LEGAL ISSUES IN eCOMMERCE

Nishith Desai Associates
Legal & Tax Counselling Worldwide

93-B MITTAL COURT, NARIMAN POINT
MUMBAI 400 021. INDIA
TEL: 91 (22) 282-0609
FAX: 91 (22) 287-5792

220 CALIFORNIA AVENUE., SUITE 201
PALO ALTO, CA 94306, USA
TEL: 1 (650) 325-7100
FAX: 1 (650) 325-7300

nda@nishithdesai.com
www.nishithdesai.com

LEGAL ISSUES IN E-COMMERCE

Aashit Shah and Parveen Nagree
Nishith Desai Associates

Nishith Desai Associates ("**NDA**") is a research based international law firm based in Mumbai and Palo Alto, Silicon Valley, specializing in information technology, e-commerce, telecommunications, media and entertainment laws, international financial and tax laws and corporate and securities laws. It has acted as strategic and legal counsel to premier corporates in their Internet forays, including IL&FS, GE Capital, Jasubhai Group, software majors such as i2 Technologies and Mahindra British Telecom and communication companies such as Space Systems/Loral, New Skies Satellite, Flag and WorldTel. Apart from structuring and acting for a large number of private equity funds in India, NDA has been involved in American Depositary Receipt (ADR) offerings of Indian companies, representing Wipro, Rediff.com and Silverline Technologies and acting as underwriter's counsel in Infosys Technologies and Satyam's ADR offerings. NDA was involved in the first cross-border stock swap merger from India - BFL's acquisition of MphasiS besides Silverline's acquisition of Seranova Inc in an ADR stock swap deal. It had prepared a white paper for the **Global Information Infrastructure Commission** titled "Legal, Tax and Policy Reforms to promote e-commerce in India". It has also advised the Government of India and Internet Service Providers Association on e-commerce issues in the WTO regime. It represented NASSCOM at a Joint WTO-World Bank Symposium on Movement of Natural Persons held in Geneva in April 2002.

NDA was recently as the **"Indian Law Firm of the Year 2000"** and **"Asian Law Firm of the Year 2001 (Pro Bono)"** by the International Financial Law Review, a Euromoney Publication. It has also been ranked as having a **leading practice in Private Equity, Media and Entertainment and IT and telecommunications law** for 2001-02 by the Global Counsel 3000.

LEGAL ISSUES IN E-COMMERCE

*Aashit Shah and Parveen Nagree **
Nishith Desai Associates

TABLE OF CONTENTS

* The authors have prepared this paper under the guidance of Annapoorna Ogoti and Vaibhav Parikh of Nishith Desai Associates.

I. INTRODUCTION

Simplistically speaking, e-commerce is the mode of conducting business through electronic means. However, there exists no standard definition for the term and different organisations have defined it diversely.

E-commerce is understood to mean the *production, distribution, marketing, sale or delivery of goods and services by electronic means*.[1] The Asia Pacific Economic Co-operation ("**APEC**") has adopted a wider definition of e-commerce to include *all business activity conducted using a combination of electronic communications and information processing technology*.[2] The United Nations Economic and Social Commission for Asia and the Pacific ("**UNESCAP**") has also defined e-commerce as '*the process of using electronic methods and procedures to conduct all forms of business activity*.[3]

Over the past few years, global trade has expanded due to the explosive growth of electronic commerce. Projections indicate that the volume of e-commerce will be approximately US$ 2 to 3 trillion in 2003-2005.[4] While e-commerce is still at a nascent stage in India, certain estimates indicate that the total transaction volume of e-commerce in India is expected to grow rapidly to Rs. 195,000 crore by 2005.[5]

Though at the outset, the prospect of conducting e-commerce may seem uncomplicated and economical, there are a variety of legal factors that an e-commerce business must seriously consider and keep in mind before commencing its activities. The importance of dealing with these complex legal issues has already been highlighted in light of the recent "Napster.com" and "ToysRUs" cases.

While governments across the globe have been grappling with these issues, it seems a long way before any concrete solutions may be reached.

The set of issues that arise may be bifurcated into "**CORE**" legal issues that are relevant to all forms of businesses and "**OTHER**" legal issues, whose relevance may depend upon each particular industry.

