Information regarding this dispute can be found at <<http://www.rru.com>>.

³²⁰ Civ No. 97-3055 (DPP). (C.D. cal.1997).

URL at the top of the screen, it alleged that by passing Ticket Master's homepage, bypassed the information including advertisements located on the homepage. Although parties settled the case out of court, the defendant's conduct may give rise to a claim for reverse passing off because the internal links create the appearance that the materials found at the Ticket Master's websites originated with the Microsoft.

As discussed earlier, the IMG linking dispute involving the Dilbert Comic Strip³²¹ also involved reverse passing off since viewers might believe that Danwallach created the Comic Strip.

Framing

Compared to linking, framing is a relatively new practice. A framing site, by using certain commands in its HTML code, links to another site, displaying that site in a window or frame. The framed site will be displayed along with the advertisements of the framing site, misleading the users into believing that the framed material belongs to the framing site or the two sites are associated some way. This has led to the sites challenging those who frame them.

The *Total News Case* involved the defendants framing the plaintiff's website.³²² Among the other claims,³²³ the plaintiff alleged that the defendant's conduct contributed trademark dilution and infringement. In particular the plaintiff's alleged that use of the plaintiffs well-known marks on the defendant's site diminished the value of the plaintiff's marks and was likely to cause confusion and mistake, and deceive users to the source or origin of the content and promote advertising on the defendant's website. The plaintiffs also alleged that the framing was likely to cause users to believe that there was some affiliation, sponsorship or approval between plaintiffs and Defendants.

On June 5, 1997, the parties entered into a settlement under which the defendant agreed to stop linking to plaintiff's sites using frames or in any other manner which would cause the plaintiffs sites to appear to the user as originating,

³²¹ The correspondence between the parties can be found at <<http://www.cs.princeton.edu/dwallach/dilbert>>.

³²² *Washington Post company et al v. Total News Inc, et al, S.D.N.Y. complaint No. 97 civ.*

³²³ Plaintiffs claim for copyright infringement, misappropriate and tortious interference is discussed.

supplied by or associated with the defendant or any third party, such as an advertiser.³²⁴

Framing violates Trademark law because framing creates doubts in the mind of the viewer as to the origin of the document, which is a traditional concern of trademark law. The confusion as the origin occurs primarily due to the fact that the URL of the framing site is appearing on the screen instead of the framed site and secondly the framing site is often surrounded by the content and advertisements of the framed site.

Meta Tags-Hidden Hypertext

If an Internet user does not know the URL of a particular website or wants to find sites discussing a certain topic, the user can use a search engine³²⁵ or spider,³²⁶ with the search comprised of the key words from the topic the name or the company the user is trying to find.³²⁷ Search engines use “Meta Tags” or “Meta Words” to find and index web pages. Meta Tags or Meta Words are intended to be ‘keywords’ or ‘Tags’ that are encoded into the hypertext markup Language (HTML) by the website owner that describe the context of the website but that do not actually appear on the web page. Instead these tags are only visible in a web page source code. When an Internet user performance search, let us consider an example, for “SHELL”, any websites with “SHELL” in their Meta tags will turn up in the result. However, just because “SHELL” is embedded in a site HTML code, does not necessarily mean that the site has anything to do with “SHELL” or even discusses “SHELL.”

When an Internet user visit the site (Site A), expecting to find information about SHELL, but finding none, the visitor may mistakenly believe that site A was retrieved in the search because there is some affiliation or connection between site A and SHELL”. Furthermore, depending on how often site A uses the term “SHELL” as a Meta tag and how many others also use “SHELL” as a Meta tag, the real SHELL’S website might be indexed so low in the search that the Internet user may never visit

³²⁴ A copy of the settlement can be found at <<http://www.ljx.internet.totalse.html>>.

³²⁵ Examples of search engines are Yahoo, Lycos, EXCITE, INFOSEEK, REDIFF, HOTBOT, ALTAVISTA etc.

³²⁶ Spider is a web program that searches for files based on the Meta tags provided.

³²⁷ C. Shipley & M. Fish, *How the World Wide Web works*, (New York, 1996), p. 20.

the site.³²⁸ Thus by using Meta tags, a competitor of SHELL, or an unhappy customer, could divert the Internet users from the real SHELL'S website to its own site.

Such a conduct, known as spamdaxing³²⁹ can result in trademark infringement, dilution, passing off, unfair competition, false advertising or right to publicity violations. Spamdaxing includes a variety of conduct. The earlier practice was to use "buried text" (tiny words camouflaged in the background colour) to incorporate extra text, relevant or not, that would be visible to the search engine but not to the public.³³⁰

The other practice is "stuffing" i.e. the use of multiple repetitions in buried text or Meta tags in an attempt to boost the apparent relevance of the page to the stuffed term. Now many search engines penalise sites engaging in these two practices.³³¹ Now the common practice is to misuse the Meta tags to accomplish the same abusive purpose that were penalised.

There are two kinds of Meta tags; Keyword and Description tags. Keyword Meta tags is invisible to the web-surfing viewer, but not to search engine robots, which use them to index the page. Description Meta tags are also similar to the above and are used to supply description of a web page for search query output. Although both types of Spamdaxing are there the majority of Spamdaxing is with keyword Meta tags.

Some overload their pages with frequently requested key words (sex, money or Pamela Anderson) or with thousands of repetitions of the same keywords³³², some use the names of celebrities,³³³ trademarks and trade names by

³²⁸ Thus a competitor of the business or a customer could divert the users from the website.

³²⁹ Reliance of web owners to supply indexing information encourages schemes to "Spam the search engines with deceptive index terms and hence this conduct is referred as 'Spamdaxing'. Ira S. Nathenson, "Internet Infoglut and Invisible Ink: Spamdaxing Search Engines With Meta tags". *Harvard Journal of Law and Technology*. vol. 8, 1997.

³³⁰ A web page buried in the text can be easily spotted by the fact that there will be excessive blank space at the bottom of the document and can be confirmed by high lighting the 'blank' space with a click-and-drag of the mouse, reverting any 'invisible text'.

³³¹ Paul C. Judge, "Revenge of the search engine" *Business week*, Nov-17, 1997, p. 146 B. In *Niton Corp v. Radiation Monitoring Devices Inc.* (no. civ. A, 98-11629-REQ, 1998 WL 812685) preliminary injunction subject to modification was granted "where the defendant copied the verbatim the description Meta tags of plaintiff competitor and used them in its own web page".

³³² Randy Mc Claim, "Snared by the web? Even the Cyber-Savvy will need patience to snag Internet success", *Baton Rouge Advoc*, Sept 20, 1997, p. 1E.

³³³ When a research of "Gillian Anderson" at Alta visitor was done (<<http://www.altavista.digital.com>>), a page offering pictures of nude girls were found. The

other,³³⁴ popular generic terms³³⁵ analogous terms³³⁶ and categorical generic terms abstracted from actual content.³³⁷ Honest web owners, frustrated by Spamdexers, may themselves be forced to Spamdax so that those who actually seek them can find them.³³⁸

In *Playboy Enterprises Inc v. Calvin Designer Label*.³³⁹ Playboy Enterprises brought an action against Calvin designer Label for trademark infringement alleging that defendants had been using Playboys marks PLAYMATE and PLAYBOY as domain names within the text of its website and in Meta tags.³⁴⁰ The U.S District Court of California restrained the Designer from using the PLAYMATE or PLAYBOY marks as domain name, directory names on its websites or as hidden Meta tags on the sites.

Web Directory World Pages allegedly found that *Infospace*; another web directory was using “world pages” in its Meta words and was appearing high on searches for the name “world pages”. Apparently, Infospace removed the terms from its Meta tags alleging that a web designer without Infospace’s knowledge placed the Tags on the pages.³⁴¹

*Insituform Technologies Inc v. National Envirotech Group L.L.C.*³⁴²

search turned up 64. 997 documents of which the offending page was the third. Its invisible buried text contained Meta tags “Gillian Anderson”, “seinfeld”, “Jeff Daniels”, “Cameron biaz” and “Jim Carry”. Quoted in Nathenson, n. 329, p. 64.

³³⁴ *Playboy Enterprises Inc v. Calvin Designer Label*. Civ. No. C-97-3204 CAL. (N.D. Cal. 1997).

³³⁵ In the foot note 333, the site used various generic term in the Meta tags like “Free”, ‘free’, ‘Porno’, ‘porno’, “Lesbians”, “LESBIANS” and Lesbians.

³³⁶ *The Advanced concepts case*, mentioned earlier in the heading under Meta tags.

³³⁷ For instance, a site created by a law student that contained legal links, course outlines and Lawyer jokes might use keyword Meta tags that would include “law”, “jokes”, “funny”, “study”, “education”. Quoted in Nathenson, n. 329, p. 64.

³³⁸ David Landgren stuffs his own name multiple times into buried text at the bottom of his homepage (URL is <<http://www.landgren.net>>). In the same buried text, he wryly apologizes for this act “I hate to spamdex like this but otherwise there are two many hits for me over at another websites and people would otherwise never hit this page when they searched for me. Please concept my apologies”. Quoted in Nathenson, n. 329, p. 64.

³³⁹ 985 F. Supp. 1220 (N.D. cal 1997). A copy of the complaint can be seen at <<http://www.patents.com/ac/playcpt.sht>>. This was the first case, which complained trademark violation due to Meta tagging.

³⁴⁰ The defendants URL were “Playmatelive.com” and “playboyxxx.com” and the ‘Playboy’ and ‘Playmate’ trademarks as the site itself in buried text. (Ibid at 1221-22).

³⁴¹ A copy of the order can be found at <<http://www.jmls.edu/cyber/cases/calvin.html>>.

³⁴² Civil Action No. 97-2064 (ED. La), available at <<http://www.cll.com./case1.html>>

In this case, Insituform Technologies Inc (Insituform) alleged that one of its largest competitors, the defendants was using ‘Insituform’s’ and ‘Insitupipe’ in Meta tags on Nationals sites so that National site would be indexed when these terms were put into search engines. In addition, Nationals site contained Insituform’s marketing materials, which suggested some sort of connection or affiliation between Insituform and National.³⁴³ The matter was settled when parties entered a consent judgment which provided that National would delete the hidden codes from its site and stop using the Insituform’s marketing materials on its site.³⁴⁴

In *Playboy Enterprises, Inc v. Welles*,³⁴⁵ the defendant Terri Welles,³⁴⁶ in 1997, established a website at ‘www.terriwelles.com’, which included photos, a fan club, posting board etc. The site included visible references to “Playboy”, “Playmate of the year”, and “PMOY” along with disclaimers.³⁴⁷ The site also used the terms “Playboy” and “Playmate”, “model”, “naked” and other such terms. PEI moved for a preliminary injunction on the basis of trademark infringement, false designation of origin and trademark dilution.³⁴⁸ The court denied the motion because the defendant’s use of PEI’s trademarks was in good faith [under 15 U.G.C. sec 1115 (b) (4) and 1125 (c) (4) (a)] and for a descriptive use (i.e. non-trademark use). The court reasoned that

“ (T)rademarks such as Playmate are not only trademarks related to Playboy magazine, but they are titles bestowed upon particular models who appear in that magazine who then use the title to describe themselves. Much like Academy Award winners, crowned Miss Americas and Heisman Trophy winners, Playboy Playmates are given a title, which becomes a part of their identity and adds value to their name. Indisputably, these winners represent the awarding organizations or sponsors but the title becomes a part of who they are to the public.”³⁴⁹

³⁴³ Information about the case be found at <<http://www.cll.com/wnewfr.html>>.

³⁴⁴ A copy of the consent judgement can be seen at <<http://www.cll.com/case/html>>.

³⁴⁵ 7 F. Supp. 2d 1098 (S.D. cal) aff’d, No. 98-55911, 1998, U.S. App. LEXIS 27739 (9th cir .oct.27,1998). Quoted in Nathenson, n. 329, p. 70.

³⁴⁶ Terri wells was playboy “playmate of the Year” in 1981 and alleged that she had referred to herself as such since than. (Ibid 7F. supp. 2d at 1100). Ibid.

³⁴⁷ The title bar stated “Terri Welles-Playboy Playmate of the year 1981” and the page itself was entitled “Terri Welles-Playmate of the year 1981”. Each Page at her site also used “PMOY ‘81” as a repeating watermark. The disclaimers noted that Ms. Welles was not affiliated with PEI and also noted that PEI’s marks were federally registered.” I bid at 1100-01.

³⁴⁸ The claims were asserted under the Lanham Act section 32 (1), 43 (a) and 43 (c). sec 15 U.S.C. sec 1141 (1), 1125 (a) (c), Quoted in Nathenson, n. 329, p. 71.

³⁴⁹ I bid at 1102.

Welles might provide guidance as to when the use of a term was sufficiently relevant, and in sufficient good faith, to constitute fair use.

However, *Playboy Enterprises Inc v. Asia Focus International, Inc*³⁵⁰ provides a contrast. Here the defendant used PEI's trademark in their website's source code. The defendants also registered a domain name that contained PEI's trademarks used PEI's trademarks in its web pages and sold playing cards, calendars, wristwatches and key chains. The judge awarded statutory damages of \$ 3,000,000 plus costs and attorney's fees ruling that the use was neither based on good faith nor had any valid authorisation or reason.

In the third case, *Oppedahl & Larson v. Advanced Concepts*,³⁵¹ plaintiffs, themselves Attorneys, asserted that the use of their names as Meta tags by the Advanced concepts, violated federal unfair competition, federal dilution and state law. The defendants were neither lawyers nor providers of legal services, however they did offer domain name registration and other Internet Services. The U.S. Court granted a permanent injunction. Unfortunately it did not have the opportunity to reach a decision on the merits. Such a decision might have helped to determine just how relevant a Meta tag must be to actual content to avoid liability, especially considering that the litigants were not competitors.

Conclusion

Domain names are accepted by the courts as synonyms to trademarks and they can be protected under trademark infringement or passing off. To win in court, the plaintiff has to prove that it has got a registered trademark and its use by the defendant amounts to a trademark infringement and/or passing off. In domain name cases, the present legal position can be summarised as follows: -

- (1) Cyber squatters will lose dearly.³⁵²
- (2) Famous marks will probably win.³⁵³

³⁵⁰ No. 97-734-A, 1998 U.S. Dist LEXIS 10359 (E.D. Va. Feb. 2, 1998). Quoted in Nathenson, n. 329, p. 71.

³⁵¹ Civ. Act. No. 97-Z-1592, 1998 U.S. Dist. LEXIS 18359 (D.Colo. Feb. 6, 1998) 1997 U.S. Dist. LEXIS 23105 (D. Colo. Dec. 19, 1997), 1997 U.S. Dist. LEXIS 23108 (D. Colo. Dec. 19, 1997). Quoted in Nathenson, n. 329, p. 68.

³⁵² E.g. are *one in million*, *Panovision Inc v. Toeppan*, *Intermatic Inc v. Toeppan*.

(3) Trademark owners will have preference over domain name registered based on the trademark.³⁵⁴

(4) Identical/similar trademarks for similar goods and/or services will not be able to win easily.³⁵⁵

The Courts have clarified the legal position with respect to two aspects of trademark violations in cyberspace, namely the traditional trademark infringement and the use of Meta tags. But the position of Hyperlinking and Framing are still not clear since all the cases in this regard were settled out of court. This can intun force the parties to redress their grievances under the action of passing off.

The trademark liability can be avoided by using a few preventive measures. Disclaimers stating that the linked or framed site has no affiliation to the linking site or a general warning like “you will be now taken to a new site” would be appropriate. These disclaimers should be clearly visible and legible, which will help the parties when using the defence of “fair use”. Another suggestion would be to use web page protection software, which eliminates unauthorised linking and framing. Solution should be sought in private settlement rather than judicial decision, since there is no concrete judgment pertaining to this area.

Courts would not accept the use of meta-tags due to the simple fact that by this practice profit is made by using someone else’s trademark. Even if the mark is not directly visible, its use is sufficient to constitute a mark violation, because the rationale behind the law of trademarks is to ensure that no person makes use of someone else’s trademark. Even if trademark were not applicable, a common law action to passing off would certainly lie.

³⁵³ *Hasbro Inc v., Internet Entertainment Group Inc, Marks and v. one in a million, Yahoo Inc v. Akash Arora,*

³⁵⁴ *Direct line Group v. direct line estate agency,* Most of the cyber squatting cases.

³⁵⁵ *Prince plc v. Prince foot wear Group* 91998) FSR 21 (ch 1997).

PAYMENTS

Getting paid on-line is one of the many challenges faced by any e-trader, primarily due to the fact that Internet is an insecure medium. In whichever way e-commerce progresses, what it needs urgently is a payment mechanism which is fast, reliable and secure. There are a number of payment options available, from the completely off-line one in which an individual uses a phone or drops a cheque, to the unique model where an individual might begin minting his own currency.³⁵⁶ To make financial transactions confidential, many sites use different procedures and protocols, which basically encrypts the financial information in the credit card number, or address of the purchaser, trader etc. Even if the message is hacked, nothing should affect the privacy of the transaction.

This section on "Payments" discusses five aspects namely the various types of protocol available for a secure transaction, the different types of credit cards and e-cash available in the e-commerce business, e-cash and reasons for its promotion as a vehicle of Internet commerce, the problems associated with the issue of e-cash and legal issues relating to regulation of on-line banking.

E-commerce seems unlikely to make a big splash unless security fears are dealt with. To secure transactions on the net, e-traders use two types of data exchange Protocols, namely Secure Sockets Layer (SSL) and Secure Electronic Transaction (SET) Protocol.

Secure Sockets Layer Protocol. (SSL)³⁵⁷

The SSL provides several features that make it suitable for the use in E-commerce transactions. In SSL, privacy is guaranteed through encryption and authentication is provided through digital certificates.

³⁵⁶ Karnvir Munrey, "Pay Your Way", *PC WORLD* (New Delhi) March 2000, p. 54.

³⁵⁷ E-Business Technology Forecast, Price Water House Coopers Report, California, 1999, p. 156; Praveen. S. Thampi, "Intimate Transfers", *Computers Today* (New Delhi), September 16-30, 1999, p. 74,

Working

In SSL, the client and server exchange public keys as they enter into transactions. Then the client generates a private encryption key referred to as a “session key”, which is generated exclusively for the current transaction. The client then encrypts the session key with the servers’ public key and forwards it to the server. For further exchanges related to this transaction, the client and the server can ensure top security using the session key for private-key encryption.

Secure Electronic Transition Protocol (SET)³⁵⁸

SET Protocol was jointly introduced by credit card leaders, Visa and MasterCard. The aim of the Protocol is to ensure privacy of credit card number and the details of the transactions, when sent over a network. For this, SET uses digital signatures, encryption and cryptographic signatures.

Working³⁵⁹

In SET, the identity of the buyer and the seller are to be authenticated through Digital Signatures. SET allows both kinds of private information, i.e. information between the buyer and the e-trader regarding the items purchased and between the buyer and the bank regarding credit card number, to be included in a single digitally signed transaction. Information to the bank is encrypted with the bank’s public key, while information for the merchant is encrypted with merchants public key. Since the e-trader has no access to credit card details, chances of any fraudulent practices are eliminated. In addition using another digital signature, which covers the whole transaction, combines both their signatures. SET thus ensures non-reputability and authenticity, which are the primary concerns of any e-transaction.

SET is a standard describing a complex authentication mechanism that makes it extremely difficult to commit fraud. The most widely used card-acceptance mechanism over the Internet, SSL, only has a weak built-in feature for authenticating

³⁵⁸ S. Thampi, n. 357, p. 75; Chissick and Kelman, n.5, p. 130, Stephenson and Bennett,” E-Payments” in Stephen York and Kenchia ed. “E-commerce: A guide to the law of electronic business” Butterworths, London 1999, p. 70-71.

³⁵⁹ Ibid.

customers and merchants. Weaknesses and strengths of both SSL and SET are outlined and summarized as follows.³⁶⁰

Characteristic	SSL	SET
Certification	Pair-wise sharing of certificate may not have certification.	Certification of all parties by trusted third party
Authentication	No mechanism exists to authenticate parties	Both customer and merchant are authenticated
Nonrepudiation	No mechanism to capture customer's commitment	Customer digitally signs commitment to purchase and pay
Risk of merchant fraud	Customer gives key financial data to the merchant	Customer gives key financial data to the payment gateway.
Liability for customer fraud	Merchant liable in case of fraud	Financial institution liable in case of fraud
Infrastructure	In place in browsers and web servers	Proven in pilot demonstrations; available as packaged software or software tools; not widely deployed
Anonymity versus auditability	Allows each party to certify itself at the onset of a transaction, but assurance of the identity is weak	Requires all parties to be certified repeatedly throughout the transaction
Interoperability	Standardized by the IETF	Standardized by SETCo
User acceptance	Widely used by customers on the Web.	Not yet in widespread use

In a SET transaction, however, a merchant has assurance that a customer is legitimate because of the built-in authentication mechanism. Many e-business merchant sites in the U.S. already have implemented SSL-based merchant servers and have shown little interest in migrating to SET.

There are about 12 methods of payments that can be used in any e-commerce transactions.³⁶¹

(1) Credit cards

In using credit cards, the consumer opens an account with a facilitator (a bank) who provides him/her with a credit card number. When the consumer makes a deal over the net, the merchant transmits a record of the sale to the facilitator who seeks a

³⁶⁰ Price Water House Coopers LLP, Report, n.357, p. 157.

confirmation from the purchaser. Once conformation is done, the facilitator debits the amount to the merchants' account and a small transaction fee is charged for this.

(2) ATM/ Debit cards

The difference between a credit and a debit card is that, with the latter, purchasing can be done only for the amount, which has been deposited by the consumer with the facilitator. The ATM/Debit cards are widely used in Europe and are becoming popular in the U.S.

(3) Purchasing cards

Purchasing cards are credit cards provided by corporations to their employees for purchasing at selected outlets and businesses. This sector is likely to become the standard mode in B2B transaction.³⁶²

(4) Smart cards³⁶³

Smart cards are credit cards that contain a stored value embedded in a microchip inside the card. The advantage of the card over other forms of transactions is that it doesn't require approval from the bank for every transaction. It can be loaded from an ATM or Card Reader or Personal Computer and can be spent at outlets using appropriate machinery to record the transaction.