[This space is left blank intentionally]

[1] "The Work Programme on Electronic Commerce; Background Note by the Secretariat", Council for Trade-Related Aspects of Intellectual Property Rights, WTO.
[2] "A. Didar Singh, "Electronic Commerce: Issues for the South" Trade-related Agenda, Development and Equity, Working Paper, South Centre, October 1999, p. 4.
[3] "A. Didar Singh, "Electronic Commerce: Issues for the South" Trade-related Agenda, Development and Equity, Working Paper, South Centre, October 1999, p. 4.
[4] See http://ecommerce.wipo.int/primer/section1.html#27 as visited on October 18, 2001. The estimates were taken from OECD (1995, 1997, 2001-2), ITU (1998) and Forrester Research, Inc. (2003-5).
[5] Current e-commerce transaction volume estimated to be between Rs. 15,000 to Rs. 20,000 crore (FY 2000): "E-commerce Opportunities for India Inc." NASSCOM-BCG Report on E-commerce (June 2001), p.7. BCG defines e-commerce to include all electronic transactions including EDI.

II. CORE LEGAL ISSUES

1. Contracts

At the heart of e-commerce is the need for parties to be able to form valid and legally binding contracts online. Basic questions relate to how e-contracts can be formed, performed, and enforced as parties replace paper documents with electronic equivalents.

a. Offer and Acceptance: The Information Technology Act, 2000 ("**IT Act**") deals with contractual aspects of use of electronic records, such as attribution, acknowledgement, time and place of dispatch and receipt. However, since the IT Act is only an enabling Act, it is to be read in conjunction with the Indian Contracts Act, 1872 ("**Contract Act**"). Formation of any contract, under the Contract Act, would involve three main ingredients. There has to be an offer, there has to be an acceptance of the said offer without modification and there has to be some consideration for the contract. These ingredients would be applicable to e-contracts. However, a difficult question that law often arises: How do we know whether the offeree has ACCEPTED the offer?

Additionally, Internet communication does not consist of a direct line of communication between the sender and receiver of e-mail as in ordinary means of communication. The message is broken into chunks in the process of delivery. This raises issues of the exact time of communication of acceptance of the contract as such a time is critical for determination of the rights of the parties. The IT Act has laid down certain methods for determining the exact time and place of despatch and receipt of the e-mail.

b. Clickwrap contracts: Further, various issues arise whether a person would be bound by the terms of a contract without even reading it or without being able to negotiate the terms. For e.g., website XYZ.com offers its newsletters by simply filling in the name and e-mail address on the form provided and then clicking the 'SUBSCRIBE' button after reading and agreeing to the terms and conditions in the Subscriber's Contract. If Mr. A fills in his name and e-mail address and clicks SUBSCRIBE, but actually does not take the time to look at, let alone read, the Subscriber's Contract. Would this amount to a contract with XYZ? This is an example of a "clickwrap contract" which is legally enforceable.[6] But in such a case, some of the issues that would need to be addressed are as to what would be the terms of the contract and would the acceptance of the Subscriber's Contract without even reading it be classified as deemed acceptance?

c. Online Identity: Transactions on the Internet, particularly consumer-related transactions, often occur between parties who have no pre-existing relationship, which may raise concerns of the person's identity with respect to issues of the person's capacity, authority and legitimacy to enter the contract. Digital signatures, is one of the methods used to determine the identity of the person. The regulatory framework with respect to digital signatures is governed by the provisions of the IT Act. However, various countries have different legislations regulating digital signatures. This has been further discussed

[6] *ProCD* v. *Zeidenberg*, available at http://www.law.emory.edu/7circuit/june96/96-1139.html

under the "**Authentication**" section.

2. Security

Security over the Internet is of immense importance to promote e-commerce. Companies that keep sensitive information on their websites must ensure that they have adequate security measures to safeguard their websites from any unauthorised intrusion. A company could face security threats externally as well as internally. Externally, the company could face problems from hackers, viruses and trojan horses. Internally, the company must ensure security against its technical staff and employees. Security can be maintained by using various security tools such as encryption, firewalls, access codes / passwords, virus scans and biometrics. For example, a company could restrict access to the contents on its website only through the use of a password or login code. Similarly confidential information on websites could be safeguarded using firewalls that would prevent any form of external intrusion. Apart from adequate security measures, appropriate legal documentation would also be needed. For example, a company could have an adequate security policy that would bind the all people working in and with the company.