(5) Digital cash³⁶⁴

In using digital cash, both participants i.e. buyer and the seller must have a special bank account with an 'e-cash' issuing bank [known as 'mint'] and a suitable software for handing 'e-cash' transaction. The coins consist of unique, digital encrypted message, each of which corresponds to a particular denomination of the chosen currency, which are produced by the buyer PC using the 'e-cash' software. Then coins are then sent to 'mint' for validation and stored in the PC. When a

³⁶¹ Complied from Mundrey, n. 356, pp. 53-57; Stephenson and Bennet, n. 358, p. 70; Kavita Kaur, "Smart Cards: The Intelligent Key", *Computers Today*, 16-30 October 1999, p. 106, Singleton and Herlbertam, n. 38, pp. 183-190.

³⁶² Purchasing card transaction in 1997 totaled \$ 20 billion in U.S. and still growing in a faster pace. Quoted in Mundrey, n. 356, p. 56.

³⁶³ Mundrey n. 356, p. 56.

³⁶⁴ Stephenson and Bennett, n. 358, p. 74, <[http:// www. Digicash.com](http://www.Digicash.com)>.

purchase takes place, sufficient 'coins' will automatically be sent from the buyer's account to the merchant's account. At the point of transaction, the 'mint' will recognise the verification signature that it made on the 'coins' initially and the unique identification number on each 'coin' to ensure that it has not been previously spent. If the numbers are acceptable, the merchant is informed that payment is valid and the goods can be dispatched to the buyer. The whole process does not take more than a few seconds. The basic difference is that unlike traditional coins and currency, e-coins are not returned to circulation but rather are spent only once.³⁶⁵

Eg: Digital cash Inc. is an 'e-cash' facilitator.

(6) Micro payments³⁶⁶

The modes of transactions mentioned earlier, could be used effectively when a large amount is involved. For smaller purchases or where the service charge of the bank might be higher than the value of articles purchased, micro payment system could be used, where in small denominations of digital cash, known as micro cash is used.

(7) Electronic Cheque³⁶⁷

This system involves a hardware chequebook coupled with user's personal computer as well as additional hardware at the merchants' end. The consumer writes an electronic cheque, signs it with his digital signature and sends it to the merchant who then forwards it to an automated clearinghouse for processing and payments.

(8) Virtual PIN³⁶⁸

Introduced by First Virtual Inc, this can be used by those consumers who are not interested in providing their credit card details over the Internet. First Virtual provides the credit card number over a voice telephone and the issues Virtual PIN to the customer. Customers can use their Virtual PIN in lieu of credit card number. When purchasing is done, First Virtual sends the user e-mail asking him to confirm

³⁶⁵ Price Water House Coopers Report, n. 357, p. 156.

³⁶⁶ Joshua .B. Konvisser, "Coin, Notes and Bits: The case for legal Tender", *Harvard journal of Law & Technology*, vol.10, n. 2, (1997), p. 325.

³⁶⁷ Price Water House Cooper Report, n. 357, p. 156, Konvisser, Ibid.

³⁶⁸ Price Water House Cooper Report, n. 357, p. 156.

the transaction. Once it gets confirmation, the credit card transaction is produced off the Internet and e-mail is sent to the merchant authorizing to dispatch the goods.

(9) Digital Wallets³⁶⁹

Introduced by CyberCash and Verifone, this process involves a facilitator who provides an encrypted code that refers to the credit card number after wallet software has been set up by the consumer, i.e. a digital wallet is a collection of customer data necessary for completing payment transactions.³⁷⁰ When a purchase is carried out, the wallet passes the code to the merchant, who hands over this along with the purchase price to the Wallet issuer who in turn verifies the transaction with the credit card company and then transfers the fund to the merchant along with an authorization to ship the products.

(10) E Charge³⁷¹

The E CHARGE system allows customers to merge the web purchases to their normal telephone bills. But this facility is available only to merchants in the U.S and Canada³⁷².

(11) Traditional Payments Methods

Since most of the above methods are still in their infancy, the traditional payment methods such as paper cheques or cash on delivery are still the commonly used payment methods in e-commerce transactions.

The basic reason for the less flourishing B2C e-commerce sector can be attributed to the fact that the means of payment that the consumers require does not exist.³⁷³ Credit card system is a failure in case of micro purchases because the cost of credit card transactions generally exceeds the price of micro purchases.³⁷⁴ Similarly, on-line checking takes between twenty-four and thirty-six hours to clear. The need of

³⁶⁹ <<http://www.cybercash.com>>.

³⁷⁰ Digital Wallets are divided into site Wallets, Remote Wallets, Distributed Wallets and Personal Wallets.

³⁷¹ Price Water House Cooper Report, n. 357, p. 156.

³⁷² Mundrey, n. 356, p.

³⁷³ Konvisser, n. 366, p. 326.

³⁷⁴ "Micro purchases means prices of goods which are on the order of pennies or less", Cited in *The Economist* "Electronic Money: So much for the cashless society", Nov.26, 1994 at 2E.

the consumer is a payment system allowing for instantaneous exchange over the net, the transaction cost of which are low enough to make micro purchases feasible.

A CASE FOR E-CASH

E-cash is the most viable system for transactions over the net because it provides nearly instantaneous and inexpensive on-line transactions of any size and the e-cash system provides for anonymity, thus by making the e-cash token even more similar to hard cash.³⁷⁵

The major concerns that e-cash raises are broadly similar to the concerns relating to any new payment system, namely, the possibilities of misunderstanding, misdirection and misuse.³⁷⁶ In e-cash transactions care should be taken regarding the following areas:-³⁷⁷

- (1) The security of the transaction between payer and payee: this includes issues relating to privacy of transaction and precisely who should have access to the details of the payer.
- (2) The identity of the payer.
- (3) The irrevocability of the payment.
- (4) The identity of the cash issuer where some form of e-cash is being used.
- (5) The ease with which small value payments i.e. micro purchases can be handled.
- (6) The universality of acceptance of the type of e-payment.

A true e-payment system should allow for the transfer of value between individuals without the need for a physical meeting. Although e-cash is being touted as the most apt mode of exchange, there are several impediments associated with it

³⁷⁵ Konvisser, n. 366, p. 328.

³⁷⁶ Ibid.

³⁷⁷ Stephenson and Bennet, n. 361, p. 67.

for which the Governments and the policy makers have to find an answer. They are enumerated below:-³⁷⁸

(1) Integrity

(2) Counterfeiting

(3) Other difficulties

(a) Privacy

(b) Seignorage loss

(c) Crimes

(d) Tax

I. E-Cash and Problem with Integrity

Many modes of encryption are being developed to ensure integrity of transaction. In traditional encryption both the sender and the recipient share a single key.³⁷⁹ This has its own inherent problems.³⁸⁰ Firstly, as the user has to transfer the key to the recipient before sending the encrypted message, there are chances of cybertheft. Secondly the personal key and lock of the user becomes less secure with the number of transactions.

RSA encryption³⁸¹ is the solution to this problem, which ensures both integrity and non-reputability. The U.S. Government prohibits export of superior encryption technology, as it could be used to further terrorist activities.³⁸² This can prove to be a

³⁷⁸ Compilation cited in n. 361 and Konvisser n. 366, pp. 337-352.

³⁷⁹ Encryption systems uses "keys" for ensuring the secrecy of the message transmitted. Keys are a logarithm used for transforming a message into an unintelligible form and then back. Simon L. Garfinkel, "The key to safe Business on the Net", *Business weekly*, February 27, (1995) p. 86.

³⁸⁰ I bid, Russell Mitchell, 'The key to safe Business on the Net', *Business weekly*, February 27, 1995, p. 86.

³⁸¹ RSA encryption named after Ron Rivest, Adi shamir and Leonard Adleman, who invented this technique in 1976. It is also known as asymmetric key encryption or public key encryption. Principle is as follows. Mr. X generates Public and Private keys. Public key is disseminated to the world at large. Any message to X can be encrypted using this public key and sent via net, which in turn can only be decrypted with Mr. X's Private key as there is a mathematical relationship between the two.

³⁸² Currently Expert Administration Regulations (EAR) prohibits "encryptions items" which includes all encryption commodities, software and technology that contain encryption features". 15. C.F.R section 772 (1998). Before this enactment, encryptions were controlled under Arms Export Control Act [22 U.S.C section 2751 (1994)] and International Traffic in Arms Regulations (22. U.S.C. 2778 (a) (1) (1994) where these were placed under United States Munitions list.

disadvantage, if the technology cannot keep in pace with the varying needs of the e-commerce.

II. Counterfeiting

In cyberspace, anything could be illegally copied and distributed across the globe in a matter of seconds. Since counterfeiting of e-cash could destroy the entire trading system, it is one of the major concerns of e-commerce.³⁸³ The technology used in Digital Cash³⁸⁴, when extended to other modes of transaction, could effectively contain this menace.

III. Other Difficulties with E-Cash

(a) Privacy

Guaranteeing a modicum of privacy is essential to the widespread use of e-commerce application over the information infrastructure.³⁸⁵ The consumers would certainly be concerned if each purchase is recorded for reporting to marketers or others. The existing legal structure doesn't support the implementation of an anonymous e-cash system. E-cash will markedly lower existing barriers to the transfer of funds across borders. Without imposing severe restrictions on individual privacy, governments may be hard pressed to track, account for, or control the flow of money across the borders. The present practice requires financial institutions to keep records of transactions, reporting to the Government, when asked to. If e-commerce is to thrive, it should not be the transactions with financial institutions that must be kept anonymous, but the individual cash transaction between non-financial institutions.³⁸⁶

(b) Seignorage loss

Daniel. R. Rua, "Cryptobabble: How Encryption Expert Disputes are shaping Free Speech for the New Millennium", *North Carolina J. of International Law and Commerce Regulations*, vol.24, No: 1, (1998), pp. 138-139, Yvonne C. Ocrant, "A constitutional challenge to encryption Expert Regulations: Software is speechless", *DePaul Law Review*, vol.48, No: 2 (1998), p..509-11.

³⁸³ Information Infrastructure Task Force, *Natural Information Infrastructure Security: The Federal Role* (1995) available at <http://www.uark.edu/niiac/fed_role.html>.

³⁸⁴ <http://www.digicash.com/e-cash/about_security.html>

³⁸⁵ Information Infrastructure Task Force, office of management and Budget, *Common Ground: fundamental Principles for the National Information Infrastructure* (1995) <<http://nii.nist.gov/pubs/common-ground.txt>>.

³⁸⁶ Konvisser, n.366, p. 347.

Many Governments indicate that if private currencies are allowed to circulate, then it may result in the seignorage losses for them.³⁸⁷ If the usage of Government printed currency is displaced by private e-cash, the government will have to respond by containing the money supply in order to fight inflation. The loss of money as seignorage gains will be to the extent of reduction in the total volume of circulated currency.³⁸⁸

Government issued electronic money would probably stem seignorage losses. Government issuance will provide legal status to e-money making it equivalent to hard currency, which “will help to promote the public trust required for the acceptance of any monetary system by the merchant and the consumer, who will use it.”

The U.S. government is actively watching the development of e-commerce without taking any real action in this particular area. The Federal Reserve is hesitant to incur the costs of minting electronic cash, in the absence of reliable evidence that the system will be a success.³⁸⁹

(c) Crimes

Major crimes in respect of e-payments are money laundering and embezzlement.

(i) Money laundering

Still another concern is that a successful e-cash regime will facilitate crime;³⁹⁰ A number of features of e-cash namely the rapidity of e-cash exchanges, the inability to mark bills in an anonymous transaction system and the inability of law enforcement officials to witness the transfer of large amounts of cash, render it particularly well suited for illegal money laundering.³⁹¹

³⁸⁷ I bid at 843.

³⁸⁸ Vanersa Houlder, “Delving into standards for a cashless society”, *Financial Post*, Feb. 21, 1996, p. 6.

³⁸⁹ Konvisser, n. 366, p. 343.

³⁹⁰ Penny Lunt, “Payments on the Net: How many? How safe? *ABA Banking Journal*, Nov. 1, (1998) at p. 54. Lunt quotes Stanley, Harris, Director of Treasury Department Financial Crimes Enforcement Network, “the changing technology could open up potential for money laundering, counterfeiting, credit card fraud and other frauds”

³⁹¹ Money laundering means causing impediments to trace illegally acquired money by passing it through ostensibly legitimate commercial transactions.

Limiting the e-cash transactions to micro purchases and defining a class of 'suspect transactions' like those above a certain amount and isolating this class for recording could be an answer to these problems.³⁹²

(ii) Embezzlement within the bank industry

There are serious apprehensions that e-cash system could be embezzled from within the banking industry.³⁹³ While current auditing schemes having time lags, e-cash transactions are almost instantaneous making the thief stealing e-cash to disappear before the audit could uncover any evidence of foul play. Embezzlement may be more severe, if unregulated non-bank entities, such as Microsoft and Intuit are allowed to mint and issue e-cash.³⁹⁴ With no regulatory framework to guide on-line auditing, internal thefts could become nearly impervious to direct Governmental action.

Limiting e-cash issuance to government and e-cash banking functions to regulated banks, together with appropriate regulatory framework, could avoid this problems to a great extent.

(d) Tax considerations

Another concern is the feasibility of a mechanism for taxing e-cash transaction.³⁹⁵ What complicates the matter is that e-commerce transactions might involve consumers, sellers and a host of network of servers, who belong to different states with varying laws of taxation. In *Quill corporation v. North Dakota ex rel Heitkamp*³⁹⁶ the U.S. Supreme Court held that states may impose taxes on out-of-state vendors only if they have a "physical presence" within the state.³⁹⁷ The question then would be, whether a local server constitutes a 'physical presence' to satisfy Quill.³⁹⁸ Then, for collection of tax, will the state governments be given authority or will the

³⁹² Konvisser, n.366, pp. 349-350.

³⁹³ Lunt,,n. 390, p. 29.

³⁹⁴ Ibid.

³⁹⁵ I bid.

³⁹⁶ 50A U.S. 298 (1992).

³⁹⁷ Physical Presence requirement has been interpreted to include stores, factories and other commercial facilities. I bid at page 317.

³⁹⁸ Cyber space transaction cannot be taxed based on Quill's ratio. Julie .M. Buechler, "Virtual Reality: Quills 'Physical Presence' Requirement Obsolete when cogitating use Tax collection in cyberspace", *North Dakota Law Review*, vol. 74, (1998), pp. 479-507.

central government directly exercise it under its power to regulate inter state commerce.

Further there can be problems of individuals storing money in computers located outside the country in order to evade the incidence of local income tax.³⁹⁹

Summary

The problem facing the governments is how to set up a regulatory body for regulating the electronic cash. Any methods device should require international cooperation, as the e-commerce has no boundaries. Consumer's request will be pouring from different corners of the world. The government should derive a policy to track e-cash without indulging into the privacy concerns of its citizens. The developed countries should be willing to part with their latest technologies so that commerce may not lag for want of technology.

³⁹⁹ Kelly Holland & Army Coster, "The Future of Money: E-cash could transform the world's Financial life", *Business weekly*, June 12, 1995, pp. 66-78.

WEB ADVERTISING

Internet advertising is at the convergence of Traditional Advertising and Direct Response Marketing.⁴⁰⁰ The online advertising has a many fold advantage over the traditional advertising due to its characteristics⁴⁰¹ like targetability,⁴⁰² tracking⁴⁰³ deliverability and flexibility⁴⁰⁴ and interactivity⁴⁰⁵.

Business has been quick to realise the advertising and market potential of the Internet than as a Worldwide-trading medium. The global Internet advertisement was of the value of \$ 906 million, \$ 1,730 million and \$ 3,000 million in the years 1997, 1998 and 1999 respectively as compared to a meagre Rs.6 crores in 1999 in India which is expected to reach Rs.15 crores by 2000⁴⁰⁶. The Aberdeen Group predicts that the global advertising revenue will reach \$ 5.1 billion by the end of 2000⁴⁰⁷.

The various Ad models for the businesses to advertise online falls into categories.

- (1) Advertising via e-mail.
- (2) Banner advertising.⁴⁰⁸
- (3) Buttons⁴⁰⁹
- (4) Text lines or 'Amazon.com' Style links⁴¹⁰.

⁴⁰⁰ Robin Zeff and Brad Aronson, *Advertising on the Internet*, (New York, 1999), p. 13.

⁴⁰¹ Ibid.

⁴⁰² Online advertisers can target their ads to specific users depending on their personal preferences, actual behaviour or specific database or companies etc.

⁴⁰³ Advertisers can track the response to the advertisement through the number of clicks the ads got or the number of purchases or leads an ad generated.

⁴⁰⁴ Ads are delivered 24 hours a day, 7 days a week, 365 days a year. Moreover an ad campaign can be launched, updated or cancelled immediately.

⁴⁰⁵ Consumers can interact with the product, test the products and then purchase e.g. Digitized Services like software, Music etc.

⁴⁰⁶ Goldman Sachs Report, cited in *Computer Today*, November 16-30, 1999, p. 60.

⁴⁰⁷ <<http://www.Aberdeen.com>>.

⁴⁰⁸ Banner advertisements are rectangular shaped ads blocks seen on every WebPages either at the top or towards the sides. Banners are divided into Static banner, Animated Banners. Interactive banners, HTML banner and Rich Media. Zeff and Aronson, n. 400, p. 46.

⁴⁰⁹ Small banner type advertisements that can be placed anywhere on a page and are linked to the button sponsor. Zeff and Aronson, n. 400, p. 46.

⁴¹⁰ Used by Amazon.com where a link is created to the Amazon.com's site when a search request is given, directing the customer to a list of books or records matching the search request. Jeremy Dickerson, David Savage, Ken Chia, "E-communicate" in Stephen York and Kenchia (ed), "E-COMMERCE – A Guide to the Law of Electronic Business," Butterworths, London, 1999, p. 16.

- (5) Sponsorships⁴¹¹.
- (6) Advertorials⁴¹².
- (7) Interstitials⁴¹³.
- (8) Screen Savers⁴¹⁴.
- (9) ISPs⁴¹⁵.
- (10) Cursor⁴¹⁶.
- (11) Portals and search engines⁴¹⁷.
- (12) Linking website with an e-mail address to facilitate the provision of data to the advertiser.⁴¹⁸
- (13) Spamming.⁴¹⁹

Pricing Of Advertisements

Pricing is done using a method known as CPM (cost per thousand page impressions). In the US sites usually charge between \$ 10 and \$ 100/CPM for a banner ad. Search engines and portals charge about \$ 18 to \$ 30/CPM. Financial news sites between \$ 49 to \$ 51/CPM and technology sites charge \$ 56 to \$ 70/CPM.⁴²⁰ Other Pricing models are 'click through'⁴²¹, 'Flat Free'⁴²², and 'pay per purchase'.⁴²³

⁴¹¹ Advertisements that entirely sponsors the specific aspect or feature of a site. For e.g. Charles Schwab sponsors the personal stock tracker on Exite.com. Zeff and Aronson, n. 400, p. 50.

⁴¹² It is Sponsorship that looks more like an editorial than like an advertisement. Zeff and Aronson, n. 400, p. 51.

⁴¹³ Ads that pop out to the Screen and interrupt users. They are usually called "Pop-ups", 'e-mercials' or 'intermercials'. Zeff and Aronson, n. 400, p.55.

⁴¹⁴ The entire Screen Savers itself can be an advertisement <<http://www.SaveScreen.com>>. Allows consumers to build their own personalized screen Savers containing integrated advertising. Zeff and Aronson, n. 400, p. 60.

⁴¹⁵ Even ISPs, are offering free Internet access for viewing ads. eg: Netzero (<<http://www.netZero.com>>). Zeff and Aronson, n. 400, p. 62.

⁴¹⁶ Cursors can be turned into an ad, for a unique form of branding. <<http://www.CometSystem.com>> has pioneered away to customize the mouse cursor, substituting graphic or animation for the conventional arrow.

⁴¹⁷ Majority of customers comes to know about a particular Web address from a search engine. So one of the way to got known, is to register with the search engines like yahoo! Alta Vista etc and provide the keywords of your business in the Meta tags.

⁴¹⁸ Len Keela, *Cyber Marketing*, (New York, 1995). pp. 181-182.

⁴¹⁹ Barbara, K. Kaye and Norman J. Medoff *The World Wide Web* (California, 1999),p. 248.

⁴²⁰ Goldman Sachs Report, cited in *Computer Today*, November 16-30, 1999, p. 60.

⁴²¹ Payment is based on the number of clicks generated by the ad. Zeff and Aronson, n. 400, p. 154.

⁴²² Charged either monthly or yearly for Ad placement. Zeff and Aronson, n. 400, p. 157.

Legal Issues of Advertisements

Problems arise in the area of Web ads primarily due to the fact that National laws are used for regulating advertisements on the net, which are disseminated to the world at large. In legal terms, jurisdiction is the most vexing issue affecting web advertising. Currently there is no international unanimity as to whether the laws applicable would be that of the country of origin [i.e. the place where the advertisement is put on the web] or the country of publication [i.e. place where the advertisement is received]. The traditional legal position is the latter, but this is recognized as impractical. The general approach illustrated by the existing cases⁴²⁴ is that the laws of “country of publication” will apply or in other words those laws of the countries in which there is evidence of ‘directed activity’⁴²⁵ will apply.

The web ads as a result of its “global reach” might breach many laws. In U.K. alone there are more than 150 different Acts⁴²⁶ and many statutory instruments affecting advertising and 20 main different bodies having their own codes, which are members of the committees of advertising practice.⁴²⁷

⁴²³ Payment will be a percentage of sales created by the advertisement. Zeff and Aronson, n. 400, p. 162.

⁴²⁴ The U.S. department of transportation fined \$ 14,000 on virgin Atlantic Airways in 1996 for publishing a false advertisement on its U.K. server, whom it was found out that they were quoting inaccurate fares and showing false fare list for flights from U.S.A. Dickerson, Savage, and Chia, n.410, p. 16.

⁴²⁵ In *U.S. v. Thomas* [1996 FED App. 0032 P (6 their) II. C.2] The operators of a pornographic electronic bulletin board in California was convicted of criminal obscenity Laws by the Federal Court in Tennessee, based on Tanners Standards of decency, holding that the site had every intention of directing activity in Tennessee although there was a general disclaimer to that effect. Ibid.

⁴²⁶ The main pieces of legislation regulating Advertisements in U.K are

- (1) Trade Descriptions Act, 1968.
- (2) The Consumer Protection Act, 1987.
- (3) The Control of Misleading Advertisement Regulations, 1988.
- (4) The Prices Act 1974.
- (5) The Undirected Goods and Services Act, 1971.
- (6) The Trade Marks Act, 1994.
- (7) The Copyright, Designs and Patents Act, 1988.
- (8) The Data Protection Act, 1984
- (9) The Defamation Acts 1952 and 1996
- (10) The Obscene Publications Act 1959 and 1964.
- (11) The Lotteries and Amusements Act, 1976.

⁴²⁷ Dickerson, Savage, and Chia, n.410, p. 15.

The legal problems that an e-trader may have to face can be categorised as⁴²⁸:

- (I) Comparative advertising.
- (II) Privacy issues.
- (III) Meta tags.
- (IV) Linking and framing.
- (V) Spamming.
- (VI) Direct e-mail and advertising.
- (VII) Advertising regulated goods and activities

(1) Comparative advertising

Comparative advertising is more prevalent today than ever before⁴²⁹. Comparisons, explicit or implied, specific or vague lie at the roof of modern advertising. It is seen as a legitimate, useful and effective marketing tool to convey a major competitive advantage. The U.S. (U.K. to a lesser extent)⁴³⁰ has encouraged comparative advertising on the basis that it is in the interest of consumers to be better informed. Most EU countries have taken the opposite approach [e.g. Germany], regarding it as an unfair competition. The net result is that lawful comparative web advertisement in one-member state is likely to breach to rules in another.

The major legal issue with comparative advertising is trademark infringement. By its very nature, an advertisement of one company comparing itself to another must incorporate the other company's name and/or trademark⁴³¹. The use by one company of another's trademark is any way historically considered as a trademark infringement.

⁴²⁸ Chissick and Kelman n. 5, pp. 184-191,

⁴²⁹ Comparative advertising is one in which the advertisement implicitly or explicitly refers to a competitor or its trademark or to goods or services offered by it.

⁴³⁰ U.K. Laws permit comparative advertising subject to the voluntary codes and the laws on Trademarks, Intellectual Property, Consumer Protection and Defamation. Under the Trademarks, Act 1994, Comparative Advertisements is mentioned under see 10 (6). Explained elsewhere in the chapter.

⁴³¹ For example, in the case of *Mc Donalds Hamburgers Ltd V. Burger king (UK)*, which alleged trademark infringement on Burger King whose advertisement caption was "Not just Big, Mac", Mac being the trademark of McDonalds.

The relevant provision dealing with comparative advertising in the UK Trademarks Act 1994 is section 10(6), which reads: -

“Nothing in the proceeding provision of this section [infringement provision] shall be considered as preventing the use of a registered trademark by any person for the purpose of identifying goods or services as those of the proprietor or a licence. But any such use otherwise than in accordance with honest produces in industrial or commercial matters shall be treated as infringing the registered trademark, if the use without due cause takes unfair advantage of or is detrimental to the distinctive character or repute of the trademark.”

The interpretation of this clause is currently something of a grey area⁴³². Hence while engaging in comparative advertisements or litigating against it, the dealer may not the case laws⁴³³ under section 10(6) which has so far laid down as follows:⁴³⁴

(1) The onus is on the trademark proprietor to show that the third party’s use which is complained of is not in accordance with honest practices in industrial or commercial matters or takes unfair advantage of or is detrimental to the distinctive character or reputation of trademark.

(2) “Use in accordance with honest practices”- test mentioned is an objective one. If members of a reasonable audience consider the use honest, then it will not infringe. If not honest, then the protection from trademark infringement is unavailable.

(3) The degree of hyperbola acceptable would depend on the nature of the product.

⁴³² Mr. Justice Laddie has stated in *Barclays Bank V. RBS Advanta* [(1996) RPC307] that ‘the primary objective of s.10 (6) was to legalese comparative advertising but it is in a mess’. This may be due to the fact that the phrases ‘honest practices’ ‘without due cause’... ‘takes unfair advantage’ ...are not defined and are new to English Law.

Dickerson, Savage, and Chia, n.410, p.19

⁴³³ The leading cases are *Barclays Bank v. RBS Advanta* [(1996) RPC 307], *Vodafone Group plc v. Orange Personal Communications Services Ltd* [(1997) 5 EIPR D-134] and *British Telecommunications plc v. AT&T Communications (U.K) ltd* [18 December, 1996, unreported]. Dickerson, Savage, and Chia, n.410, p. 19.

⁴³⁴ Dickerson, Savage, and Chia, n.410, pp. 19-20.

(4) The advertisement must in all cases be considered as a whole and not broken down into minute details. Minute textual examination of an advertisement is not something on which the reasonable reader would embark and therefore neither should the courts.

(5) The omission of certain facts may in certain circumstances be dishonest if, for instance, it would be significantly misleading.

(6) The more precise the claim is, the more likely it is to be construed as a serious claim by the public and therefore would almost certainly be seen as misleading or dishonest if not entirely true.

A. A.S.A. codes of practice

The Advertising Standards Authority (A.S.A.) is an independent body that regulates the British Codes of Advertising and Sales Promotion, which governs advertising and sales promotion in U.K. If any individual or Business wants to make a complaint regarding an advertisement, which have breached the advertising codes, it can complain before the A.S.A. The A.S.A. codes permit comparative advertisements in the interests of vigorous competitions and public information.

A.S.A. codes⁴³⁵ dealing with comparative advertisement is enumerated in section 19. According to section 19(1), comparison can be explicit or implied and can relate to advertisers' own products or to those of their competitors. Section 19(2) states that comparisons should be clear and fair and the elements of any comparison used should not be selected in a way that gives the advertisers an artificial advantage.

With a view to harmonising the law in the EU, the European Commission has adopted a Directive on Comparative Advertising.⁴³⁶ The Directive states that comparative advertising shall be permitted when a few conditions⁴³⁷ are met. The

⁴³⁵ www.asa.org.uk.

⁴³⁶ Directive 97/55 published in O.J. L290 Vol. 40, 23.10.97.

⁴³⁷ The conditions mentioned under Art 3 (a) are

- (1) The comparison is not misleading.
- (2) It compares like with like.
- (3) The comparison objectively compares one or more material, relevant, verifiable and representative features of these goods and services, which may include price;
- (4) The comparison does not create confusion in market place between the advertiser and a competitor or between the advertisers' trademarks, trade names, other distinguishing marks, goods, services, activities or circumstances of a competitor.

U.K. government current position is to adopt the Directive by means of an amendment to the Misleading Advertising regulations.⁴³⁸

Other relevant codes

The International Chamber of Commerce (ICC) has brought out guidelines on Webadvertising. ICC⁴³⁹ promotes high standards of ethics in marketing and advertising on the Internet via self-regulating codes. Advertisements containing comparisons should not mislead and should comply with the principles of fair competition, national laws and regulations concerning comparative advertising. ICC guidelines state that points of comparison should be based on facts, which can be substantiated and should not be unfairly selected. According to ICC, legality of Webadvertisements should be determined with reference to the laws of country of origin of the advertisements.

(II) Collection and Use of Personal Data

The ability to collect data through on-line survey marketing and browser technology has obvious advantages for on-line marketers. At the same time, it raises privacy concerns for regulators. European Law has been the most aggressive in protecting consumers' personal data on the Internet.

The Council of Better Business in the U.S. [the equivalent of U.K.'s A.S.A] has launched its own privacy policy interactive that will allow complaint sites to display its seal of approval. In U.K., the Data Protection Act 1998 (DPA), places even greater responsibilities to the 'data collector' who has to fairly process the personal data and comply with the eight data protection principle.⁴⁴⁰ Moreover the e-merchant

-
- (5) The comparison does not discredit or denigrate the trademarks, other distinguishing marks, goods, services, activities or circumstances of a competitor.
 - (6) For products with designation of origin, the comparison relates in each case to products with the same designation.
 - (7) Comparison does not take unfair advantage of the other mark or product and
 - (8) The comparison does not present goods or services as invitations or replicas of goods or services bearing or protected trademark or trade names.

⁴³⁸ Chissick and Kelman n. 5, p. 185.

⁴³⁹ Guidelines are available at www.icwbo.org/commissions/marketing/internet-guidelines.html.

⁴⁴⁰ The eight principles enshrined in the UK Data Protection Act (DPA) and EU Data Protection Directive which must be followed are

- (1) Personal data shall be processed fairly and carefully and in particular shall not be processed unless
 - a. At least one of the conditions in sch 2 is not met;

should provide the security warning that the data requested during a visit to company's website by the subject that the data may not be secure during transmission from one server to another ⁴⁴¹ Data Subjects have a explicit right to 'opt-out' of having their data used for direct marketing purposes and controller must cease such use within a reasonable period of receiving a request to do so. The DPA also prevents also prevents the data being transferred to countries outside the EEA unless those countries have adequate data protection laws in place or the individual has consented.

Failure to comply with U.K. Data Protection Act⁴⁴² may result in criminal penalties for companies and their individual managers in U.K.

(III) Meta tags

The practice of using numerous Meta tags for advertising of a site is generally legitimate but problems may arise when these tags include the trademarks of another party. Trademark owners often object to this practice because, just like similar domain names, they divert customers away from their own websites.

-
- b. In the case of sensitive personal data, at least one of the conditions in sch 3 is also met.
- (2) Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
 - (3) Personal data shall be adequate, relevant and not excessive in relation to the purposes or purposes for which they are processed.
 - (4) Personal data shall be accurate and, where necessary, kept up to data.
 - (5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
 - (6) Personal data shall be processed in accordance with the rights of data subjects under this Act.
 - (7) Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
 - (8) Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

⁴⁴¹ A notice can be pasted in the web page on which the requisition form is for downloading that "e-merchant will not guarantee that the information will be secure during transmission to our web server."

⁴⁴² The UK, Data Protection Act (DPA) will apply

- (1) If you are established in UK i.e. are ordinarily, resident, a UK incorporated body, partnership or unincorporated association or have an office, branch or agency which carries or any activity or a regular practice in UK;
- (2) If you are not established in the EEA but use equipment in the UK for processing data (unless the information is merely in transit).
- (3) Practically, if data is exported to you from the UK.

Although there is no U.K. case as yet on the topic,⁴⁴³ US Federal Appeals Court in California has mapped out the dos and don'ts of the Meta tag use. In a dispute over the use of "moviebuff.com",⁴⁴⁴ the court basically extended the concept of 'initial-interest confusion' used in *Dr. Seuss*⁴⁴⁵ and *Mobil Oil Corporation v. Pegasus Petroleum Corporation*⁴⁴⁶ to Meta tag cases and concluded that: -

" When a firm uses a competitor's trademark in the domain name of its website, users are likely to be confused as to its source or sponsorship. Similarly using a competitor's trademark in the Meta tags of such website is likely to cause what we have described as initial interest confusion. These forms of confusion are exactly what the trademarks laws are designed to prevent. Using another's trademark in one's Meta tags is much like posting a sign with another's trademark in front of one's store."⁴⁴⁷

The emphasis of this judgement is on "fair use" and the court added that not every use of a Meta tag would infringe the trademark owner's right: -

" We are not in anyway restricting west coast's right to use terms in a manner which would constitute fair use under the Lanham Act, 1984. Fair Use doctrine applies in cyberspace as it does in the real world."⁴⁴⁸

(IV) Linking and Framing

Linking has benefits such as increasing the potential audience of a site but it can also bring undesirable results. A link may be to a specific item on the site and causes browsers to bypass the homepage, where there might be advertisements which the site owner would have wished all visitors to see. Similarly in Framing, sometimes the advertisement of the framed page will be blocked by the framing site. Thus Linking and Framing could affect the potential advertising revenue, if they carry the third party advertisements or violate sponsorship obligations in the process.

⁴⁴³ But if there are cases alleging Meta tag violation in UK, then see 10 (6) of the Trademark Act, 1994. Dickerson, Savage, and Chia, n.410, p. 24

⁴⁴⁴ *Brookfield Communications Inc v. West Court Entertainment Corporation*. [<http://www.vcilp.org/Fed-ct/circuit/9th/opinions/9856918.htm>].

⁴⁴⁵ 109 F 3d at 1405. Dickerson, Savage, and Chia, n.410, p. 23.

⁴⁴⁶ 818 F 2d 254,257-58 (2d cir 1987) 24. Ibid.

⁴⁴⁷ Dickerson, Savage, and Chia, n.410, p. 23.

⁴⁴⁸ Ibid.

Recent cases in the U.S. and the U.K. point to unauthorised links on the basis that they may infringe copyright, trademark and related business reputation rights. *The Shetland Times Case*⁴⁴⁹ has given an indication of the attitude of the U.K. courts on the question of copyright infringement by hyperlinks. Similar would have been the results in the U.S. in *Ticket Master v. Microsoft Case*.⁴⁵⁰

The Courts through various decisions had already pointed out that framing, constitute copyright and trademark infringement.⁴⁵¹

The Courts of countries other than U.S. or U.K. could take a different attitude towards linking and framing liability. Till the issue is finally resolved, “deep linking” into the website of a third party is to be avoided. Linking to a third party homepage may be less risky.⁴⁵²

(V) Spamming⁴⁵³

Direct marketing in Internet involves largely the use of e-mails to reach consumers. Usually customers will subscribe to a mailing list, but usually and increasingly, these take the form of unsolicited commercial e-mails (Spam). It is irritating to consumers, as they have to spend on-line time downloading and reading the Spam. It poses a threat to consumer confidence in e-commerce because lately fraud operators involving fictitious information about the sender, misleading subject lines and extravagant claims or earnings or performance about goods and services or chain letters and pyramid selling have used it. Spamming also burdens ISP and frustrates their customers who have to suffer poorer performance levels. This is unfair because the recipient bears much of the cost of access and the service providers bear much more of the cost providing the infrastructure than the sender does (if at all).⁴⁵⁴

These concerns have led large service providers like AOL⁴⁵⁵ to litigate successfully against Spammers. In U.S. various legislative measures⁴⁵⁶ are being

⁴⁴⁹ A copy of courts opinion can be found at <<http://www.jmls.edu/cyber/cases/shetd1.htm>>.

⁴⁵⁰ Civ. No. 97-3055 (DPP) (C.D.Cal.1997)

⁴⁵¹ Mentioned under copyright in page-----.

⁴⁵² Ibid.

⁴⁵³ Spamming is sending unsolicited junk e-mails.

⁴⁵⁴ Susan Singleton, n.38, p. 178.

⁴⁵⁵ *AOL V- LCDN* (10 Nov 1998) (US District Court for the earlier District of Virginia) cited in *Electronics Business Law*, April 1999, p. 15.

introduced to stop spamming at both Federal and state level. In U.S., the ISPs have sued Spammers under the following headings.⁴⁵⁷

- (1) The Computer Fraud and Abuse Act, 1920 (For knowingly and intentionally causing the transmission of information to and accessing, protected computer facilities without authorisation and as a result recklessly causing damage).
- (2) The Lanham Act (for false designation of origin, Dilution of trademark).
- (3) Various State Computer Crimes Acts.
- (4) Conversion or trespass to chattels under common law.

In U.K., there have been no reported decisions yet, but liability under the Torts (Interference with Goods) Act 1977, the Computer Misuse Act 1990 and Trademark and Passing off Law may be insisted. LINX,⁴⁵⁸ the London Internet Exchange List, provides its members with guidelines referred to as "LINX Best Current Practice for which as follows⁴⁵⁹ combating Unsolicited Bulk E-mail.

- (1) ISP must ensure that their e-mail system will not relay e-mail for unauthorised third parties.
- (2) ISP must ensure that all e-mails generated with in their network can be traced to its source.

AOL sued the defendants for sending a huge number of unsolicited e-mails advertising their pornographic website to AOL members. As many as 92 million web messages at the rate of 300,000 per day have been sent from AOL's server. AOL were the injection. Their claim was based on

- (1) Dilution under US Trademark Law (e-mails contained AOL.com in the heading).
- (2) Trepan to chattels (As AOL's property was used without consent).

456

The U.S. Position

There are presently four pending pieces of legislation, which are designed to prevent unsolicited commercial e-mail (Spam).

- (1) Unsolicited Commercial Electronic Mail Choice Act of 1997 (S.771).
- (2) Electronic mailbox protection Act of 1997 (S.875).
- (3) Netizens Protection Act (HR. 1748).
- (4) E-mail Users Protection Act of 1998 (HR 4124).

In U.S., states like California, Nevada, Washington, Massachusetts, and Connecticut have passed anti-spamming legislation. In California, spamming insures criminal liability (up to one years fail) and the e-mail service provider can recover their actual monetary loss or liquidated damages of \$ 50 [per e-mail (maximum \$ 25,000 a day). in Washington recipients can called \$ 500 for each piece of Spam. Supra Note 8, p. 25.

457

I bid.

458

LINX is London. Internet Exchange Ltd, which regulates the ISPs. It has currently 72 members and represents the main UK ISPs together with ISPA.

- (3) The ISP must ensure that all e-mail generated within their own networks can be attributed to a particular customer of system.
- (4) The ISP must operate appropriate arrangement for handling reports of abuse by their customers and must take effective steps to prevent the customers from sending further Unsolicited Bulk e-mails (UBE).
- (5) ISP must disseminate information on the action taken in regard to customers who sent UBE.
- (6) ISP must make its customers aware that sending UBE will be treated as unacceptable behaviour.

The best practice document also contains suggested specimen clauses which the customers should check, whether the ISP have included these terms and conditions in their agenda.

(VI) Direct e-mail Advertising

Well-known manufacturers use solicited e-mail to give their consumers information they have requested about available products, service and sales. This is a cheap and effective method of advertising because customers can be reached anywhere in the world at a very little cost. The U.K. Direct Marketing Association (DMA)⁴⁶⁰ urges that all advertisements must comply with ASA standards. Accordingly the following information must be included in any direct marketing material sent by e-mail.⁴⁶¹

- (1) How a consumer should exercise any right to withdraw from any contractual obligations.
- (2) How to cancel any open-ended commitments entered into as a direct result of the e-mail material.
- (3) Other terms and conditions such as guarantees of any contract entered into for advertised products.

⁴⁵⁹ <<http://www.linx.net/noncore/bcp/ube-bcp.html>>.

- (4) The member's address where consumers may contact them with a complaint or enquiry.

E-mail advertising is also regulated in the U.K. by the Distance Selling Directive,⁴⁶² which urges the members States to ensure that all means of distance marketing communications, unsolicited or not, including electronic mails, traditional mail Shots and calls will be used only when there is no clear objection from the consumers. Consumers should be given the opportunity to register his/her objection to receiving such communication.⁴⁶³ Whichever form of communication is used, the identity of the suppliers and the commercial aim of the communication will have to be stated at the outset.

(VII) Advertisement of Regulated activities, goods and services

Certain types of advertising are banned in some jurisdictions. Electronic commerce business must therefore be alert to the potential sensitive nature of the global audience to whom they offer their products. Web advertising in 3 sectors have received particular attention namely tobacco, alcohol and children.

A. Tobacco advertising

Advertising tobacco products should be taken special care especially in Europe. On July 6, 1998,⁴⁶⁴ the tobacco Advertising Directive was adopted by the E.U, which imposes a ban on all forms of advertising and sponsorship.⁴⁶⁵ The ban will be applicable to all forms of communications or sponsorships, which have a direct or indirect effect of promoting a tobacco product, including the use of any distinctive features of tobacco products such as trademarks or logos.

⁴⁶⁰ DMA deals with the code of conduct for marketing and Advertising activities in U.K. the rules and regulations regarding Internet advertisement are also regulated by it.

⁴⁶¹ Dickerson, Savage, and Chia, n.410, p. 26.

⁴⁶² Chissick and Kelman, n. 5, p. 188.

⁴⁶³ Options are either an opt-in or an opt-out system.

⁴⁶⁴ Directive 98/43 relating to advertising and sponsorship of tobacco products. O.J. L 213/9.

⁴⁶⁵ The first implementation date is July 30, 2001. A five year transitional period is allowed considering press, Sponsorship and exceptional global event sponsorship. By Oct 1, 2006 all the provisions of the directive are to be implemented.

B. Alcohol advertising

The Broadcasting Directive,⁴⁶⁶ which prescribes the rules of advertising in EU. It urged the market states to adopt stricter rules than those laid down in the Directive.⁴⁶⁷ This has led various countries, most notably France, banning alcohol advertising altogether. In most Arab countries, alcohol is a banned product. Hence the web advertisers should be careful when dealing alcohol advertising.

C. Advertising to Children

Many countries ⁴⁶⁸ have placed outright bans or heavy restrictions on advertising to children. In the U.K., ⁴⁶⁹ these are based on both voluntary codes and stature. The U.S. is however ahead of EU on the protection of children online. The children's on-line Privacy Protection Act requires commercial website operations to provide clear notice of their information collection practices and obtain parental consent prior to eliciting personal information from children under the age 13. It also urges parents to access and check such information and curtail its use.⁴⁷⁰

Indian Law

In India also, various statutory bodies and organisations regulate advertisements. There are different codes for advertising in All India Radio or on Doordarshan or in Print Media. In all these advertisings codes, it is mentions fifteen laws, which are to be taken into consideration while advertising in India.⁴⁷¹ These are Drugs and Cosmetics Act, 1940; Drugs Control Act, 1950; Drugs and Magic Remedies (objectionable advertisement) Act, 1954; Copyright Act, 1957; Trade and Merchandise Act, 1958; Prevention of Food Adulteration Act, 1954; Pharmacy Act, 1948; Prize competition Act. 1955; Emblem and Names (Prevention of Improper Use) Act, 1950; Consumer Protection Act, 1986; Indecent Representation of Women (prohibition) Act, 1986; AIR/Doordarshan Code; Code of Ethics for advertising in

⁴⁶⁶ The Television Without Frontiers Directive. 89/552 and 97/36.