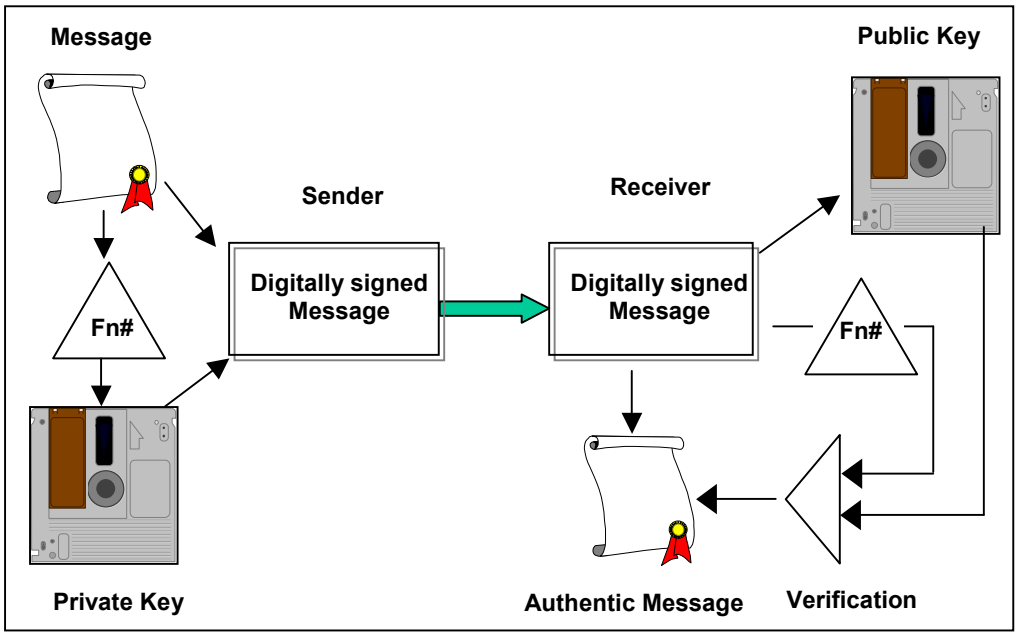
Moreover, a company could also be held liable for inadequate security procedures on its website. For example, last year, a person decided to sue Nike because the Nike's website was hacked and the contents of the domain were re-directed through the person's web servers in the U.K., bogging them down and costing the web hosting company time and money.[7]

3. Authentication

Though the Internet eliminates the need for physical contact, it does not do away with the fact that any form of contract or transaction would have to be authenticated. Different authentication technologies have evolved over a period of time to ensure the identity of the parties entering into online transactions. However, there are some issues that need to be considered by companies.

a. Digital Signatures to be used as authentication tools: The IT Act stipulates that digital signatures should be used for the purposes of authenticating an electronic contract. The digital signature must follow the Public Key infrastructure ("**PKI**"). This acts as a limitation on the use of any other technology for authentication purposes. If Indian e-commerce companies use some other form of authentication technology, it could be said that there has been no authentication at all.

[7] See http://www.wired.com/news/politics/0,1283,37286,00.html (as visited on October 22, 2001).



b. Evolving inter-operable technology standards: Laws of different countries provide different authentication standards, sometimes specifying a clear technology bias. These different authentication standards need to be inter-operable so as to facilitate cross-border transactions. This would need a high degree of co- operation between countries and the technology providers. For example, an e-commerce company that uses PKI authentication technology for online contracts with Indian consumers, may use different / other forms of technology while entering into online contracts with consumers in other countries. In such a case, these contracts with foreign consumers may not be recognised in India as the authentication technology used is not PKI. However, such contracts may be enforceable in the foreign jurisdiction depending upon the laws of the foreign country.