⁴⁶⁷ According to the Directive, advertising of any product containing 1.2 percent by volume of alcohol or above is banned. Moreover the advertisement cannot give the impression that the consumption of alcohol can lead to increased success.

⁴⁶⁸ In October 1994, the Greek Government banned advertising of toys on television between 0700 hrs and 22 hrs. Sweden has a ban on T.V. advertising to children under age of 12. Spain operates a defacto ban on the advertising of "war toys" on T.V.

⁴⁶⁹ Goldman Sachs Report, cited in *Computer Today*, November 16-30, 1999, p. 60.

⁴⁷⁰ Chissick and Kelman, n. 5, p. 187.

India issued by the Advertising Council of India; Code of standards in relation to the advertising of medicines and treatment and Standard of Practice for Advertising Agencies.

⁴⁷¹

D.V. Gandhi, *Advertiser's Hand Book 1999-2000*, (New Delhi, 1999), p. 116.

The International Response To Regulating E-Commerce

Internet is a network of networks, started for furthering military communications. It was then taken over by the academic institutions, which helped them to further the dissemination of information across the globe. The business opportunities on the net were found out late in the mid 90's and the race was on to establish a presence on the web. The question, who is in charge of the web, often has no definite answers.

Internationally many organisations came forward to strike an understanding among their members. These include UNICTRAL, OECD, EU, ICC, APEC, WTO, WIPO, and ECE. The international approach enumerated here, analyses the work of WIPO, WTO and UNCITRAL in regulating e-commerce. Also the legal instrument brought out by EU is discussed at the end of the study.

World Intellectual Property Organisation (WIPO)

WIPO concentrates its attention on the implications of Copyright, Trademark and Patent protection safeguard in the realm of e-commerce. WIPO's main task in the area of e-commerce is to resolve the issue of domain name disputes. Domain name disputes have been caused primarily due to the wrong registration procedures followed by the Registration Agencies. In order to curtail this, WIPO brought out a Report on Internet Domain Name Process in April 30, 1999. WIPO, to fulfil its report set up an Arbitration and Mediation center to resolve the disputes arising out of E-commerce, which is an on-line disputes resolution system.

WIPO's initiatives in this area are spelt out in the WIPO Digital Agenda¹, which consists of ten principles. Digital Agenda contains the various issues to be addressed in the digital era. More than half of the objectives directly addresses issues relating to e-commerce. WIPO aims to develop an international legislative framework to facilitate e-commerce, which includes the extension of the principles of the WIPO Performances and Phonograms Treaty (WPPT), 1996, to the audio-visual performances, adaptation of broadcasters' rights to the digital era and protection of databases. WIPO recommends for

¹ <http://www.wipo.org/ecommerce> – To view the full-text of the Digital Agenda.

the implementation of the Report of the WIPO Domain Name Process and the development of appropriate rules for determining the intellectual property liability of the online service providers. In the coming years, WIPO would study any other emerging intellectual property issues relating to electronic commerce. WIPO would also coordinate with other international organizations in the development of norms on horizontal issues affecting intellectual property, particularly the validity of electronic contracts and jurisdiction.

WIPO has updated Berne Convention by adapting two new treaties namely, WIPO Copyright Treaty (WCT), 1996, and WIPO Performances and Phonogram Treaty (WPPT), 1996. These treaties are supposed to address the IP issues of cyber space. However the treaties are yet to get sufficient ratification to come into force. Article 18 of WCT, provides for adequate legal protection against the circumvention of effective technological measures used by the authors to prevent copyright infringements. The treaty also provides for Rights Management Information (RMI) and removal of RMI to be punished by enacting appropriate national Laws². The silences of the treaty on interoperability, protection of business models, online service providers' liability etc. are causing concerns not only to the public but also e-com entrepreneurs of developing countries.

WPPT, 1996 addresses the Rights of performers and the Producers of Phonograms. The rights of performers include the Moral Rights, Economic Rights of performers in their unfixed performances, the Right reproduction distribution, rental and making available of fixed performances³. The rights of producers of phonograms include the rights of reproduction, distribution, rental and making available of phonograms⁴. WPPT also urges the contracting parties to provide adequate legal protection to technological measures and RMI⁵. It is yet to be seen how the provisions of WPPT address the, right of performances and Producers in the online media. A Diplomatic conference is convened by WIPO, which is to be held this year to discuss this issue.

² Art.12 of WCT

³ Art. 5-10 of WPPT

⁴ Ibid. Art. 11-14

⁵ Ibid. Art.18-19

WIPO Report on Domain Name Protection

The multi-jurisdictional and multifunctional nature of the Internet means that, inevitably, many different interests in many different parts of the world will be concerned with. Any endeavour to formulate specific policies, special care needs to be exercised to ensure that any policy developed for one interest or function does not impact unduly on, or interference with, other interests or function.

The WIPO's Report is divided into five chapters. The second chapter deals with the best practices to be followed by the registration authorities so that the domain name disputes may be curtailed from the very beginning. The next chapter deals with WIPO's uniform disputes resolution policy and the fourth chapter refers to famous and well-known marks.

Best Practices for Registration Authorities

The report in the beginning itself addresses the question whether the registration of domain names should take place through electronic medium or not. The report states that the contractual relationship between the Domain Name Registrant (registrant) and the Registration Authority (authority) can be achieved through an electronic agreement and where the validity of electronic records are not recognised, the registration can be reflected in a paper document.

Anonymity, one of the advantages of the Internet, is also its main drawback. Regarding the registration procedure, the WIPO report recommends that for legitimate protection and enforcement of intellectual property rights, the accurate contact details of the registrant should be the prior condition for domain name registration.⁶ The contact details should contain the full name of the applicant, his postal address,⁷ e-mail address, telephone number, facsimile number (if available) and if the applicant is an organisation, association or corporation, then the name of authorised person for administrative or legal

⁶ WIPO, *Final Report of the Internet Domain Name Process*, April 30, 1999, Para 66, available at <http://wipo2.wipo.int>.

⁷ The postal address should include street address or post office box, city, State or Province, postal code and country.

contact purposes.⁸ Moreover, the contact details of holders of domain name is all open gTLDs be made publicly available in real time. In the report, in order to take into consideration the privacy concerns, the introduction of one or multi use-restricted, non-commercial domains as a means was advocated and suggested that ICANN should start a separate process for the consultation on this question.⁹

In order to prevent unwarranted intrusion into the privacy of the domain name holder like data Mining practices, spamming etc, the report urges that the contact details collected be made available for limited purposes and these purposes should be brought to the notice of the registrant by the authority at the time of registration.¹⁰

The report does not recommend that the registration agreement contain a statement of bonafide intention to use a domain name, as WIPO considers that there can be legitimate circumstances where one may register a domain name and hold it without using it for a definite period.¹¹ The report states that the registration agreement should contain representations that the registration of the domain name does not directly or indirectly infringe the intellectual property right of another party¹² and a representation that the information provided by the domain name applicant is true and accurate. The registration agreement should contain a clause that providing inaccurate information by the domain name holder or failure to update the information, as a material breach of the registration agreement and can be the basis of cancellation of the registration by the registration authority.¹³

The procedure for cancellation of a domain name should be started by a third party. He should state that the registration infringes an intellectual property right and the registrant cannot be contacted due to inaccurate details furnished. The authority further

⁸ WIPO, n.6, para 73.

⁹ Ibid, para 86.

¹⁰ Ibid para 90.

¹¹ Ibid para 94.

¹² Ibid para 109.

¹³ Ibid para 119.

verifies this notification and if he is also unable to contact the registrant within a reasonable period, the domain name can be cancelled automatically.¹⁴

The WIPO report in its third chapter discusses the various dispute resolution methods available to a registrant. The intellectual property rights holder primarily suffers because disputes have become numerous, while the mechanism for their settlement, other than litigation, are neither satisfactory nor readily available.¹⁵ The report recommends court litigation as a means of resolving disputes; guiding principles in the design of the administrative dispute-resolution policy; mandatory administrative procedure for abusive registration; the availability of voluntary arbitration; and the role of mediation.

Court litigation

WIPO recommends to the private, non-profit corporation that manage DNS (ICANN), clarify that they are not properly concerned with matters that fall within the purview of civil laws. However, WIPO report preserves the right to litigate.¹⁶ It recommends that any dispute-resolution system alternative to litigation that might be adopted for a domain name dispute should not deprive the parties to the disputes of their right of access to court litigation.¹⁷ In the domain name registration agreement, the parties should submit to the jurisdiction of the court of the country of domicile of the domain name applicant and the country where the registrar is located.¹⁸

Guiding Principles for the Designs of the Administrative Dispute Resolution Policy

Court litigation¹⁹ may have several limitations as a means of dealing with such disputes. In particular, because of the multi-jurisdictional character of many such disputes, court action in several countries may be necessary in order to obtain an effective solution. In addition in many countries litigation can be time-consuming resulting in great loss or damage by the virtue of an infringing domain name. Moreover, the cost of

¹⁴ Ibid para 123.

¹⁵ Ibid para 130.

¹⁶ Ibid para 137.

¹⁷ Ibid para 139.

¹⁸ Ibid para 147.

¹⁹ Ibid para 148.

litigation and the cost of domain name registration will be poles apart. Since a number of courts may be involved, inconsistent decisions may result in conflicting principles concerning the relationship between domain name and IPR.

Taking into account these perceived limitations, the WIPO recommendations concerning administration procedure has been based upon the following principles.²⁰

- (1) The procedure should resolve the dispute expeditiously and at a low cost.
- (2) The procedure should ensure procedural fairness to all parties concerned.
- (3) The procedure should be uniform across all open gTLDS.
- (4) The availability of administration procedure should not preclude resort to court litigation by a party.
- (5) The determination of the procedure should not be binding precedent in national courts.
- (6) The remedies available should be restricted to the status of domain name registration itself.
- (7) Any decision in from a court in a country, which is party to the Paris convention for protection of Industrial property or under TRIPS agreement, prevails over the Administrative Determination.

Mandatory Administrative Procedure Concerning Abusive Registrations

The WIPO report states that the scope of the procedure would be limited to cases of abusive registration and would not be available for disputes between parties with competing rights action in good faith. The administrative procedure is to be adopted for all open gTLDS.²¹ The registration agreement should require the applicant to submit to the Administrative Dispute Resolution Procedure.²² The Administration Procedure is

²⁰ Ibid para 150.

²¹ Ibid para 153.

²² Ibid para 162.

limited to the abusive registration of domain names.²³ Cybersquatting is the term used in the report to describe the deliberate, bad faith abusive registration of a domain name in violation of rights in trademarks and service marks.²⁴

The definition of abusive registration be applied in the administrative procedure is as follows:²⁵

- (1) The registration of a domain name shall be considered to be abusive when all of the following conditions are met:
 - (i) The domain name is identical or misleadingly similar to a trade or service mark in which the complainant has rights; and
 - (ii) The holder of the domain name has no rights or legitimate interests in respect of the domain name; and
 - (iii) The domain name has been registered and is used in bad faith.
- (2) For the purposes of paragraph (1) (iii), the following, in particular, shall be evidence of the registration and use of a domain name in bad faith:
 - (a) an offer to sell, rent or otherwise transfer the domain name to the owner of the trade or service mark, or to a competitor of the owner of the trade or service mark, for valuable consideration; or
 - (b) an attempt to attract, for financial gain, Internet users to the domain name holder's website or other on-line location, by creating confusion with the trade or service mark of the complainant; or
 - (c) the registration of the domain name in order to prevent the owner of the trade or service mark from reflecting the mark in a corresponding domain

²³ Ibid para 169.

²⁴ Ibid para 170.

²⁵ Ibid para 171.

name, provided that a pattern of such conduct has been established on the part of the domain name holder; or

(d) the registration of the domain name in order to disrupt the business of a competitor.

According to the report the panel of decision makers shall to the extent necessary, apply the law or rules of law that it determines to be appropriate in view of all the circumstances of the case.²⁶ The remedies available under the administration procedure is limited to the cancellation of the domain name registered, the transfer of domain name registration to the third party complainant and the allocation of the responsibility.²⁷

Relationship with national courts

The report states that the parties could go to national courts to initiate litigation even after completion of administration procedure. If the administrative procedure is pending while the litigation is filed, the panel shall have the discretion to suspend or continue with the procedure. A decision of a court of competent jurisdiction, shall override the Administrative Determination.²⁸ Regarding the length of proceedings, the report held that the final determination on claims has to be completed within forty-five days of the initiation of procedure.²⁹

According to the report, provision should be made in the procedural rules for secure electronic filing of all pleadings in cases.³⁰ The report reasoned that the use of on-line facilities in the context of domain name disputes is appropriate for the following reasons.³¹

- (1) On-line facilities can eliminate barrier of distance as the parties may be from different corners of the world.

²⁶ Ibid para 177.

²⁷ Ibid para 188.

²⁸ Ibid para 196.

²⁹ Ibid para 203.

³⁰ Ibid para 214.

³¹ Ibid para 213.

- (2) It can increase the speed with which the dispute resolution can be conducted.
- (3) Many domain name disputes may be capable of being resolved by reference to documents only.
- (4) Most of the parties to the dispute are having technical facilities to participate in the on-line resolution of the dispute.
- (5) On-line filing of disputes is easier as many of the parties of the dispute may not have significant experience in legal matter on their filing procedures.

No recommendation was provided by the report for the establishment of a centralised appeal process from the determination of the administration procedure.³²

Availability of Voluntary Arbitration

The registration agreement should contain a provision for the applicant to submit of any dispute in relation to the domain name, but this should only be an optional choice.³³ Taking into consideration the fact that the parties to the disputes may be located in different part of the world, the WIPO report suggests for the establishment for an on-line arbitration procedure, which will be advantageous as a means of containing the costs of dispute resolution procedure.³⁴

Role of Mediation

While the parties are allowed to resolve the disputes based on mediation the WIPO doesn't recommend that a submission, which is either mandatory or optional, be incorporated in the domain name registration agreement.³⁵

The WIPO's report also contains a recommendation for resolving the domain name disputes in case of famous and well-known names. The WIPO reasons that because of the special attention that fame attracts, famous and well-known marks have for a long time

³² Ibid para 222.

³³ Ibid para 235.

³⁴ Ibid para 238.

³⁵ Ibid para 244.

been considered in intellectual property laws to warrant special protection, over and above that accorded to ordinary marks.

Famous and well known marks

Although there was stiff opposition to the WIPO's Interim report to give an exclusion to the famous and well known marks, prohibiting any third party to register the mark as domain name, reasoning that the owners of famous and well-known marks have had to invest large amount of human and financial efforts, WIPO in its final report stood by its decision in the interim report.

WIPO³⁶ based its decision on the international protection that is conferred on famous and well known marks by the two multilateral treaties namely the Paris convention for the protection of industrial property³⁷ (The Paris convention) and the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement.³⁸

The Report recommends for the establishment of a mechanism to identify an exclude famous and well-known marks across the difficult geographical area and across different classes of goods and services before the introduction of any new open gTLDs.³⁹ According to the report this should be carried out by ICANN through a policy adopted by

³⁶ Ibid para 252.

³⁷ Paris Convention, Article 6bis, section (1), state, "The countries of the Union undertake, ex officio if their legislation so permits, or at the request of an interested party, to refuse or to cancel the registration, and to prohibit the use, of a trademark which constitutes a reproduction, an imitation, or a translation, liable to create confusion, of a mark considered by the competent authority of the country of registration or use to be well known in that country as being already the mark of a person entitled to the benefits of this Convention and used for identical or similar goods. These provisions shall also apply when the essential part of the mark constitutes a reproduction of any such well-known mark or an imitation liable to create confusion therewith."

³⁸ TRIPS Agreement. Article 16.2 and 16.3 contain the following provisions:
"2. Article 6bis of the Paris Convention (1967) shall apply, mutatis mutandis, to services. In determining whether a trademark is well-known, Members Shall take account of the knowledge of the trademark in the relevant sector of the public, including knowledge in the Member concerned which has been obtained as a result of the promotion of the trademark."

"3. Article 6bis of the Paris convention (1967) shall apply, mutatis mutandis, to goods or services which are not similar to those in respect of which a trademark is registered, provided that use of that trademark in relation to those goods or services would indicate a connection between those goods or services and the owner of the registered trademark and provided that the interests of the owner of the registered trademark are likely to be damaged by such use."

³⁹ WIPO, n. 6, para 275.

it and should be carried on by other registration authorities under ICANN. These recommendations are not beaching on national courts in their implementations of international norms for the protection of famous marks.⁴⁰

The report recommends the following criteria for determining whether a mark its famous or not:

- (a) The component authority shall take into account any circumstances from which it may be inferred that the mark is well known.
- (b) In particular, the competent authority shall consider to, information concerning the following:
 - (1) The degree of knowledge or recognition of the mark in the relevant sector of the public;
 - (2) The duration, extent and geographical area of any use of the mark;
 - (3) The duration, extent and geographical area of any promotion of the mark, including advertising or publicity and the presentations, at fairs or exhibitions, of the goods and/or services to which the mark applies;
 - (4) The duration and geographical area of any registrations, and/or any applications for registration of the mark, to the extent that they reflect use or recognition of the mark;
 - (5) The record of successful enforcement of rights in the mark, in particular, the extent which the mark was recognized as well known by courts or other component authorities; and
 - (6) The value associated with the mark.

⁴⁰ Ibid para 277.

- (7) Evidence of the mark being the subject of attempts by non-authorised third parties to register the same or misleadingly similar names as domain names.

The report on famous and well-known marks concludes with the final recommendation urging ICANN to institute a process to address the problem of abusive registration of the names andonyms of International Non-proprietary names before the introduction of any new gTLDs.⁴¹

Arbitration and Mediation Center under WIPO

WIPO starts its International Disputes Settlement Mechanism aimed at curtailing the abuse of trademarks on the Internet after the Uniform Dispute Resolution Policy was adopted by ICANN on August 26. A panel of one or three experts, depending on the request of the parties is appointed by the WIPO Arbitration and Mediation Centre. The Arbitration panel will apply streamlined, quick and cost effective procedures to review and eliminate cases of clear abuse of trademark rights, leaving the complex cases to the courts. Cases are to be decided within 45 days.

Electronic commerce and the WTO

Since 1998, WTO members have begun to explore how the World Trade Organization should deal with the question of electronic commerce. Given the unique nature of this emerging mode of delivering products (goods and services), many questions remain to be answered. The moot question is how to regulate the international trade through Internet . Products which are bought and paid for over the Internet but are delivered physically would be subject to existing WTO rules on trade in goods. But the situation is more complicated for products that are delivered as digitalized information over the Internet, as a variety of issues arise relating to the appropriate policy regime.

The Geneva Declaration (Second Ministerial Conference 1998) on e-commerce entrusted to establish a work Programme to examine all trade-related issues relating to

⁴¹ Ibid para 303.

global electronic commerce, including those issues identified by Members.⁴² The work programme aims to “involve the relevant World Trade Organization (“WTO”) bodies, take into account the economic, financial, and development needs of developing countries, and recognize that work is also being undertaken in other international fora”.⁴³ Members also agreed to continue their current practice of not imposing customs duties on electronic transmissions. For the purposes of the work programme, the term “electronic commerce” is understood to mean the production, distribution, marketing, sale or delivery of goods and services by electronic means.⁴⁴ The work programme also includes consideration of issues relating to the development of the infrastructure for electronic commerce.

The Council for Trade in Services, Council for Trade in Goods, TRIPS Council and Committee for Trade and Development are entrusted to study the implications in their respective sectors under the supervision of the General Council.

Council for Trade in Services

The Council for Trade in Services has to examine and report on the treatment of electronic commerce in the GATS legal framework. The issues to be examined includes:⁴⁵

- (1) scope (including modes of supply) (Article I);
- (2) MFN (Article II);
- (3) transparency (Article III);
- (4) increasing participation of developing countries (Article IV);
- (5) domestic regulation, standards, and recognition (Articles VI and VII);

⁴² Declaration of Second Ministerial Conference, Geneva, 1998, available at <www.wto.org/ecommerce>.

⁴³ Ibid.

⁴⁴ Ibid.

⁴⁵ WTO General Council Annual Report, 1999, available at <www.wto.org/ecommerce>.

- (6) competition (Articles VIII and IX);
- (7) protection of privacy and public morals and the prevention of fraud (Article XIV);
- (8) market-access commitments on electronic supply of services (including commitments on basic and value added telecommunications services and on distribution services) (Article XVI);
- (9) national treatment (Article XVII);
- (10) access to and use of public telecommunications transport networks and services (Annex on Telecommunications);
- (11) customs duties;
- (12) classification issues.

Council for Trade in Goods

The Council for Trade in Goods⁴⁶ has to examine and report on aspects of electronic commerce relevant to the provisions of GATT 1994, the multilateral trade agreements covered under Annex 1A of the WTO Agreement, and the approved work programme. The issues to be studied includes market access for and access to products related to electronic commerce; valuation issues arising from the application of the Agreement on Implementation of Article VII of the GATT 1994; issues arising from the application of the Agreement on Import Licensing Procedures; customs duties and other duties and charges as defined under Article II of GATT 1994; standards in relation to electronic commerce; rules of origin issues and classification issues.

⁴⁶ Council for Trade in Goods, Work Programme on Electronic Commerce, Information provided to General Council, G/C/W/158, 26 July 1999, (99-3144).

Council for TRIPS

The Council for TRIPS⁴⁷ has to report on the intellectual property issues arising in connection with electronic commerce. The issues to be examined shall include protection and enforcement of copyright and related rights; protection and enforcement of trademarks and new technologies and access to technology.