4. Privacy and Data Protection

An important consideration for every e-commerce website is to maintain the privacy of its users. Use of innovative technologies and lack of secure systems makes it easy to obtain personal and confidential information about individuals and organisations. In July 2001, a dozen privacy groups filed a complaint in the US about the privacy issues in Microsoft's Windows XP operating system. Some features of the Operating System store personal information such as passwords and credit card data so that users are not required to constantly re-enter this information as they surf through websites. However, though the Operating System was launched successfully on October 25, 2001, privacy groups have still have criticised the Federal Trade Commission of not taking any action on the complaint.

The web cookie also faces the risk of extinction under a proposed European Commission directive. However, the Interactive Advertising Bureau of UK has marshalled support from several businesses across Europe to launch a lobbying effort that it calls "Save our Cookies" as it believes that British companies could lose approximately US$ 272.1 million

if web-cookies are banned.[8]

Privacy concerns have also been raised regarding the Internet Corporation for Assigned Names and Numbers ("**ICANN**") "Whois" database, which is a publicly searchable resource used to determine the identity of domain name registrants. The database includes the name of the individual or company that registered a given domain name, as well as the owner's address, the dates on which the domain was created, when it expires and when it was last updated. Privacy groups criticised the company for selling information about its registrants, arguing that many of them are individuals who never agreed to having their information sold as a commodity when they signed up for the service.

Some of the important privacy concerns over the Internet include:

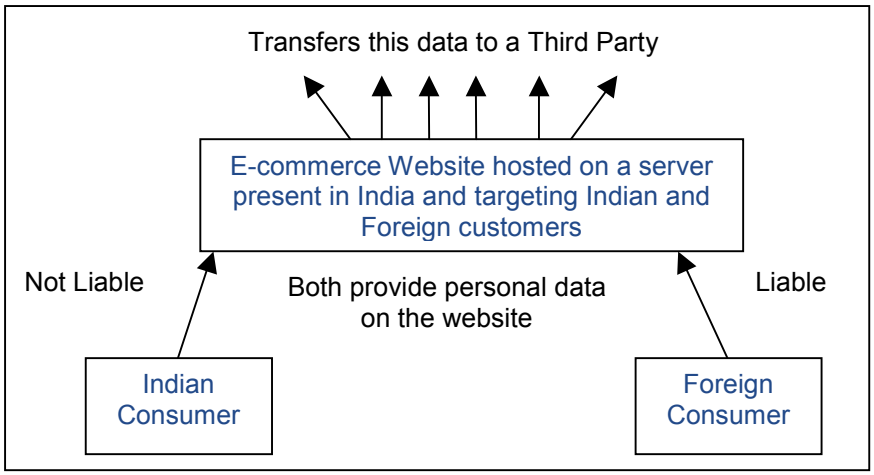
i dissemination of sensitive and confidential medical, financial and personal records of individuals and organisations;

ii sending spam (unsolicited) e-mails;

iii tracking activities of consumers by using web cookies; and

iv unreasonable check and scrutiny on an employee's activities, including their email correspondence.

Presently there exists no legislation in India that upholds the privacy rights of an individual or organisation against private parties. While the Constitution of India upholds the right to privacy as a fundamental right of every citizen,[9] the right is exercisable only against a State action. Even the IT Act addresses the issue of protecting privacy rights only from Government action.[10]



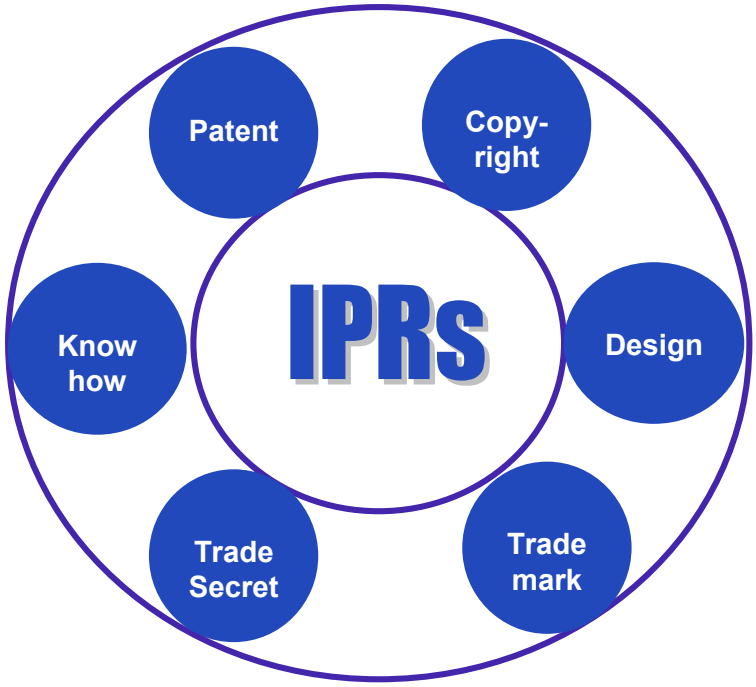
[8] "Europe Goes After the Cookie", October 31, 2001 at www.unwired.com
[9] Article 19 (1)(a) and Article 21 of the Constitution. Refer to *Unni Krishnan, J.P.* v. *State of AP* (1993) 1 SCC 645, *Kharak Singh* v. *State of U.P* AIR 1963 SC 1295, *Gobind* v. *State of Madhya Pradesh* (1975) SCC (Cri) 468. & *People's Union of Civil Liberties* v. *the Union of India* (1997) 1 SCC 318.
[10] Section 69 and Section 72 of the Information Technology Act, 2000.