Committee for Trade and Development

The Committee on Trade and Development was delegated to report on the development implications of electronic commerce, taking into account the economic, financial and development needs of developing countries. The issues to be examined by the committee contained⁴⁸

- (1) effects of electronic commerce on the trade and economic prospects of developing countries, notably of their small- and medium-sized enterprises (SMEs), and means of maximizing possible benefits accruing to them;
- (2) challenges to and ways of enhancing the participation of developing countries in electronic commerce, in particular as exporters of electronically delivered products: role of improved access to infrastructure and transfer of technology, and of movement of natural persons;
- (3) use of information technology in the integration of developing countries in the multilateral trading system;
- (4) implications for developing countries of the possible impact of electronic commerce on the traditional means of distribution of physical goods; financial implications of electronic commerce for developing countries.

⁴⁷ Council for TRIPS, Annual Report (1998), of the Council for TRIPS, IP/C/15, 4 December 1998, (98-4875).

⁴⁸ Report (1998) of the Council for Trade and Development, WT/ COMTD/ 15, 30 November 1998, (98-4799).

The progress achieved by Council for Trade in Services, Council for Trade in Goods, Council for TRIPS and Committee for Trade and Development are mentioned below from their reports submitted to the WTO.

Council for Trade in Service

During the deliberations in the council, Members agreed that some issues would require further substantial study before their implications could be properly understood. However there was a general view that the electronic delivery of services falls within the scope of the GATS, since the Agreement applies to all services regardless of the means by which they are delivered, and that electronic delivery can take place under any of the four modes of supply. Further, the Measures affecting the electronic delivery of services are measures affecting trade in services in the sense of Article I of the GATS and therefore are covered by GATS obligations. It was also the general view that the GATS is technologically neutral in the sense that it does not contain any provisions that distinguish between the different technological means through which a service may be supplied.⁴⁹ It was recognized that services could be supplied electronically under any of the four modes of supply. However, there was particular difficulty in making a distinction between supply under modes 1 and 2 in the case of electronic commerce, but no conclusion was reached as to how to clarify the matter, and it was agreed that further work is necessary.⁵⁰ On some other issues, however, discussions had progressed closer towards a common understanding. Issues on which a common understanding appeared to be emerging include the following:⁵¹

- (1) The electronic delivery of services falls within the scope of the GATS, since the Agreement applies to all services regardless of the means by which they are delivered, and electronic delivery can take place under any of the four modes of supply. Measures affecting the electronic delivery of services are measures affecting trade in services and would therefore be covered by GATS obligations.

⁴⁹ Council for Trade in Services Progress Report on Electronic Commerce, 1999, available at <www.wto.org/ecommerce>.

⁵⁰ Ibid.

⁵¹ Ibid.

- (2) The technological neutrality of the Agreement would also mean that electronic supply of services is permitted by specific commitments unless the schedule states otherwise.
- (3) All GATS provisions, whether relating to general obligations (e.g. MFN, transparency, domestic regulation, competition, payments and transfer, etc.) or specific commitments (Market Access, National Treatment or Additional Commitments), are applicable to the supply of services through electronic means.

The discussions have also identified a number of issues, which require considerable further examination. Those include:⁵²

- (1) The need to clarify the distinction between modes 1 and 2 in situations where a service is being delivered electronically on a cross-border basis or through consumption abroad.
- (2) The need to give consideration to the classification and scheduling of new services that are likely to arise in the context of electronic commerce.
- (3) The need to clarify the classification and improve the scheduling of Internet access and other related services, and to clarify their relationship with telecommunications commitments and the obligations in the Annex on Telecommunications.
- (4) The question whether certain products delivered electronically might be classified as goods, and therefore subject to GATT disciplines, rather than as services.
- (5) The need for further discussion of the question of likeness, particularly in relation to the MFN and national treatment principles.
- (6) The need for further work on the implications of Article VI for domestic regulations affecting electronic commerce.

⁵²

Ibid.

- (7) The need to clarify the scope of the Annex on Telecommunications in relation to access to and use of Internet access and other related services.
- (8) The applicability of the principles contained in the reference paper on basic telecommunications to electronic commerce and whether there is a need to consider the development of any additional disciplines under the GATS.
- (9) The need to study further the application of customs duties on electronic transmissions.
- (10) The question of the proper valuation of electronically transmitted products in the context of encrypted electronic payments and related issues.

TRIPS COUNCIL on E-Commerce

The task assigned to the Council for TRIPS under the Work Programme on Electronic Commerce adopted by the General Council was to "examine and report on the intellectual property issues arising in connection with electronic commerce".⁵³ It was specified that "the issues to be examined shall include: Protection and enforcement of copyright and related rights; protection and enforcement of trademarks; and new technologies and access to technology. It was pointed out by the members "the basic principles of intellectual property had survived rapid technological change and that the language used in the TRIPS Agreement was generally neutral in relation to technology."⁵⁴ In this connection, it was also suggested that, "while the growth and technological development of electronic commerce posed some challenges for the protection and use of intellectual property rights, such challenges could be addressed essentially within the established international framework for intellectual property law."⁵⁵

Regarding the copyright issues it was agreed that electronic networks could play in facilitating the collective management of rights, particular reference was made to the potential contribution they could make in respect of rights related to folklore and other

⁵³ Council for TRIPS, Work Programme on Electronic Commerce Progress Report to the General Council, IP/C/18, 30 July 1999, (99-3254).

⁵⁴ Ibid.

forms of traditional expression. Members also recognised the role of World Intellectual Property Organization in providing the legal framework.

The issues identified related to trademark are use of trademarks on the Internet, in particular in the light of the territorial nature of trademark rights and their general specificity to particular products or services, the protection of well-known trademarks, and the relationship between trademarks and Internet domain names. In connection with the latter issue, the Council was informed of the final report of the WIPO Internet Domain Name Process entitled "The Management of Internet Names and Addresses: Intellectual Property Issues."⁵⁶

On the issue of access of technology it was pointed out that the provisions of Article 7 of the TRIPS Agreement which states that the protection and enforcement of intellectual property rights should contribute to the promotion of technological innovation and to the transfer and dissemination of technology. The council identified a number of issues for the enforcement of intellectual property rights, traditionally undertaken on a territorial basis, arising out of the growing use of global electronic networks. These include the implications for questions of determining the appropriate jurisdiction and applicable law, the liability of service providers for intellectual property infringements, the role of technological measures for facilitating protection of copyright and related rights and the role of electronic rights management information.

Council For Trade in Goods

A central element of the discussions at all three meetings was the question of characterisation of electronic transmissions as services, goods or something else, as well as practical problems related to this question. The issue was brought up under several headings (i.e., customs duties, classification, customs valuation, rules of origin, and import licensing).

⁵⁵ Ibid.

⁵⁶ Published by WIPO on 30 April 1999.

There was a prevalent perception by most delegations that it was necessary to characterise electronic transmissions. The WTO provisions in the goods area (i.e., the GATT 1994 and the multilateral trade agreements covered under Annex 1A of the WTO Agreement) would be relevant for electronic transmissions where and in as far as the content of these transmissions could be qualified as goods.⁵⁷

It was also stated that the electronic transmission of data itself was a delivery service, which was covered by the General Agreement on Trade in Services (GATS). According to some delegations electronic transmissions were always to be considered services, and the disciplines developed under the GATS would apply. According to them the GATS was technology neutral and would not discriminate between different modes of delivery. Other delegations responded that this failed to take into account the dynamic and evolving nature of the Internet.

Another Question raised was whether the legal disciplines of the GATT could be applied to digitalized contents delivered through electronic means, in as far as these contents could be characterized as goods.⁵⁸ The contents of some electronic transmissions did resemble or were close substitute to goods. Examples given in this context related to music downloaded from the Internet in the form of digitalized data vs. a physical CD purchased in a shop. In the circumstances where software downloaded from the Internet was a perfect substitute for software on a disk or CD. Another closely related aspect addressed the question of whether an importation did take place when transmitting data electronically.⁵⁹ One delegation stated that, where customs duties were applied to goods in the delegation's country, a cross-border trade transaction was always involved. With electronic commerce, especially in the internet realm, it was unclear whether there was a 'thing' that actually moved across a border, which would lead to the conclusion that an "importation" in the sense of Article II of the GATT had not taken place. GATT Article II referred to customs duties applied in connection with an importation. If no

⁵⁷ Council for Trade in Goods, Work Programme on Electronic Commerce, Information provided to General Council, G/C/W/158, 26 July 1999, (99-3144).

⁵⁸ Ibid.

⁵⁹ Ibid.

importation was involved, electronic transmissions would be taken out of the realm of applying customs duties.

The work Programme is yet to reach consensus on the above-mentioned issues. The third ministerial conference failed to reach any progress in this regard. Therefore one has to look at the state practice to identify the international norms for the regulation of e-commerce.

B. Analysis of Legal Instruments Adopted by UNCITRAL and EU

UNCITRAL in June 1996 adopted a Model Law on Electronic Commerce. The main objective of the Model Law is to facilitate electronic trading by providing a set of internationally acceptable rules that can be used by states in enacting legislations to overcome legal obstacles and uncertainties, which may arise in relation to the use of electronic means of communication in international trade.⁶⁰ The model law provides guidelines for making contractual agreements and is accompanied by a “Guide to Enactment”, which aims at assisting legislators and users by providing explanations and clarifications as to the meaning and intent of the provisions of the model law.

1. UNCITRAL MODEL LAW ON E-COMMERCE⁶¹

The model law comprises of two parts. The first part covers provisions applicable to electronic commerce in general and the second deals with specific areas of electronic commerce. While the Model Law purports to be a model code relating to e-commerce, the term “electronic commerce” has not been defined in the Model Law. Instead, the term ‘Electronic Data Interchange (EDI) has been defined. Act 2(b) defines EDI as “the electronic transfer of information from computer to computer using an agreed standard to structure the information.

According to the act, the validity and enforceability of information cannot be denied simply because it is provided in the form of a “data message.”⁶² Art 5 bis⁶³ is a

⁶⁰ Electronic Commerce: Legal Considerations; UNCTAD/SDTE/BFB/1, p. 6, para 10.

⁶¹ UNCITRAL Model Law, 1996, available at
<<http://www.un.or.at/uncitral/englisht/texts/electcom/ml-ec.htm>>.

new inclusion into the model law, which aims to give legal recognition to data messages, which are not a part of the original message, but referred to in that data message. The addition is aimed at recognizing the validity of data messages like the e-mail messages, which sometimes may not contain nothing more than references to the earlier e-mail messages.

Requirements for writing

If information in a data message is accessible so as to be usable for subsequent reference, such a data message shall be valid for the purpose of law.⁶⁴ The term “accessible” implies that “information in the form of computer data should be readable and interpretable, and that the software that might be necessary to render such information readable should be retained.”⁶⁵ The word “usable” is not intended to cover not only human use but also computer processing.⁶⁶

Validity of Electronic Signature

The model law establishes the general conditions under which data messages should be regarded as having been authenticated with sufficient credibility, as to be enforceable in the context of signature requirements of existing laws. It allows a broad definition by stating that ‘any law which states that the signature of any person is necessary shall be deemed to have been satisfied, so long as a method is used to identify that person and to indicate his approval of the message.’⁶⁷ The model law thus provides a technology-neutral suggestion.

Originality

The model law lays down the minimum acceptable requirements that need to be met by a data message, before it can be considered to be the functional equivalent of an

⁶² Art 5, UNCITRAL Model Law, 1996.

⁶³ Adopted by the Commission at its thirty- first session, in June 1998.

⁶⁴ Art 6, UNCITRAL Model Law, 1996.

⁶⁵ Supra note 60, p. 34, para 97.

⁶⁶ Guide to Enactment of the Model Law, para 50.

⁶⁷ Art 7 UNCITRAL Model Law, 1996.

original.⁶⁸ It sets down the criteria for assessing the integrity and reliability of a data message. The necessary additions to a data message, such as an endorsement and notarisation, do not affect the originality of the data message, as long as the information in the message remains unaltered.⁶⁹ The model law permits enacting states to exclude certain situations from its application.⁷⁰

Evidential value of Data Messages

The model law specifies the circumstances under which data messages would be admissible as evidence⁷¹. It clearly states that data messages should not be denied admissibility on the sole ground that they are in electronic form.⁷² It also suggests that due evidential weight must be given to information presented in the form of a data message. The criteria for assessing the evidential weight shall take into consideration:⁷³

- (1) the reliability of the manner in which the data message was generated, stored or communicated.
- (2) the manner in which the integrity of the information was maintained.
- (3) the manner in which its originator was identified, as well as any other relevant factors, that might arise.

Formation and validity of contracts

Chapter III of the model law address the law relating to the formation of contracts concluded electronically.⁷⁴ It establishes that contracts created by the exchange of data messages, i.e. offer and acceptance of offer, being in the form of data messages, are

⁶⁸ Art 8, Ibid.
⁶⁹ Art 8(3) (a), Ibid.
⁷⁰ Art 8(4), Ibid.
⁷¹ Art 9, Ibid.
⁷² Art 9(1) (a), Ibid.
⁷³ Art 9(2), Ibid.
⁷⁴ Art 11, Ibid.

enforceable and cannot be denied validity or enforceability on the sole ground that data messages were used for that purpose.⁷⁵

The Model Law does not impose any rigid conditions for parties entering into contracts. The use of the clause “unless otherwise agreed by the parties”⁷⁶ clearly recognizes the parties freedom of contract.

Attribution of data messages

So long as the originator of the message, agreed to authenticate a message using given authentication method, the message shall be deemed to have been sent by the originator, if the receiver can verify that it has been sent by using that authentication method.⁷⁷ Accordingly, the addressee would be entitled to act on the assumption that the data message was sent by the origination or even if it is sent by a person who had the authority to act on the behalf of the originator⁷⁸ or a message from an automated information system, programmed on behalf of the originator⁷⁹, relying on the authentication method agreed upon.

Time, place of dispatch and the receipt of data messages

The time of dispatch of data messages occurs when it enters any information system outside the control of the originator or of the person who on behalf of the originator sends the message.⁸⁰ The time of receipt of the data message depends upon two things namely whether the addressee has a designated information system or not. If he has a designated information system, then the time of receipt is the time at which it enters that system.⁸¹ The time of receipt is the time at which the data message is retrieved by the addressee, if he does not have a designated system.⁸²

⁷⁵ Art 11 (1) , Ibid.
⁷⁶ Art 11 (1), Ibid.
⁷⁷ Art 13 (3), Ibid.
⁷⁸ 13 (2) (a), Ibid.
⁷⁹ Art 13(2)(b), Ibid.
⁸⁰ Art 15(1) , Ibid.
⁸¹ Art 15 (2)(i) , Ibid.
⁸² Art 15 (2) (ii) , Ibid.

According to the Model Law, the place of dispatch of the data message is the place of business of the originator and it is received at the place of business of addressee.⁸³ If they have more than one place of business, then it is that place which has the closest relationship to the underlying transaction, or where there is no underlying transaction, then it is the principal place of business.⁸⁴ If the originator or addressee doesn't have a principal place of business, then the habitual residence is to be considered the place of business.⁸⁵

Conclusion

The UNCITRAL Model law provides only a basic framework upon which domestic laws relating to e-commerce may be based upon. Various countries have enacted laws relating to e-commerce based on the principles set out in the model law. The Malaysian Computer Crimes Act, 1998 and the Information Technology Act, 2000 were modelled upon the principles laid down by the Model Law.

EUROPEAN ELECTRONIC COMMERCE DIRECTIVE

The primary objective of the directive is to ensure that following the coming into force of the European Electronic Commerce Directive, the Information society services will be able to benefit fully from the free movement of services between members.

Chapter II is divided into five sections. Section I enumerates the various principles adopted. Art 4 is on the principle of exclusion of prior authorisation. The purpose of this article is to give effect to the principle of freedom to provide services by facilitating access to the supply of services on the Internet. It thus establishes a sort of 'right to a site' which can be exercised by any operator, company or self-employed person deciding to use the Internet to provide a service. Art 5 refers to the informations, which has to be provided by the service provider. Art 5 (2) stipulates that this information collected is vital for protecting the consumer and other recipients of the service and for ensuring fair trading.

⁸³ Art 15 (4) , Ibid.

⁸⁴ Art 15 (4) (a) , Ibid.

⁸⁵ Art 15 (4) (b) , Ibid.

Section II of chapter II deals with commercial communications. Article 7 deals with ‘spamming’ practices to consumers or discussion groups, and requires that unsolicited communications must have a specific message on the envelope so that the recipients can instantly identify it as a commercial communication without having to open it.

Art 8 deals with regulated professions. This provision sets out the general principle that commercial communication is permitted for regulated professions to the extent necessary for these professions to be able to provide an information society service, provided it meets the professional rules of conduct applicable to them. It also provides that if necessary, the European Commission might take action to define what types of information are compatible with the ethical rules of conduct in association with the member states in the context of a committee set up under Art 23.

The treatment of electronic contracts is dealt with in Art 9. The article provides for states to carry out a systematic review of those rules which might prevent, limit or deter the use of electronic contracts and to carry out this review in a qualitative way i.e. not to simply amend the key words in the rules but to identify everything which might in practice prevent the “effective” use of electronic contracts. The scope of analysis to be carried out by the member states should include various stages of contractual process like the invitation to treat, offer, negotiations, the conclusion of the contract, registration, cancellation or amendment of the contract, invoicing, archiving of the contract.

There is an emphasis of fair-trading in the EU directive. Art 10 states that in order ensure a high standard of fair trading and consumer protection, there should be transparency regarding various stages of contractual formation, in particular the need to describe in advance what different steps are necessary before the formal conclusion of a contract. Para 3 aims to allow the recipient of the service to have access to relevant codes of conduct concerning contractual aspects that the service provider is subject to. Art 11 seeks to determine clearly the time at which a contract is concluded.

Section IV, deals with the liability of intermediaries and exemption from liability. Art 12 establishes an exemption from liability as regards acts of transmission of

information in communication networks where the service provider play a passive role as a conduit of information for third parties.

The liability exemption covers both the vicarious liability and contributory liability. However this article does not exclude, the possibility of an action for injunctive relief. Conditions to be fulfilled for this are that the On-line Service Provider should not initiate the transmission and should not select nor modify any information contained in the transmission. Art 13 addresses the temporary forms of storage of messages most often referred to as 'caching'. The service provider should not be held liable if he does not modify the information, does not interfere with the technology, consistent with the industrial standard.

Art 14 establishes a limit on liability as regards the activity of storage of information provided by the recipients of service and at their request. The exemption of liability cannot be granted if a service provider knows that a user of his service is undertaking illegal activity (actual knowledge). Art 15 establishes that no general obligations should be imposed on providers to screen or to actively monitor third party content in order to prevent or fight specific illegal activity.

Chapter III of the directive deals with its implementation. Art 17 establishes an obligation to allow recourse of other remedies like out-of-court dispute settlement or on-line dispute resolution mechanism. Art 19 provides for cooperation between member states and the commission. Art 23 provides for setting up a consultative committee charged with assisting the commission in implementing its powers of enforcement.

National Laws Regulating E-commerce

Till date there has not been any consensus upon the laws pertaining to electronic commerce at the International level. Twelve countries, including India have enacted laws to regulate electronic transactions so far. The other countries are USA, UK, Japan, Germany, Ghana, Singapore, Malaysia, Canada, France, China and Brazil. The Information Technology Act, 2000, the law that regulates e-commerce transactions is

based on UNCITRAL Model Law and Singapore Electronic Transaction Act, 1998. This section makes a study of the Singapore Act.

SINGAPORE ELECTRONIC TRANSACTIONS ACT, 1998:⁸⁶

The Singapore act is modelled on the UNCITRAL Model Law, the Illinois Electronic Commerce Security Act and Utah Digital Signature Act. It is brought to facilitate electronic communications,⁸⁷ electronic commerce⁸⁸, electronic filing of documents with government agencies and statutory corporations⁸⁹ and to minimise forged electronic records and fraud in e-commerce.⁹⁰

The Act is divided into twelve parts, describing the legal positions as to formation of Contracts, Secure Electronics Records, Digital Signatures, Certification Authorities, Liability of the Network Service Providers and Government use of Electronic Records and Signatures and a General section addressing the issues of confidentiality, power to investigate, General penalties, offences and amendments to other acts.

Electronic Signature

The Act defines an Electronic Signature as any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record and executed or adopted with the intention of authenticating or approving the electronic record.⁹¹ It provides that electronic signature is not applicable in the creation or execution of a will, negotiable instruments, disposition of immovable property, the creation of power of attorney and documents of title, where the law requires writing or signature as essential.⁹² It is explicitly mentioned in the act, that for all purpose other than those mentioned in section 4, the information shall not be denied legal validity solely on the

⁸⁶ Reproduced from <http://www.cc.gov.sg/>

⁸⁷ Section 3 (a) Singapore was the first country to enact UNICITRAL Model Law or Electronic Commerce as a part of national law. Singleton and Halbestam, *Business, The Internet and The Law*, (Great Britain,1999), p 152.

⁸⁸ Section 3 (b), Singapore Electronic Transaction Act, 1998.

⁸⁹ Section 3(c) , Ibid.

⁹⁰ Section 3(d) , Ibid.

⁹¹ Section 2 , Ibid.

⁹² Section 4, Ibid.

ground that it is in the form of an electronic record.⁹³ This has been given further emphasis in section 8(1), which states that an electronic record satisfies a rule of law, if that rule of law requires a signature or provides for certain consequences if document is not signed. It is further referred in the act that contracts formed by exchange of electronic records, constituting offer and acceptance of offer, shall be given legal effect.⁹⁴

The Act defines a secure electronic record as one which is unique to a person using it and is capable of being identified with such a person, which is created in such a manner or using the means under the sole control of the person using it and it is linked to the electronic record in such a manner that if the record is changed, the electronic signature should be invalidated.⁹⁵

When an electronic record is signed by a digital signature, which is created during the operational period of a valid certificate, encrypted by the public key listed in the certificate; the validity of the certificate being issued by the licensed certification authority or issued by a certification authority outside Singapore, the digital signature can be treated as a secure electronic signature as specified by the act.⁹⁶

Time and place of dispatch and receipt

According to the Act, the dispatch of an electronic record occurs when it enters an information system outside the control of the originator.⁹⁷ The time of receipt is the time when the electronic record is retrieved by the addressee.⁹⁸

The place of dispatch of electronic record is the place of business of the originator. The place of receipt is the place where the addressee has his/her place of business.⁹⁹ If the originator or addressee has more than one place of business, then the place, which has the closest relationship to the underlying transaction, would be considered the place of business. And if there is no such underlying transaction, then the

⁹³ Section 6, Ibid.