Nevertheless, in order to gain the confidence of a wary consumer, protecting their privacy rights is a critical concern. For example, if an e-commerce website seeks information from a user and disseminates this information to third parties, it would amount to a violation of the privacy rights of the user and this may turn away existing and potential users from accessing the site in the future.

Moreover, when an e-commerce company caters to consumers in foreign jurisdictions, the foreign jurisdictions may have laws that could make the e-commerce company liable for violating the foreign consumer's privacy rights. For example, Company A in India, that receives some personal data from a consumer in the European Union, and disseminates the information to companies in the US, may be liable for invasion of privacy rights of the consumer.

5. Intellectual Property Rights

One of the foremost considerations that any company intending to commence e-commerce activities should bear in mind is the protection of its intellectual assets. The Internet is a boundless and unregulated medium and therefore the protection of intellectual property rights ("**IPRs**") is a challenge and a growing concern amongst most e-businesses. While there exist laws in India that protect IPRs in the physical world, the efficacy of these laws to safeguard these rights in e-commerce is uncertain. Some of the significant issues that arise with respect protecting IPRs in e-commerce are discussed hereunder.



a. Determining the subject matter of protection: With the advent of new technologies, new forms of IPRs are evolving and the challenge for any business would be in identifying how best its intellectual assets can be protected. For example, a software company would have to keep in mind that in order to patent its software, the software may have to be combined with physical objects for it to obtain a patent.

b. Ascertaining novelty / originality: Most intellectual property laws require that the work / mark / invention must be novel or original. However, the issue is whether publication or use of a work / invention / mark in electronic form on the Internet would hinder a subsequent novelty or originality claim in an IPR application for the work / invention / mark. An e-commerce company would have to devote attention to satisfying the parameters of intellectual property protection including originality requirements in its works to preclude any infringement actions from third parties who own similar IPRs.

c. Enforcing IPRs: As will be discussed under the "**Jurisdiction**" issue, it is difficult to adjudicate and decide cyber-disputes. The Internet makes the duplication, or dissemination of IPR- protected works easy and instantaneous and its anonymous environment makes it virtually impossible to detect the infringer. Moreover, infringing material may be available at a particular location for only a very short period of time.[11] A company must also keep in mind that since IPRs are inherently territorial in nature, it may be difficult to adjudge as to whether the IPR in a work or invention is infringed, if it is published or used over the Internet, which is intrinsically boundless in nature. For example, if 'Company A' has a trademark registered in India for software products, but a web portal based in the US uses the same trademark for marketing either software products or for marketing some other goods, it may become difficult for Company A to sue for infringement. Moreover, due to differences in laws of different nations, what constitutes infringement in one country may not constitute infringement in another. Further, even if Company A succeeds in proving an infringement action, since the IPR that it owns is only valid for India, the scope of remedies that may be available to Company A would be territorial and not global. Thus, the web-portal may be restrained from displaying its site in India or may have to put sufficient disclaimer's on its website. In order to restrain infringement in other countries, Company A may need to file proceedings those countries also. This process may prove to be time-consuming and expensive for the aggrieved Company.