⁹⁴ Section 11 (1), Ibid.

⁹⁵ Section 17, Ibid.

⁹⁶ Section 13, Ibid.

⁹⁷ Section 15 (1), Ibid.

⁹⁸ Section 15 (2) (a) (ii), Ibid.

place will be the principle place of business, if the originator or addressee does not have a place of business, then reference is made to the usual place of residence.¹⁰⁰

Certification Authority

A certification authority may issue a certificate upon the request from a prospective subscriber and on the production of certification practice statement.¹⁰¹ In the absence of a certification practice statement, the certification authority shall issue the certificate only after it confirms the identity of the subscriber. If he is acting through any agent, then the certification authority should verify that the agent has the custody of the subscriber's private key and the corresponding public key. The accuracy of the information in the certificate to be issued and the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the prospective subscriber.¹⁰²

The certification authority shall revoke a certificate it has issued, on the request of the subscriber, or on receiving a certified copy of the presentation of documents effecting a dissolution of the subscriber or if the subscriber has ceased to exist.¹⁰³ The authority shall revoke the certificate without subscriber's consent, if any material fact represented in the certificate is false, or any requirement for the issuance of the certificate was not met with or the certification authority's private key or trustworthy system was compromised in a manner materially affecting the certificates reliability.¹⁰⁴ The certification authorities shall be regulated by the controller of certification authorities, who licenses, certifies, monitors and oversees the activities of the certification authorities.¹⁰⁵ The controller shall have powers to:

- (1) authorise any officer to exercise any of the powers of the controller

⁹⁹ Section 15 (4), Ibid.
¹⁰⁰ Section 15 (5), Ibid.
¹⁰¹ Section 29 (4), Ibid.
¹⁰² Section 29 (2), Ibid.
¹⁰³ Section 32, Ibid.
¹⁰⁴ Section 13, Ibid.
¹⁰⁵ Section 41 (1), Ibid.

- (2) prevent by a written notice, any activity of the certification authority or employee to take such measures that are specified in the notice, if they are necessary to ensure compliance with the provisions of the act.
- (3) investigate by himself or through any officer appointed by him.
- (4) Access the computers and data, if there is any reasonable suspicion of any offences mentioned in the act.
- (5) Compound any offences under the act, by collecting an amount not exceeding \$5,000 from a person reasonably suspected to have committed the offence.

Offences

The Act also lists the possible offences like publishing fraudulent certificates, impersonation obstructing the duties of the certification authorities or controller of certification authorities, breach of confidentiality of public and private keys etc and lays down the punishments for those contraventions of the Act. The offences and punishments are as follows:

- 1) Any person who publishes a certificate for fraudulent or unlawful purpose shall be punished by an imprisonment for a term not exceeding 2 years or a fine not exceeding \$ 20,000 or both.¹⁰⁶
- 2) Any person who knowingly misrepresents to the certification authority for requisition, suspension or revocation of a certificate shall be punishable with a fine not exceeding \$ 10,000 or imprisonment not exceeding 6 months or both.¹⁰⁷
- 3) Any person violating the provisions of Section 42 (2), which defines the functions, procedures etc of certification authorities shall be punished with a fine not exceeding \$ 50, 000 or imprisonment for 12 months or both.¹⁰⁸

¹⁰⁶ Section 25, Ibid.

¹⁰⁷ Section 26, Ibid.

¹⁰⁸ Section 42 (3), Ibid.

- 4) Any person violating the obligation of confidentiality mentioned under 48(b) shall be punished by a fine exceeding \$10,000 or imprisonment for a term not exceeding 12 months or both.¹⁰⁹
- 5) Any person who obstructs the lawful exercise of the powers of the controller mentioned under Sec 53 shall be liable for a fine not exceeding \$ 20,000 or imprisonment of a term not exceeding 12 months or both.¹¹⁰

Summary

The contributions from the part of WIPO, WTO and UNCITRAL have settled few issues that came to the fora with the advent of e-commerce. The WIPO arbitration and mediation mechanism has been highly successful in dealing with the cybersquatting. The Internet commerce in the coming years is to expand many folds than we experience today. The WTO, which consists of 132 nations, would be the right forum to deal with the issues of electronic commerce. The participation of developing countries in electronic commerce is negligible when compared with US, UK or countries in European Union. The WTO should take a detailed study before deciding further moratorium on taxing, as it will be having deep implications on the economic sector in developing countries.

¹⁰⁹ Section 48 (2), Ibid.

¹¹⁰ Section 53 (2) , Ibid.

The Indian Response To Regulating E-Commerce

Recognizing the necessity for a comprehensive law to govern various aspects of electronic commerce transactions, both the houses of the Parliament of India passed the Information Technology Act on 16 May 2000. The Act was passed in furtherance of the United Nations General Assembly Resolution urging the member states to enact/or revise their laws in order to create a uniform legal environment for regulating alternatives to paper based methods of communication usually referred to as the electronic commerce, taking into consideration; the UNCITRAL model law on electronic commerce, 1996. The Act not only transforms the model law into domestic legislation but also brings in a procedural infrastructure seeking to regulate the e-market place with a global perspective.

Objective and Purpose

The Act aims at providing legal recognition to alternatives to paper based method transactions, so that the advantages showered by the advent of digital technology like the cost effectiveness, less storage space, speed of data transmission etc can be utilized both by the common man and the business sector. It aims to create an environment in which the laws are transparent and the advantages of the new technology can be utilized. The Act provides legal recognition to all electronic transactions coming under the gamut of electronic commerce.

The purpose of the Act is to facilitate electronic commerce transactions by providing legal recognition to electronic records and digital signatures, to provide a regulatory regime to supervise the functioning of the Certifying Authorities and to prevent the misuse of the electronic medium for furthering criminal activities. The Act legalizes the electronic filing of documents and maintenance of electronic records taking into consideration, the global developments, the Act also aims to facilitating electronic governance by the use and acceptance of electronic records and digital signatures in government offices and its agencies, thus making the “ interaction with the governmental offices hassle free.”¹

The Act is divided into thirteen chapters or parts, namely Digital Signatures², Electronic Governance³, the Attribution of Electronic Records⁴, Secure Electronic

¹ Information Technology Act, 2000, Preamble, Para 4,

² Ibid. Chapter II

Records⁵, Regulation of Certifying Authorities⁶, Digital Signature Certificates⁷, Duties of the Subscriber⁸, Penalties and Adjudication⁹, Cyber Regulation Appellate Tribunal¹⁰, Offences¹¹, Network Service Provides Liability¹², and Miscellaneous¹³. The Act not only lays down new substantive law but also makes incidental and consequential amendments to the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Bankers Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934.¹⁴

Applicability of the Act

The Act applies to the whole of India and also applies to any offence or contravention conceived outside India by any person¹⁵ i.e. the Act is also extra-terrestrial in application. The Act exempts from its purview the following areas namely negotiable instruments, power of attorney, trusts, will or other testamentary dispositions, any contract for the sale or conveyance of immovable property or any interest in such property and any such class of documents or transactions as may be notified by the central government.¹⁶

Further, in case of offences, the Act applies to any offences or contravention outside India by any person irrespective of his nationality, if the act constituting the offence or contravention involves a computer, computer system or computer network located in India.¹⁷

Moreover according to the Act, the provisions of the Act have an overriding effect over any existing principles of law that are inconsistent to them.¹⁸

3 Ibid. Chapter III
4 Ibid. Chapter IV
5 Ibid. Chapter V
6 Ibid. Chapter VI
7 Ibid. Chapter VII
8 Ibid. Chapter VIII
9 Ibid. Chapter IX
10 Ibid. Chapter X
11 Ibid. Chapter XI
12 Ibid. Chapter XII
13 Ibid. Chapter XIII
14 Ibid. Chapter XIII, Sections 91-94
15 Ibid. Section 1(2)
16 Ibid. Section 1(4)
17 Ibid. Section 75.
18 Ibid. Section 81.

Digital Signature

The Act defines Digital Signature as an electronic signature¹⁹, consisting of a transformation of an electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signers public key, can accurately determine,

- (1) Whether transformation was created using the private key that corresponds to the signers public key; and
- (2) Whether initial electronic record has been altered since the transformation was made.

The Act states that when the law requires any matter to be authenticated by affixing the signature or any document should be signed, that requirement is met, if the document has been authenticated by means of a Digital Signature in a manner prescribed by the government.²⁰ The Act also provides legal recognition of any information or matter available in electronic form, if used in place of written, typewritten or printed form, the only condition being the information is to be made available in electronic form and it should be usable for a subsequent reference.²¹

The legal recognition of digital signatures and electronic records envisages the “functional-equivalent”²² approach of the Act. The Act does not attempt to define a computer-based equivalent to any kind of paper document. Instead it singles out basic functions of paper based form requirement, with a view to providing criteria which, once they are met by data messages, enable such data messages to enjoy the same level of recognition as their corresponding paper document, performing the same function.

The Act validates the use of Electronic Records and Digital Signatures in Government and its agencies²³ for the filing of any form²⁴, application or for the issue

¹⁹ Ibid. Section 3.

²⁰ Ibid. Section 5.

²¹ Ibid. Section 4.

²² Electronic commerce: legal consideration; UNCTAD/SDTE/BFB/1.

²³ Section 6, Information Technology Act, 2000.

²⁴ Ibid. Section 6(a).

grant of any license²⁵, receipt or payment of money etc²⁶. It states that the Central Government may prescribe the rules regarding the type of Digital Signature, the manner and format in which the Digital Signature shall be affixed, the manner or procedure which facilitates identification of the person affixing the Digital Signature and the procedures to ensure adequate integrity, security, and confidentiality of the electronic records or payments.²⁷

Secure Electronic Record and Secure Digital Signatures

For facilitating the various functions under the Act, the central government shall, taking into consideration the commercial circumstances prevailing at the time, prescribe the security procedure²⁸ for any transactions coming under the connotation of electronic commerce or electronic governance. When the said security procedure is applied to an electronic record, it can be further considered as a secure electronic record.²⁹

According to the Act, for a Digital Signature to be considered as a Secure Digital Signature³⁰, it is essential that the security procedure should be unique to the subscriber affixing it³¹, is capable of identifying such subscriber³² and created in a manner under the exclusive control of the subscriber and is linked to the electronic record in such a manner that if the electronic record was altered, the Digital Signature would be invalidated.³³

Digital Signature Certificate

As per the terms of the Act, a certification Authority may issue a Digital Signature Certificate to a prospective subscriber if it has received a request for issuance together with prescribed fee³⁴ and certification practice statement.³⁵ The

²⁵ Ibid. Section 6(b).

²⁶ Ibid. Section 6(c).

²⁷ Ibid. Section 10.

²⁸ Ibid. Section 16.

²⁹ Ibid. Section 14.

³⁰ Ibid. Section 15.

³¹ Ibid. Section 15(a).

³² Ibid. Section 15(b).

³³ Ibid. Section 15(c).

³⁴ Ibid. Section 35(2).

³⁵ Ibid. Section 35(3).

Certifying Authority shall grant the certificate if it is satisfied that the applicant³⁶ holds the private key which is capable of creating a digital signature, corresponding to the public key to be listed in the Digital Signature affixed by the private key held by the applicant. The Act provides for suspension of Digital Signature Certificate upon request of the subscriber³⁷ or any person authorised by him³⁸ or on the basis of public interest.³⁹

Certifying Authority can revoke the certificate upon the death of the subscriber or upon the dissolution or winding up of the company⁴⁰ where the subscriber is a firm or a company. It can also revoke the certificate, if it is of the opinion that some material facts mentioned in the certificate were false or has been concealed or the private key of security system was compromised or any other requirement was compromised or any other requirement was not satisfied.⁴¹

Electronic Governance

The Act paves the way for electronic governance in the country. The functional equivalent approach that has been extended to electronic form and Digital Signature has been extended to all functions of the government and its agencies.⁴²

Where it has been provided by law that any document, record or information is to be retained, then that requirement shall be deemed to be satisfied if they are retained in the electronic form, subject to the requirement that the information remains accessible so as to be usable for a subsequent reference, that the electronic record is retained in the format originally generated, sent or received or in a format which can accurately represent this information and which will facilitate the identification of the origin, destination, date and time of despatch or receipt of such electronic record are available in the electronic record.⁴³

The Act further facilitates e-governance by stating that the requirement of publication in the Official Gazette will be satisfied, if the information is published in

³⁶ Ibid. Section 35(4).

³⁷ Ibid. Section 37 (a) (i).

³⁸ Ibid. Section 37(a) (ii).

³⁹ Ibid. Section 37 (b).

⁴⁰ Ibid. Section 38 (1).

⁴¹ Ibid. Section 38 (2).

⁴² Ibid. Section 6.

Electronic Gazette⁴⁴. But the Act provides safety valve for the government by stating that no right is conferred upon any person to insist that the Government should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in electronic form.⁴⁵

Attribution, Acknowledgement and Dispatch of Electronic Records

An electronic record, according to the Act, is attributed to the originator if it was sent by him or by any person who had the authority to act on behalf of the originator or by an information system programmed by or on behalf of the originator to operate automatically.⁴⁶ The acknowledgement if not agreed between the originator and the addressee, then can be in any form of communication.⁴⁷ But if the originator prescribes a form of acknowledgement,⁴⁸ the electronic record shall be binding on him only after the receipt of such acknowledgement. The time and place of despatch and receipt of electronic record are the same as those prescribed by the Singapore Electronic Transaction Act, 1998.⁴⁹

Certifying Authority

The Act empowers the Central Government to appoint a Controller of Certifying Authorities and a number of Deputy Controllers and Assistant Controllers as it deems fit.⁵⁰ The functions of the controller includes among many specified, the supervision over the activities of the Certifying Authorities, resolving conflict of interest involving Certifying Authority and its subscribers, specifying the form and content of Digital Certificates,⁵¹ the Controller shall be acting as the repository of all Digital Signature Certificates⁵² and maintain a computerised database of all public keys and make available both to any members of the public.⁵³

⁴³ Ibid. Section 7

⁴⁴ Ibid. Section 8.

⁴⁵ Ibid. Section 9.

⁴⁶ Ibid. Section 11.

⁴⁷ Ibid. Section 12.

⁴⁸ Ibid. Section 12(2).

⁴⁹ Mentioned in the chapter 3.

⁵⁰ Ibid. Section 17, Information Technology Act, 2000.

⁵¹ Ibid. Section 18.

⁵² Ibid. Section 20(1).

⁵³ Ibid. Section 20(3).

A Foreign Certifying Authority can be recognised by the controller upon the previous approval from the central government and by notifying in the Official Gazette, thus making the Digital Certificates issued by them, valid for the all the purposes mentioned in the Act.⁵⁴ The Controller can revoke this approval, if the said Authority has contravened any of the conditions and restrictions subjected to which the recognition was granted.⁵⁵

For Digital Signature Certificate, the applicant has to apply to the Controller of Certifying Authorities. Every application should be accompanied by a practice statement,⁵⁶ a self-identification statement, prescribed fees and other documents as may be prescribed by central government.⁵⁷

The licence shall be issued only after the applicant fulfils the requirement with respect to qualification, experience, manpower, financial resources and other infrastructural facilities.⁵⁸ The license once granted shall be valid for a prescribed period, non-transferable or heritable and subject those conditions specified at the time of granting the certificate.⁵⁹

The Controller may revoke the licence issued by the Certifying Authority, if it has made any statement incorrect or false for the issue or renewal of licence or failed to comply with the terms and to observe those standards prescribed by the central government or contravened any provisions of the Act, rule or regulation made under it.⁶⁰

Duties of the Subscriber

Upon receiving the Digital Signature Certificate, the subscriber shall generate the key pair by applying the security procedure.⁶¹ The Act provides that by accepting the Digital Signature Certificate, the subscriber shall have a duty to exercise reasonable care to retain the control of the private key, corresponding to the public key listed in the certificate and not to disclose to any person not authorised to affix the

⁵⁴ Ibid. Section 19(1).

⁵⁵ Ibid. Section 19(3).

⁵⁶ Ibid. Section 21(1).

⁵⁷ Ibid. Section 22.

⁵⁸ Ibid. Section 21(2).

⁵⁹ Ibid. Section 21(3).

⁶⁰ Ibid. Section 25.

Digital Signature of the subscriber.⁶² He has primary duty to communicate to the Certifying Authority, if the private key has been compromised and shall be liable till the information reaches the Certifying Authority.⁶³

When a subscriber accepts a Digital Signature Certificate, the presumption by all who corresponding private key to the public key listed in the certificate and all the representations made by him to certifying authority and those mentioned in the certificate are true.⁶⁴

Penalties

The Act divides the provisions into two separate categories namely contraventions and information technology offences. While the former may result in only monetary penalties, the latter may result in imprisonment or fine or both. The following acts if done without permission of the owner are contravention⁶⁵

- (1) Accessing or securing access to computer/network.
- (2) Downloading any data or information.
- (3) Introducing any computer contaminant or virus.
- (4) Damaging or causing to be damaged the computer/network, data, computer database or any programmes in it.
- (5) Disrupting or causing the disruption of computer/network.
- (6) Causing denial of access to any person authorised to access the computer/network.
- (7) Providing assistance to any person to facilitate access to any compute/network in contravention of the provision of the Act.
- (8) Charging the services availed by a person to the account of another person by tampering with or manipulating any computer/network.

⁶¹ Ibid. Section 40.

⁶² Ibid. Section 42(1).

⁶³ Ibid. Section 42(2).

⁶⁴ Ibid. Section 41(2).

Any person contravening any of these shall be liable to pay damages⁶⁶ not exceeding one crore rupees to the person so affected. The Act also provides penalties for failure to furnish information, returns etc.⁶⁷ The quantum of compensation is decided by the adjudicating officer taking into consideration the amount of unfair advantage gained, the amount of losses caused and the repetitive nature of the default.⁶⁸ The adjudicating officer can compound the contravention upon the payment of the amount prescribed.⁶⁹ But compounding is inapplicable to a person who has committed same or similar contravention within a period of three years and was compounded for the first offence.⁷⁰ According to the Act, penalties mentioned in the Act does not interfere with other punishments i.e. even when a penalty is imposed for any contravention, still the offender can be punished for other crimes which he will be liable under any other law.⁷¹

The Act creates a new breed of offences, the prevention of which is necessary for the smooth running of transactions carried out through the electronic media' and prescribes punishments in terms of imprisonment or both. The Act in detail, identifies situation, which amounts to computer crimes. The offences identified are tampering with a computer source code,⁷² hacking with computer system,⁷³ publishing of information, which is obscene in electronic form,⁷⁴ failure to comply with Controller's directions,⁷⁵ failure of the subscriber to comply with controller's offences order to extend facilities to decrypt information,⁷⁶ accessing a designated protected system,⁷⁷ misrepresentation before the Controller of Certifying Authority (CCA),⁷⁸

⁶⁵ Ibid. Section 43.
⁶⁶ Ibid.
⁶⁷ Ibid. Section 44.
⁶⁸ Ibid. Section 47.
⁶⁹ Ibid. Section 63.
⁷⁰ Ibid. Section 63(2).
⁷¹ Ibid. Section 77.
⁷² Ibid. Section 65.
⁷³ Ibid. Section 66.
⁷⁴ Ibid. Section 67.
⁷⁵ Ibid. Section 68.
⁷⁶ Ibid. Section 69.
⁷⁷ Ibid. Section 70(3)
⁷⁸ Ibid. Section 71.

breach of confidentiality and privacy,⁷⁹ publishing false Digital Signature Certificate⁸⁰ and making available Digital Signature for fraudulent purposes.⁸¹

According to the Act any computer, computer systems, floppies, compact disks, tape drives or any other accessories related in respect to which a contravention of the Act has occurred, shall be liable to confiscation.⁸²

The Act further supplements the punishment to the offences but stating that no penalty imposed or confiscation made under the Act, does not prevent the further imposition of any other law for the time being in force.⁸³

The Cyber Regulation Appellate Tribunal

The Central Government shall by notification establish one or more appellate tribunal known as Cyber Regulation Appellate Tribunal (CRAT),⁸⁴ consisting of a single member known as Presiding Officer,⁸⁵ who will hear and dispose appeals from the orders of the Controller of Certifying Authorities and the Adjudicating Officers.⁸⁶ In its proceedings, CRAT is free to determine its own procedure but shall be guided by principles of natural justice.⁸⁷ CRAT will also have all powers of a civil court as prescribed by the Code of Civil Procedure, 1908 such as summoning witnesses requiring the production of documents or electronic records, receiving evidence on affidavits, issuing commission, reviewing its decision etc.⁸⁸

When any matter is pending before CRAT, no civil court will have jurisdiction over such a matter and no injunction shall be granted by any court in respect of any Action taken or to be taken by CRAT.⁸⁹ Any person aggrieved of any decision or

⁷⁹ Ibid. Section 72.
⁸⁰ Ibid. Section 73.
⁸¹ Ibid. Section 74.
⁸² Ibid. Section 76.
⁸³ Ibid. Section 77.
⁸⁴ Ibid. Section 48.
⁸⁵ Ibid. Section 49.
⁸⁶ Ibid. Section 57(1).
⁸⁷ Ibid. Section 58(1).
⁸⁸ Ibid. Section 58(2).
⁸⁹ Ibid. Section 61.

order of CRAT can file an appeal to the High Court.⁹⁰ CRAT has the power to compound contraventions.⁹¹

Investigation Under the Act

The Act specifies that any offence under the Act shall be investigated by a police officer not below the rank of Deputy Superintendent of Police⁹² (DSP). It empowers a police officer not below the rank of DSP or any other officer of the central government or a state government authorised by the Central Government to enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act.⁹³ For entry, search or arrest, the provisions of the Code of Criminal Procedure 1973 (2 of 1974) shall apply.⁹⁴

The Cyber Regulations Advisory Committee

As soon as the Act is put into affect, the government shall take steps to constitute a Cyber Regulation Advisory Committee (CRAC).⁹⁵ The CRAC will advise the central government generally or for any purpose connected with the Act⁹⁶ and also CCA in framing the regulations under the Act.⁹⁷

Liability of Network Service Provider

The Act establishes that the network service provider will not be liable for providing any third party information or data made available by him, if the offence was committed without his knowledge or that he had exercised due diligence to prevent the commission of such offence or contravention.⁹⁸

To facilitate alternatives to paper based communications, the Act made consequential amendments in some of the existing statutes namely the Indian Penal

⁹⁰ Ibid. Section 62.