In light of certain technology driven mechanisms such as electronic copyright management systems ("**ECMS**") and other digital technologies that are evolving to prevent infringement, the recent World Intellectual Property Organisation ("**WIPO**") Copyright Treaty[12] explicitly mandates that all contracting parties to the treaty shall have to provide adequate legal remedies against actions intended to circumvent the effective technological measures that may used by authors to prevent infringement of their works.[13] However, these mechanisms may not be commercially viable and their use may also depend on international inter-operability standards, as well as privacy concerns.

d. Preventing unauthorised hyperlinking and meta tagging: The judiciary in many countries is grappling with issues concerning infringement of IPRs arising from hyperlinking and meta tagging activities. Courts in certain jurisdictions have held that hyperlinking, especially deep-linking may constitute copyright infringement, whereas meta tagging may constitute trademark infringement. For example, Company A's website

[11] "Hosts" and web page creators can delete files within a matter of hours or days after their posting.
[12] India has not signed this treaty. Pursuant to this treaty, the US Government has enacted that Digital Millenium Copyright Act to afford protection to digital copyrights
[13] Article 11, WIPO Copyright Treaty, 1996.

provides an unauthorised link to Company B's website, or if Company A's website uses meta-tags that are similar to Company B's trademarks, Company A could be sued for violating Company B's IPRs.

e. Protection against unfair competition: Protection against unfair competition covers a broad scope of issues relevant for electronic commerce. So far, electronic commerce has not been subject to specific regulations dealing with matters of unfair competition. Companies on the Internet, have to constantly adapt to and use the particular technical features of the Internet, such as its interactivity and support of multimedia applications, for their marketing practices. Problems may arise with regard to the use of certain marketing practices such as (i) Interactive marketing practices (ii) spamming (discussed under the "**Privacy and Data Protection**" section) and (iii) immersive marketing. Further, questions regarding the territorial applicability of such standards would also arise.

6. Domain Names

A company that commences e-commerce activities would at first have to get its domain name registered. While registering domain names, if the company chooses a domain name that is similar to some domain name or some existing trademark of a third party, the company could be held liable for cybersquatting.

Over the past few years, domestic and international fora have handled and decided numerous cybersquatting disputes. Recently the ".info" top-level domain was opened for registration and within no time the WIPO has already received two cases for dispute-settlement.[14] Further, another US Company, NeuLevel Inc. who had been restrained from distributing the ".biz" domain names, has now been allowed to do so as the plaintiffs declined to post a bond that would have prevented the company from handling out new domain names.[15] Moreover, the ICANN recently confirmed that it had finalised a contract with Museum Domain Management Association whereby ".museum" has also been included as a generic top-level domain in the global domain name system.[16]

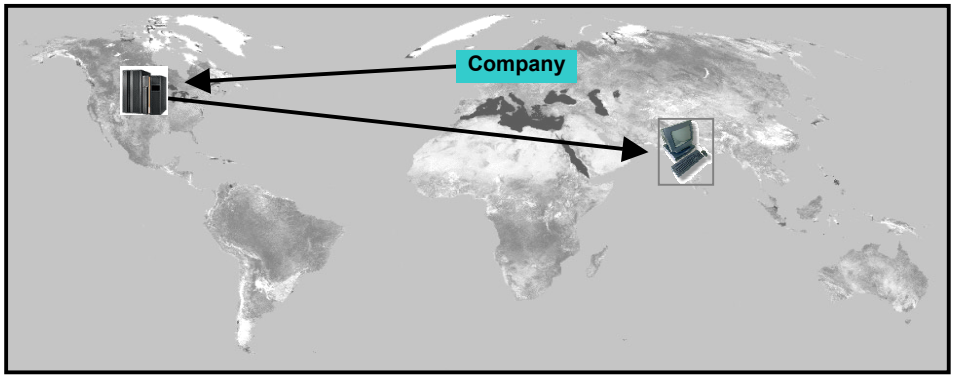
7. Jurisdiction

In addition to the nature of corporate structure, decisions will also have to be taken with respect to the jurisdiction in which the corporate structure should be situated, as it will determine the extent of any liability that may arise against the website. According to the traditional rules of private international law, the jurisdiction of a nation only extends to individuals who are within the country or to the transactions and events that occur within the natural borders of the nation.[17] However, in e-commerce transactions, if a business derives customers from a particular country as a result of their website, it may be required to defend any litigation that may result in that country. As a result, any content placed on a website should be reviewed for compliance with the laws of any jurisdiction where an organisation wishes to market, promote or sell its products or services as it may run the