⁹¹ Ibid. Section 63.

⁹² Ibid. Section 78.

⁹³ Ibid. Section 80.

⁹⁴ Ibid. Section 80(3).

⁹⁵ Ibid. Section 88.

⁹⁶ Ibid. Section 88(3)(a).

⁹⁷ Ibid. Section 88(3)(b).

⁹⁸ Ibid. Section 79.

Code, 1860,⁹⁹ the Indian Evidence Act, 1872,¹⁰⁰ Bankers Book Evidence Act, 1891¹⁰¹ and the Reserved Bank of India Act, 1934.¹⁰²

A Review of the IT Act, 2000

India has still a long way to travel for implementing a successful e-commerce legal regime. The passing of IT Act can be seen only as one of the means and not the end. Still there are a lot of grey areas left unanswered by the Act and the policy makers.

One of the primary concerns of any netizen is that relating to privacy in the online environment. The Act does not address this critical issue of protecting privacy on-line. The Act refers to on-line privacy in only two areas namely in sections 43 and 72. Section 43 refers to unauthorised access into computer, computer system/network downloading data, causing denial of access of any person authorised to access, causing disruption to any computer, introducing computer contaminant etc. Section 72 speaks of punishing the person, who has secured access to any electronic record, book, register, correspondence, information, document or other material in pursuance of any powers conferred on him under the Act, discloses such information without the consent of the person is liable for the breach of confidentiality and privacy. However, section 43 and 72 does not have nay bearing on the violation of individual's privacy in cyberspace.

These two sections do not mitigate the privacy concerns of any person in this digital era. Does the introduction of these two provisions prevent the data mining practices adopted by most of the online advertising agencies? What is needed is a clear-cut provision prohibiting practices like spamming. Most of the states in U.S. already have legislations prohibiting spamming. The importance given to online privacy in U.S. can be understood from its act of introducing four legislations to address this issue, while not even a specific clause is mentioned in the IT Act.

Consumer is worried about his personal data collected by various commercial agencies. Who protects this data on the network? Is this to be done by the businesses

⁹⁹ Ibid. Section 91.

¹⁰⁰ Ibid. Section 92.

¹⁰¹ Ibid. Section 93.

who collects it or the service provider or the government or any person authorized by the government or any independent body? What control will data subjects have over their personal data, which is collected? What data will be available? What are the purposes for which this data is used? Before transferring data to a third party, will the prior permission from the data subjects be obtained? The IT Act has no answers to these questions.

It has been an accepted practice in most of the civilised jurisdictions that Internet Service Providers (ISP) are not responsible for any crime committed by it's subscribers. ISP transmits third party content from their computers to other without any human intervention from the ISP. Perfect example is the On-Line Copyright Infringement Liability Act, 1998, where every function of a service provider is explained along with his liability and procedure to be followed in each case, which makes it explicitly clear. But IT Act responds to the service providers' liability by stating that he is not liable "if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention". It is very difficult to prove "lack of knowledge" and the term "due diligence" has not been explained anywhere in the Act. The Act should have taken into consideration the fact that it is practically impossible for any ISP to monitor every information the subscribers are sending, taking into consideration the global reach of the Internet. A few ISPs allow users to have their messages transmitted anonymously to other ISPs. To screen all anonymous messages for content is difficult and this would place an undue burden on the ISP.

The Act totally ignores the intellectual property regime, which should be the backbone of any e-commerce transactions. Although it is argued in this dissertation for an overhauling of the Copyright Act i.e. for the separate addressing of intellectual property rights like the enactment of the Digital Millennium Copyright Act, it is honestly believed that the Act should have at least addressed the basic issues like the right and liabilities of a domain name holder, good faith registration etc.

The Act is also silent about the regulation of payment gateways. Moreover, the Act doesn't address the issue of encryption standards and other subsidiary issues arising out of the export and import of encryption technologies.

¹⁰² Ibid. Section 94.

The IT Act creates a few fresh problems also. It is mentioned that the Act applies to any offence or contravention committed outside India by any person. It is further stipulated that with regard to offences and contraventions, nationality of the accused is irrelevant, if the act constituting the offence involves a computer, computer system/network located in India. It is not mentioned anywhere in the Act, how the extra-territoriality of the Act will be enforced. The second concern regarding jurisdiction is that, the Act does not talk about the territorial jurisdiction of the Adjudicating Officer and the CRAT.

Comparison of Indian legal system with that of select countries

Countries	Digital signature	Encryption	E-commerce	Privacy	IPRs
U.K.	√	√	√	√	√
U.S.A.	√	√	√	√	√
Australia	√	X	√	√	√
Canada	√	X	√	√	√
Malaysia	√	X	√	X	√
Singapore	√	X	√	√	√
India	√	X	√	X	X

√ Countries having either enacted legislation or are in the process of doing so in the above-mentioned areas.

Not only the four Acts mentioned in the IT Act, there are more than a dozen Acts to be amended to provide the adequate legal framework, if the e-commerce is to flourish in India. If only there is a clear-cut regulatory framework, the businessmen

and the consumers will get confidence to engage in digital transactions. The crucial areas to be dealt immediately are the following¹⁰³.

- (1) IT Act needs amendment, as it is not applicable to Negotiable Instruments and thus creating impediments for digitalisation of Negotiable Instruments.
- (2) Any entry in Banker's Book shall be deemed to be primary evidence of such entry and such Banker's Book should be regarded as document under sec 62 of Evidence Act, 1872.
- (3) Section 4 of proposed Electronic Fund Transfer Act is required to be brought into force immediately as it prohibits organising, promoting and operating EFT system without prior authorisation of RBI.
- (4) Sections dealing with consumer protection are required to be enacted in the Proposed Electronic Fund Transfer Act.
- (5) Should give effect to following Draft Bills provided by Sheare Committee.
 - (1) Draft Electronic Fund Transfer (EFT) Act.
 - (2) Draft Amendment to Reserve Bank of India (RBI) Act.
 - (3) Draft Amendment to Banker's Book Evidence Act.
 - (4) Draft RBI (EFT) regulations.
- (6) Amend RBI Act to bring organisations issuing E-cash under the control of RBI by asking them to keep an account with RBI so that RBI can keep track of their activity and to make E-cash legal tender.
- (7) Amend the Negotiable Instruments Act, 1888, to make E-cash a Negotiable Instrument.
- (8) The Trade Marks Act, 1999 needs amendment so that the Trademark holder shall get pre-emptive rights over Domain name.

¹⁰³ The suggestions no. (2), (3), (4), (5), (6) were given by Dr. N.L. Mitra to the Researcher in unstructured interview on 16 April 2000, at National Law School of India University,

- (9) The Copyright Act, 1957 needs a new appearance to control copyright violations over the Internet.
- (10) The Indian Telegraphs Act, 1885 needs an amendment to implement encryption system as a tool for security and confidentiality.
- (11) The Company's Act, 1956 and the SEBI Act need an amendment in order to get incorporated the new virtual market.
- (12) The Consumer Protection Act, 1986 needs an amendment in the line of Distance Selling Directive of the U.K/EU.
- (13) The Monopolies and Restrictive Trade Practice (MRTP) Act, 1969 needs an amendment taking into consideration, the on-line advertising issues like comparative advertising, promotion policies, regulated activities etc.
- (14) The Indian Post Offices Act, 1888 and the Indian Wireless Telegraphy Act of 1993 should be suitably modified in the light of growing importance of Information Technology in our day-to-day life.
- (15) Income Tax Act, 1961 needs to be amended after the decision on the method of taxing the e-commerce revenue, like whether consumer will be based under the central government or under Interstate commerce.
- (16) A Privacy legislation has to be enacted in tune of United States of America's Unsolicited Commercial Electronic Mail Choice Act of 1997, Electronic Mailbox Protection Act of 1997, and E-mail Users Protection Act of 1998.
- (17) A Data Protection Legislation has to be enacted in tune of the UK Data Protection Act, 1998.

CONCLUSION

The very idea of setting up of a separate nodal agency in Ministry of Information Technology to deal with infotech is justified by the holistic nature of Information Technology-cutting across the conventional portfolios like electronics,

Banglore. The suggestions (8) and (9) were provided by Prof. N.S. Gopala Krishnan, Cochin University of Science and Technology on 26 April 2000.

communication, Information and broadcasting and bodies like National Information centre. According to Government notification, the Ministry will indeed focus on the promotion of the Internet and e-commerce, Electronics, software exports and all IT related policy matters.

Accordingly the Government Policy should be, to harmonise law governing electronic commerce, to facilitate cross-border recognition and enforcement of electronic transactions and signatures, to enact legislation to update laws governing e-commerce. Business can thrive only when a good domestic environment, which facilitated by the government, supports it. This is true for e-commerce also. A supportive domestic framework creates a favourable climate for investment. The government should encourage commercial applications such as using smart cards, e-governance etc, have legislation to protect the privacy, intellectual property rights, have a rational taxation plan, security laws etc. This may not necessarily mean the introduction of new laws but the tough enforcement of existing laws. As commerce moves from paper records to electronic records, simple, predictable and equitable legal and regulatory solution both at the domestic and international levels is warranted.

Conclusion

It is sure enough that India, which is on the threshold of another IT revolution in which E-commerce is the focus, can gain immensely by way of clear policy direction backed by a structured government apparatus. E-commerce, the new business paradigm is creating problem for the regulators and policy makers. An international understanding is yet to be reached, with only a handful of countries having created legal regimes to deal with electronic transactions. Since e-commerce has made irrelevant the political boundaries any policy or law to be evolved, should take into consideration, the global aspirations. Already, in a world where countries are divided on political or geographical or economic basis, it is extremely difficult to arrive at a policy to satisfy everybody. The question yet to be answered is who will gain at whose cost?

E-commerce for the producers and consumers has created ample opportunities, which have never been thought before. The big businesses have already started reaping the gains of e-commerce. For them cheap means of communications, mass customerisation, global presence, and eradication of supply chains have resulted in the low production cost. Customers on the other hand enjoy a global choice of goods at a low cost, personalised products, etc from his home.

Technology with its benefits also has disadvantages. Still there has to be evolved a safe security standards for business transaction, so that the confidentiality of communication can be maintained. Consumer is also worried of his privacy rights. In E-governance, the policy maker will find a difficulty in arriving at a conclusion of the debate between Privacy rights and the freedom of expression.

The research works mainly focused on a few legal issues that came to the fore in specified areas like Contracts, Intellectual Property Rights with concentration on Copyright and Trademarks issues, Payments and Advertisements. The research focused on the identification of the issues and how legal systems have addressed it.

Just like any other commercial transaction, the e-commerce transactions also involve formation of contracts. But On-line contract formation has no ceremonialities present like the traditional contract. A contract is usually formed after several negotiations, each participant trying to make their specific terms reflect in the final

agreement. Through these negotiation processes, contracting parties will try to clarify any ambiguity present in agreed terms. The terms and conditions in the contract are displayed on the website and are given to the consumer in the form of a 'take-it-or-leave-it' basis.

Consent of the contracting parties is essential for contract formation. It can happen that a party might accept a contract by clicking 'I agree' button without actually reviewing the terms and conditions which are placed in some other webpages. This may lead to the party claiming the contract to be void. Answer to such a situation depends on the visibility of the terms and conditions to the contracting party. Knowing the identity of the customer is also important for any contract formation as law prohibits contracts with certain individuals like persons having unsound mind, minors etc. This may create problems for the On-line merchant, as the above said details of a person cannot be understood from his e-mail address.

The section on contract discussed in detail about the requisites for an On-line contract formation. Still there are many legal positions to be made clear both in the national and international level regarding the issues like whether an electronic mail falls under the postal rule or receipt rule? There should be an uniform understanding of issues like whether web advertisements is an offer or invitation to offer, when is offer and acceptance completed, what should be the standard terms and conditions in a contract, the question of "satisfactory quality" etc are to be addressed. Where should the standard terms and conditions of the On-line contract be displayed? Where is the contract-concluded etc. The area of contracts will have to be addressed in the international level, since the players are from the corners of the globe. The law regarding contract formation through paper medium, telephonic messages, telex etc are clear. In case of On-line contracts, the position is still vague.

As far as intellectual property protection in cyber space are concerned the major issues are issues of copyright and trademark. The basic criterion for obtaining a copyright in countries like U.S., Canada etc is fixation along with originality and creativity. The Indian Copyright Act is silent about the requirement of fixation. When one logs onto a website, the computer cache will always have a copy of the web page stored temporarily in its Random Access Memory (RAM). The US Courts have held that even this practice

is sufficient to satisfy the fixation requirement. The Copyright Act should make clear, whether such temporary storage can be considered as fixation and thus entitled to copyright protection. Section 52 of the copyright Act deals with certain Acts, which are not considered as copyright infringement. This section should be amended to include browsing also. The Act should also make it clear whether publishing on the web constitute communication to the public and if so, required sections have to be amended.

The WIPO Copyright Treaty, 1996 makes it obligatory for signatories to provide protection against the removal or alteration of any electronic RMI without authority. The Indian Copyright Act makes it mandatory only in case of sound recording (section 52A) and video film [52A(2)] suitable amendments should be made to this section so as to include online works also. The WIPO Treaty also makes it an offence to remove or alter any electronic rights management information without authority and also the practice of distributing the work, broadcasting or communicating to the public etc. knowing that RMI has been removed or altered without authority. The Indian Act should also be amended to include this clause. The Information Technology Act, 2000 does not address the liability of the Internet Service Providers adequately. The copyright Act should be amended to the tune of Online Copyright Infringement Liability Limitation Act, 1998 and also the EU E-Commerce Directive. The Act should also clarify whether the practices like linking, framing, coaching, archiving etc may amount to copyright infringement or not.

The new Trademark Act is silent about the issues of domain name. It is yet to be seen the provisions pertained to well known mark would take care of the misuse of trademark for domain name registration. . Domain name can be included in one of these classes, taking into consideration, the protection of service marks and the practice of attributing trademark rights to domain name. The Indian courts have made the legal position clear in case of domain name disputes. The trademark violations in cyberspace like use of Meta tags, Linking, Framing etc. have to be addressed by a new amendment to the Trademark Act, 1999.

The new issues that cropped up in the field of intellectual property rights due to the emergence of Internet should have a uniform answer. Presently courts in the same

country are giving different opinions. Without having a concrete understanding, the industry is also indulging in the practice of out of court settlement, which makes it difficult the emergence of the new legal position.

Getting paid for the goods/services delivered is important for any form of commerce to progress. In the digital world the traditional payment mechanisms have become obsolete. E-cash is the future of on line trade. But its introduction is causing problems to regulators and policy makers. The important question thrown to the fora that whether Private Agencies should be allowed in minting e-currencies? If not, will government mint e-currencies, so that industry can maintain the speed at which technology is making changes. An entirely new framework is needed for addressing these issues. E-cash pose problems for the central government to have control over the economy. Presently it is impossible to predict how it may affect the behaviour of many economic actors. Private e-cash currencies will make it difficult for the central banks to control or even measure monetary aggregates. Sometimes these currencies may be beyond the regulatory framework of the state. With higher degree of encryption it will almost became impossible to trace e-cash. It may be impossible for the government to track e-cash without indulging into the privacy concerns of its citizens. The greater debate would be that of privacy of citizen versus legal enforcement.

More basically, who imposes tax on goods/services purchased or in general terms, the question of jurisdiction becomes another bone of contention. Seignorage loss is yet another area, which is causing concerns for the governments. E-cash also brings to the fore new forms of financial crimes and frauds that may be hard to detect and since the players involved may be from different corners of the world, it may be impossible to detect fraudsters. One of the biggest stumbling blocks to online payments is the level of security. While Indian companies uses only 48kbps level encryption code, their American counterparts use 128kbps encryption, which is presently not available to India due to the export restriction imposed by U.S. on encryption technologies.

E-cash has its consequences on economic and political governance. Government's control over economic and political factors stems from its control over the territory it governs. But e-cash and e-commerce do not occur on any territory but in the cyberspace

where nobody has any control i.e. the basic or the fundamental problem that e-cash poses for governance results from this disconnection between electronic markets and political territories. Hence, a digital economy demands an increase in international co-operation, harmonisation of national legislations and strengthening of international monetary institutions.

Internet advertising is another area where commercial use has not been fully exploited due to the uncertainty remaining regarding the laws, which are to be used for regulating those advertisements. Presently national laws and regulations are used to regulate web advertisements, which has been published to the world at large. As a result of this practice, what may be legal in one jurisdiction may be illegal in some other jurisdiction (for example, alcohol advertising). Businesses are finding difficulty in satisfying the laws of both the country of origin and the country of publication. The real essence of the problem is the issue of jurisdiction i.e. where can an advertiser be sued? Moreover a variety of legal issues have sprung up with regard to web advertising like comparative advertising, privacy issues due to the collection of personal data and the practice of spamming, trademark issues like linking, framing use of meta tags etc and advertising of regulated products.

To minimise the risk of being challenged by several national laws the advertiser should curtail his advertisements to certain jurisdictions only. There can be done with the help of disclaimers. Customers from certain jurisdictions can be eliminated after identifying their country of origin from the e-mail addressed or using server checks etc. The webadvertisers should be cautious of the regulated activities, prohibited advertisements especially those directed at children, financial advertisements etc. The e-trader should take into consideration the Cultural, Political, Religions and Social polarisations in this world and should basically ensure that an advertisement should not hurt these sentiments.

In the coming years, even if a universal framework cannot be reached, at least a minimum standard for regulating should be arrived at so that unnecessary burden may not be placed on the online business which is already facing many impediments. Taking into

consideration the fact that there is no international understanding regarding web advertising, the e-trader in case of any doubts, should always err on the side of caution.

There is no specific law ensuring privacy in India. For e-commerce to flourish there should be a legislation, which should address the privacy of the citizens. In U.K., the data Protection Act 1998, adequately answers the privacy regarding the personal data collected. The eighth principle of the Act protects the transfer of personal data to any country outside the European Economic Area, ensuring adequate protection for the rights of the data subjects. It is essential for the e-commerce businesses to transfer data to other countries for processing at the time of contract formation, payment etc. Hence legislating one is essential for the furtherance of E-commerce business. Spamming is yet another act which raises privacy concerns. In U.S. there are four legislations addressing this issue. A Privacy Act, which takes care of, all these issues are to be addressed in the new Act. The act of gathering personal data through cookies will also have to be addressed.

Consumer Protection Act, 1986 needs an amendment to the tune of the UK unfair Contract Terms Act, 1977. Our Consumer Protection Act, 1986 does not address the unfair contract terms in a Contract. E-traders always develops the terms and conditions in the web contracts to suit their convenience. In order to protect the rights of the consumer in the digital era, this lacunae should be removed in the Consumer Protection Act. The EU Distance selling Directive is another legislation that addresses the consumer rights in the Digital era. The Directive imposes certain requirement consumer contracts negotiated away from business places. They the right to withdraw without compensation, contracts from which includes credit and instalment terms, the main characteristic of the product or service, the estimated delivery time, refund if not delivered with in 30 days are some of the features of the Act. India should also amend Consumer Protection Act, 1986, to the tune of the U.K. Distance selling directive.

The international approach enumerated the work of UNCITRAL, WIPO and WTO. UNICTRAL Model Law has helped many countries in the enactment of e-commerce legislations. With more countries, accepting the same way of approach, will foster an international regime, which accepts a common set of rules for e-commerce transactions. The EU Directive, which was enacted after two years of the enactment of

Model Law is much more precise and addresses the key issues of contract formation, Intellectual property aspects, ISP liability etc taking into account, the American and European experience with e-commerce transaction. The WIPO's contribution in the area of intellectual property especially its On-line dispute resolution mechanism in case of domain name has brought some light in case of alternate dispute settlement mechanism, which has been previously in a chaotic situation. The WTO proposal of tax concession is causing concerns for the developing countries. There are doubtful, or most of the progress in this area has been achieved by the developed world and opening their market in cyberspace may lead to huge loss of revenue in form of tax concession.

India also rose up to the occasion with her passing the Information Technology Act, 2000. Although the basic requirements for e-commerce transactions are answered, it fails to cover all the necessary aspects of information technology law. The regulators should now focus on amending other traditional legislations that hinder the way for a successful e-commerce legal regime. Any laws regulated, should be done with an international perspective, as one has to be in tune with the international regime because cyberspace has no boundaries. The legal regime is one, which should provide backbone to the industry. Traditional Laws should be amended to suit to the digital era. Wherever there are gaps left, new legislation should be enacted especially for answering the privacy issues, encryption standards etc.

Policy Considerations

E-commerce can be considered as a great leveller. It doesn't need the initial huge capital for starting a web based commercial venture. What it needs is a website for taking orders and the efficiency of the business mainly lies in the supply chain management. The new commerce thus saves a lot of money for starting a venture like constructing a company, having a big warehouse, maintaining retail outlets at every big city etc. With a domain name, one can take orders from any part of the world and fulfil it within a specified period. Any new comer can access any remote markets without having actual knowledge of its prior existence. It is no longer the big company beating the small, but in e-commerce transactions, it is the fast beating the slow.

Industrial nations have already obtained a lead due to their better infrastructure facilities and technological base. What the e-commerce business entities urge, is a helping hand from the Government in these areas. To realise the full potential of this business sector, the Government should adopt a non-regulatory, market-oriented approach, with a predictable legal environment to support the industry. As e-commerce is becoming the order of the day, India is still grappling with issues like full convertibility, partial convertibility, taxation, monopolies, competitive laws etc. These issues can hinder a possible growth of business and consequently of national economy.

The primary policy consideration is to have a government vision. For creating a supportive domestic online environment India has evolved a Prime Minister's National Task Force on Information Technology and Software Development in 1998. But many of its recommendations like National Policy on Information Security, Privacy and Data Protection Act, Development of Cryptology and Cyber Security, amendment of Indian Telegraph Act, 1885, Indian Wireless Telegraphy Act, 1993 etc are yet to be realised. Countries like Singapore and Great Britain are actively promoting the information society by clear Governmental actions like moving to e-governance by the year 2001 and 2008 respectively.

A supportive domestic legislations facilitating a clear, predictable legal environment is *sine qua non* for getting confidence of international business entities in promoting foreign direct investments in India. Legislations enforcing copyright protection for materials traded online, maintaining secure delivery, protecting privacy of the individuals and removing other legal impediments are essential for the smooth functioning of e-commerce. For example, Italy, U.S., Singapore, European Union frameworks for legally binding digital signatures encourages commercial application like shopping using latest credit card technologies.

Telecommunication infrastructure development is yet another one. Across many countries, government supports the industry by enabling adequate telecom infrastructure like high band with reasonable cost, which is one of the key elements in promoting on-line trade. For example in China, fibre optic lines doubled in 1996 to 100,000; the total

number of telephone lines will reach one seventy million and the Government has constructed a ChinaNet Programme to develop basic internet networks for the public. Providing infrastructure is primarily done by privatising and deregulating the government sector. A typical example is Finland, whose early initiatives towards deregulating the telecom sector has led to the development of a wide range of value added telecommunication services, including the Internet. Conversely, across Southern Europe telecommunications liberalisation has been slower retarding the value added telecommunication services like the Internet.

The government should take initiative by being the leading user of online services. G2G and G2B procurements will help to a large extent in moulding industry confidence in online commerce. In Canada, delivering Government service and procurement functions on-line boosts the on-line capacity of firms. In Hong Kong, the Trade link program encourages several thousands of small and medium sized firms to go on-line. Singapore Government project for implementing smart cards, created opportunities for its citizens to use various digital product while the efforts of Hong Kong government in the banking sector helped the booming of the banking industry in adopting various e-payment methods like digital cash, Mondex, smart cards etc.

A well-planned Industry policy will encourage on-line commerce. The Singapore Government progress of EDI standardisation has led to the uptake of e-commerce by the manufacturing industries. Small and medium sized enterprises should be encouraged to go on-line. In Australia, government support for initiatives like Australian Electronic Business Network (AeBN) boosts small firms awareness of how e-commerce can help achieve business objectives and contributes to rising skills levels in implementing on-line business models.

Venture capital is yet another area where government should allow consideration. Indian government has allowed an Rs 100 crores venture capital fund for IT industry. Moreover the government encourages listing on to U.S. equity markets to circumvent shortages in venture capital, which has been a move in the right direction.

Research and Development of the existing technologies together with an apt industrial policy is essential in the arena of e-commerce as the technology is changing in every 18 months.

Research can be further extended to areas like Taxation, Competition Law, Alternative Dispute Settlement Mechanism, Privacy Law, Security Law and Insurance Law. Also the role of e-commerce in the advancement of developing countries will call for a separate and focused attention. In fact a well-rounded study of emerging international norms in this field is in order.

Selected Bibliography

1. Primary Sources

International and National Documents

WTO Declaration of Second Ministerial Conference, Geneva, 1998

WTO General Council Annual Report, 1999

WIPO, Final Report of the Internet Domain Name Process, April 30, 1999

Council for Trade in Goods, Work Programme on Electronic Commerce, Information provided to General Council, G/C/W/158, 26 July 1999 (99-3144)

Report of the Committee on Trade and Development, WT, COMTD, 15, 30 November 1998, (98-4799)

Council for Trade Related Intellectual Property Rights, Annual Report (1998) of the Council for TRIPS. IP/C/15, 4 December 1998, (98-4875)

Council for Trade in Services, Work Programme on Electronic Commerce, Interim Report to the General Council, S/C/8, 31 March 1999, (99-1371)

Council for TRIPS, Work Programme on Electronic Commerce, Progress Report to the General Council, IP/C/18, 30 July 1999, (99-3254)

UNCTAD : Electronic Commerce : Legal Consideration; UNCTAD/SDTE/BFB/1

Electronic Signature and Records : Legal, Policy and Technical Consideration, Appendix G to the statement by the legislative and policy making group of America Bar Association

International Treaties and National Statutes

European Electronic Commerce Directive

Singapore Electronic Transaction Act, 1998

WIPO, Performances and Phonograms Treaty, 1996

WIPO Copyright Treaty, 1996

Paris Convention

TRIPS Agreement, 1994

Information Technology Act, 2000

Reserve Bank of India Act

Bankers Book Evidence Act

Negotiable Instrument Act

Trade Marks Act, 1999

Copy Right Act, 1957

Indian Telegraph Act, 1885

Companies Act 1956

The Consumer Protection Act, 1986

Monopolies and Restrictive Trade Practices Act, 1969

The Indian Post Office Act, 1888

Income Tax Act, 1961
Indian Contract Act, 1872
National Task Force on Information Technology and Software Development
Indian Wireless Telegraphy Act
U.K. Sales of Goods Act, 1979
U.K. Supply of Goods and Services Act, 1982
U.K. Misrepresentation Act, 1967
U.K. Minors Contract Act, 1987
U.K. Copyright, Designs and Patents Act, 1988
U.K. Unfair Contract Terms Act, 1977
U.S. Digital Millennium Copyright Act, 1998
U.S. Online Copyright Infringement Liability Limitation Act, 1998
European Copyright Directive
EC Data Protection Directive, 96/9/
U.K. Data Protection Act 1987
U.S. The Lanham Act

2. SECONDARY SOURCES

BOOKS

Brown, David "Cyber trends": *Chaos, Power and Accountability in the Information Age*, Dengein Books, London, 1997.

Chissick, Michael & Kelman, Alistair, *Electronic Commerce: Law and Practice*, (Sweet and Maxwell, London, 1999).

Corp, Cyber, – *The new business revolution James Martin, amacom*, New York, 1996.

Creach, Kennieth C. *Electronic Media Law and Regulation* focal Press, 2000.

Dalme, Jacob, *Electronic mail*, 1995, Artech House-re, Boston,

Dasan, Vasanthan S., Luis r. Ordorica, '*Hernds-on Intranets*', Sun Microsystems Press, 1998, California.

Drai, Alan, *Cyber stocks and Investors guide to Internet companies*, Hover's Business Press, Austin, Texas, 1996.

Gates, Bill, *Business the Speed of Thought*", Warner Books, New York, 1999.

Gates, Bill, *The Road Ahead* Viking, New York, 1995.

Kalakota, Ravi & Whinston, Andrew, *Electronic Commerce: A Manager's Guide* (Addison-Wesley), 1997.

Kalakota, Ravi & Whinston, Andrew, *Readings in Electronic Commerce* (Addison-Wesley), 1997.

- Kaye, Barbara, K. and Medoff, Norman J. *The World Wide Web* California, 1999.
- Keeler, Len, *Cyber Marketing* American Management Association, 1995.
- Kimberley, Paul, *Electronic Data Interchange*, Mc Graw Hill, Inc., New York, 1991.
- Mattan Rahul; *Law Relating to computers and the Internet*, Butterworths New Delhi, 2000.
- Richard Y. Wang Information Technology in Action: Trends and Perspectives". PTR Prentice Hall, New Jersey, 1993.
- Robert A. Paterson, *Electronic Marketing and the consumers*, New Delhi, 1997.
- Robert Groth, *Data Mining- A hands-on Approach for Business Professionals*, Prentice Hall PTR, New Jersey, 1998.
- Rose, Marshall T., *The Internet Message*, PTR prentice Hall, Inc., New Jersey, 1993.
- Rosenoer, Jonathan, *Cyber law: the Law of the Internet*, springier, New York, 1997.
- Sadanandan, P. & Chandrasekar, R., *Information Technology for Development* (Tata McGraw-Hill Publishing Co. Ltd., New Delhi, 1987).
- Schneier Bruce *E-mail security*, John Wiley sons, New York, 1995.
- Schwartz, Evan I., *Web economics: "nine essential principles for growing your business on the World Wide Web"* Broad way Books, New York, 1997.
- Schwartz, Gvan I, 'Digital Darwinism', Broad way Books, New York, 1999.
- Seybold, Patricia B. and Marshak, Ronni T., *Customers.com*, Times Books, New York, 1998.
- Singleton, Susan and Halbstern, Simon, *The Law, Business and the Internet*, Tolley's, Great Britain, 1999.
- Smith, Graham J.H., *Internet Law and Regulation*, London, 1998.
- Sokol, Phyllis. K., *From EDI to Electronic Commerce*, New York, 1994.
- Wang, Charles B., *Techno Vision II: Every Executives guide to understand and mastering technology and the Internet*, McGraw Hill, New York, 1997.
- Zeff, Robin and Aronson, Brad, *Advertising on the Internet*, second edn, John Wiley & Sons Inc. New York, 1999.

A. ARTICLES

Anand, M., Hooked!, *Business World*, 8 November, 1999, p.22-28.

Anand, M., Pick the Right ISP, *Business World*, 15 November, 1999. p.58-59.

Anand, M., Trading on the Net, *Business World*, 26 July, 1999, p.30-34.

Arora, Vikas, Is Your Information Safely Locked?, *The Complete Magazine on IT*, February, 2000 p.49-51.

Babani, Anoop, CyberNews, *Business India*, 18-31 October, 1999, p.18.

Bala, M.L., Electronic Commerce – the EDI Way, *Invention Intelligence*, March, 1998, p.112-118.

Bharati, Pragma Can EDI Provide Solutions for E-Commerce, *Express Computer*, June 15, 1998.

Bharati, Pragma Internet: A Powerful Information Tool, *Express Computer*, March 23, 1998.

Bhargava, Mala, Why a Website? *Business World*, 17 May, 1999, p.56.

Bhatia, Rochika, E-Commerce Security, Singh, *Telematics India*, June, 1999, p.30-32.

Chander, Bring Subhash, Informatic Security Imperatives: An Over-view, *Telematics India*, March, 1999, p.55-57.

Chowdhary, Sudhir, Big Leap for Net Services, *Computers Today*, 15 February, 2000, p.68-69.

Chowdhury, Sudhir and Vishesh Prakash, Where Net Managing Need Not be a Nightmare, *Computers Today*, 1 August, 1999, p.42-51.

Coleman, Arthur, Innards of an E-Corporation, *Computers Today*, 1 October, 1999, p.56-59.

D. Srilatha, M.K. Shankar, Gunzan Bannerjee, E-Commerce – is it working, *Computer Today*, June 1998.

Dash, Jnan R, Click and Mortar, *Dataquest*, 16 November, 1999, p.59-60.

Datt, Namrata, Ready for 2004?, *Business World*, 13 December, 1999, p.30-33.

Deb, G.K., How Secure is Internet?, *Telematics India*, January, 1998, p.67-71.

Deshpande, Vinay L., Whither India's IT Manufacturing Industry?, *Dataquest*, 31 January, 2000, p.99-102.

Ellis, Eric, Dotcom Mania, *Time*, 7 February, 2000, p.34-43.

- Garcia, D. Linda, *Networked Commerce: Public Policy Issues in a Deregulated Communication Environment*, *The Information Society*, Vol.13, No.1, January-March 1997.
- Gattani, Abhishek, Hachers: A Vilified Lot of Heroes, *The Complete Magazine on IT*, July, 1999, p.35-38.
- George, Philip, A High-Scoring Website, *Business World*, 13 December, 1999, p.52.
- George, Philip, Bang on Target, *Business World*, 29 November, 1999. p.50.
- George, Philip, Pitfalls of Net Adds, *Business World*, 1 November, 1999, p.58.
- Gralla, Preston, Online Shopping, *Computers Today*, 15 May, 2000, p.85-89.
- Gupta, Sanjeev and Shameena Gupta, E-Commerce and You, *Paradigm*, January, 1999, 3(1), p.145-153.
- Halbe, Anand, How to Build a Safe Network, *Computers Today*, 1 September, 1999, p.60-62.
- Hodges, Mark, Is Web Business Good Business?, *Technology Review*, Vol.100, No. 6, August-September, 1997.
- Hoffman, Donna L. & Novak, Thomas P. A New Marketing Paradigm for Electronic Commerce, *The Information Society*, Vol.13, No.1, January-March 1997.
- J. Kobrin, Stephen Electronic Cash and the End of National Markets, *Foreign Policy*, Summer, 1997.
- Jones, Chris End to End Internet Security Still Depends on Encryption Apps, *INFO WORLD*, Vol.19, No.14, April 7, 1997.
- Joshi, Vineet, E-Commerce: Are You Ready for it?, *The Complete Magazine on IT*, October, 1998, p.51-55.
- Karnani, Roop, The E-Biz Show, *Business India*, 29 November, 1999, p.140-141.
- Kaur, Kavita, Cheques and Balances, *Computers Today*, 15 August, 1999, p.42-45.
- Kaur, Kavita, Penny for Revolution, *Computers Today*, 1 December, 1999. p.80-83.
- Kaur, Kavita, The Portal War, *Computers Today*, 16 March, 2000, p.42-52.
- Khandekar, Sreekant, Our Product is Knowledge, *Business World*, 24 May, 1999, p.56-57.
- Khanduri, Manish, Digital Does a Reboot, *Business World*, 17 May, 1999, p.46.

- Kirn, Walter, DotCom Vs. NotCom, *Time*, 31 January, 2000, p.46.
- Kittu, Vijaya, Hackers Versus Security, *The Complete Magazine on IT*, May, 1998, p.80-83.
- Kittu, Vijaya, The New World Order, *The Complete Magazine on IT*, July, 1998, p.29-30.
- Kobrin, Stephen J., Opening Doors for Global Trade, *The Complete Magazine on IT*, April, 1998, p.68-71.
- Kumar, Vasant, Strategy in the New Age, *Business World*, 14 February, 2000, p.54.
- Kuttappan, Latha and Chandradeep, E-Business / E-Commerce, *Dataquest*, 31 October, 1999, p.144-149.
- Mathur, Sandeep, Innovation, Leadership and Knowledge Management, *Dataquest*, 31 January, 2000, p.103-104.
- McCarthy, Terry, China Dot Now, *Time*, 28 February, 2000, p.16-23.
- Mohideen, Nabeel, Rising Star?, *Business World*, 29 November, 1999, p.52.
- Motial, S.S., Electronic Commerce: The Promises and the Security Risks-An Overview, *Telematics India*, May, 1999, p.73-75.
- Mucller, Milton, Telecommunications Access in the Age Electronic Commerce: Towards A Third Generation Universal service Policy, *Federal Communications Law Journal*, Vol.49, No.3, April 1, 1997.
- Mundrey, Karnvir, To B2B Or Not to B2B, *PC World*, February, 2000, p.101-106.
- Netke, Shirish, E-Com Shadows, *Computers Today*, 15 January, 2000, p.66-67.
- Nishar, Atul, TheNet Within, *Business India*, 29 November, 1999, p.147.
- Ohri, Swasthi, Electronic Store: Selecting the Right Software, *The Complete Magazine on IT*, January, 1999, p.28-30.
- Pal, B.N., Real Life Applications Information Security Systems, *Telematics India*, March, 1999, p.58-61.
- Penny Lunt, "Payments on the Net: How many? How safe?" *ABA Banking Journal*, Nov. 1, (1998)
- Picot, Arnold, Organisation of Electronic Markets: Contribution from the New Institutional Economics, *The Information Society*, Vol. 13, No. 1, January-March 1997.

- Pitroda, Sam, Getting Indian to go Online, *Business World*, 31 January, 2000, p.28-33.
- Powell, Mark D., Electronic Commerce: An Overview of the Legal and Regulatory Issues, *International Trade Law and Regulation*, Vol.3, No.3, June 1, 1997.
- Prabhu, Rajendra, Centre Planning to go, *Telematics India*, January, 1998, p.44-49.
- Prakash, Vishesh, Your Home on E-State, *Computers Today*, 1 August, 1999, p.74-77.
- Prasad, Shishir and Navjit Gill, Angels at Large, *Business World*, 15 November, 1999, p.28-33.
- Puri, Karan, Demystifying Smart sourcing, *Computers Today*, 1 September, 1999, p.56-58.
- Raigaga, Haridas, Cyber Laws, *Telematics India*, March, 1999, p.52-53.
- Raigaga, Haridas, Security and Governance for eCommerce, *Computers Today*, 15 February, 2000, p.114-126.
- Roberts, Johnnie L., Desperately Seeking a Deal, *Newsweek*, 24 January, 2000, p.8-15.
- Roy, Roopen, Bits and Atoms, *Dataquest*, 31 January, 2000, p.94-97.
- Sanction, Thomas, A Great Leap, *Time*, 31 January, 2000, p.34-38.
- Satpathy, C., WTO Work Programme on Electronic Commerce, *Economic and Political Weekly*, 25 September, 1999, 34(39), p.2771-2776.
- Sealey, Peter, How E-Commerce Will Trump Brand Management, *Harvard Business Review*, July, 1999, p.171-176.
- Seshan, Sekhar, E-bargaining, *Business India*, 29 November, 1999, p.139.
- Shah, Shimul and Sandeep Joseph, Used cars Dot Com, *Business World*, 8 November, 1999, p.66-67.
- Shah, Shimul, Changing Track, *Business World*, 6 December, 1999, p.68-69.
- Shah, Shimul, Selling Yourself, *Business World*, 6 December, 1999, p.70.
- Shah, Shimul, Surfing the Shops, *Business World*, 31 January, 2000, p.58-59.
- Shapiro, Andrew L. Privacy For Sale: Peddling Data On The Internet, *NATION*, Vol. 264, No. 24, June 23, 1997.

- Shenoy, Meena, Going Global, *Business India*, 18-31 October, 1999, p.92-94.
- Singh, Ranjit, E-Commerce: Into the Age of Borderless Markets, *Telematics India*, May, 1999, p.6-11.
- Singh, Ranjit, Global Information Economy, *Telematics India*, September, 1999, 12(12), p.6-13.
- Singh, Ranjit, Internet Security Concerns, *Telematics India*, May, 1999, p.47-48.
- Singh, Ranjit, Internet: From Education to E-Commerce, *Telematics India*, January, 1998, p.73.
- Sinha, Arunava, E-Biz Models, *Business Today*, 7 October, 1999, p.59-71.
- Sloan, Allan, Hunting the Big Bucks, *Newsweek*, 24 January, 2000, p.16-17.
- Srivastava, Nitin, The S-Bit Bait, *Business World*, 26 July, 1999, p.14-16.
- Stein, Joel, You Can Come Out Now!, *Time*, 1 January, 2000, p.36-40.
- Sundaram, Chandar, A New Chapter for Electronic Commerce in India, *The Economic Times*, Bangalore, March 25, 1998.
- Suresh. N., The Next Generation Business, *Dataquest*, 31 October, 1999, p.59-62.
- Thampi, Praveen S., Snakes and Ladders, *Dataquest*, 16 November, 1999, p.52-58.
- Tucker, Michael Jay The New Money: Transactions Pour Across the Web, *Datamation*, Vol. 43, No. 4, April 1997.
- Vijay, Srinivas, Who Serves the Net Game?, *Computers Today*, 16 July, 1999, p.76-77.
- Vijaykar, Atul, Beyond the Internet Revolution, *Dataquest*, 31 January, 2000, p.97-98.
- Viswanathan, Vidya, Masters of the Web, *Business World*, 24 May, 1999, p.30-35.
- Viswanathan, Vidya, New Hot Dot Coms, *Business World*, 24 January, 2000, p.21-29.
- Waltham, Tony, Managing Your Online Identity, *Computers Today*, 1 September, 1999, p.66-68.
- Wang, Charles B and Sanjay Kumar, I Think We Have an Infrastructure Strategy that Enables E-Business, *Dataquest*, 31 October, 1999, p.64-66.
- Wang, Charles, Wang's World, *Business World*, 6 December, 1999, p.63-64.

UNIFORM RESOURCE LOCATOR

Cyberlaw Series, Department of Electronics, <http://www.doe.gov.in>

Doing business with an "e", <http://www.ibm.com/e-business/what>

Electronic Commerce ... An Introduction,
<http://www.cordis.lu/esprit/src/ecomint.htm>

Electronic Commerce and Digital Signature Legislations,
<http://www.mbc.com/legis/table 02>.

Electronic Commerce and EDI, <http://www.unbsj.ca/library/subject/edi.htm>

Electronic Commerce and the European Union,
<http://www.ispo.cec.lc/Ecommerce>

Electronic Commerce in the National Information Infrastructure, Corporation for National Research Initiatives, <http://www.xiwt.org/XIWT/documents/Ecomm-doc/EcommTOC2.html>

European Union Home Page, <http://www.s700.uminho.pt/ec.html>

Lawrence H. Summers, Deputy Secretary, Department of Treasury, United States,
http://www.treas.gov/treasury/press/pr_052297a.html.

Massachusetts Electronic Records and Signatures Act,
<http://www.magnet.state.ma.us/itd/legal/mersa.htm>

Price Waterhouse Predicts Explosives E-Commerce Growth,
<http://www.internetnews.com/ec-news/1998/03/2601-pw.html>

The Organisation for Economic Cooperation and Development,
<http://www.oecd.org>

The US House of Representatives Internet Law Library <http://www.law.house.gov>

US Department of Commerce –

<http://www.doc.gov/ecommerce>

<http://www.ita.doc.gov/itahome.html> (International Trade Administration)

<http://www.ita.doc.gov/industry/osi.html> (Service Industry and Finance)

<http://www.nist.gov> (National Institute of Standard and Technology)

<http://www.doc.gov/ecommerce> (Secretariat for Electronic Commerce)

<http://www.ntia.doc.gov> (National Telecommunication and Information Administration)

<http://www.uspto.gov> (Patent and Trade Mark Office)

United Nations Commission on International Trade Law,
<http://www.un.or.at/uncitral>

Utah Digital Signature Development Program,
<http://www.commerce.state.ut.us/webcommerce/digsig/dsmain.htm>

WIPO <http://www.wipo.org>.

World Trade Organisation, <http://www.wto.org>