[14] See: http://www.it.mycareer.com.au/breaking/2001/10/22/FFX18I063TC.html (as visited on November 5, 2001).
[15] See: http://news.zdnet.co.uk/story/0,,t269-s2098080,00.html (as visited on November 5, 2001).
[16] See: http://www.washtech.com/news/regulation/13217-1.html (as visited on November 5, 2001).
17 "Private International Law", Cheshire and North, 11th Ed. pg. 188

risk of being sued in any jurisdiction where the goods are bought or where the services are availed of.

The fact that parties to a contract formed through the Internet may be located in different jurisdictions may have implications for the interpretation and enforcement of the contract.



For example, XYZ, a company in London, having its server in USA, may sell its products to customers in India or other countries. In such a situation, if you receive defective goods or if you regret having made the purchase, the question would arise as to which jurisdiction can you sue the company or claim damages or withdrawal respectively. The company, on the other hand, might find itself confronted with foreign laws, which he may not be aware of. For example, the US courts have in numerous cases have held a company in X state liable in Y state on the basis that the website could be accessed in Y state.[18]

Action, against the host company, may be by way of a civil law suit, criminal prosecution or an action by regulators. The US courts have developed the "minimum contacts" theory whereby the courts may exercise personal jurisdiction over persons who have sufficient minimum contacts with the forum state.[19] These "minimum contacts" may consist of physical presence, financial gain, stream of commerce, and election of the appropriate court via contract.[20] Various courts have held that statements purposely directed at the forum may create sufficient contacts for jurisdiction.[21] This would mean that even if you are not physically present in a nation, you can be sued in that foreign court as long as your website has minimum contacts with that nation. Therefore, a company should insert appropriate choice of law and choice of forum clauses in its online contract, which should specify the jurisdiction to which the parties to the contract would be subject to. Such clauses have been held by courts to be binding upon the parties.[22]

---

[18] California Software Incorporated v. Reliability Research, Inc., 631 F. Supp. 1356 (C.D. Cal. 1986) cited from Julian S. Millstein et al *Doing Business on the Internet: Forms and Analysis (1999)*.

[19] The Due Process Clause of the 14th Amendment of the Constitution of the United States as referred to in "A Separate Jurisdiction for Cyberspace?" by Juliet M. Oberding and Terje Norderhaug http://www.ascusc.org/jcmc/vol2/issue1/juris.html.

[20] International Shoe Co. v. Washington, 326 U.S. 310 (1945) cited from"A Separate Jurisdiction for Cyberspace?" by Juliet M. Oberding and Terje Norderhaug. http://www.ascusc.org/jcmc/vol2/issue1/juris.html.

[21] *Calder* v. *Jones*, 465 U.S. 783 (1984) cited from"A Separate Jurisdiction for Cyberspace?" by Juliet M. Oberding and Terje Norderhaug. http://www.ascusc.org/jcmc/vol2/issue1/juris.html. However, Indian courts have yet not taken any particular stance regarding the "minimum contacts" theory.

[22] *CompuServe, Inc.* vs. *Pattterson*, 89 F.3d 1257, 1259-1260 (6th Cir. 1996) cited from Julian S. Millstein et al *Doing Business on the Internet: Forms and Analysis (1999)*.

8. Liability

Owners of websites should guard against the potential sources of liability which could lead to legal claims against them. Since the Internet knows no boundaries, the owner of a website could be confronted with legal liability for non-compliance or violation of laws of almost any country. Liability may arise due to various activities *inter alia* due to hyperlinking (inserting a clickable link to another site) and framing (incorporating another website into a frame or window appearing within a webpage on the linking site),[23] fraud, libel and defamation,[24] invasion of privacy, trademark and copyright infringement.

a. Contractual Liability: A website that offers goods or services should contain an online contract to which the customer must assent. The contract needs to be carefully drafted to protect the website owner from liability and should address the key terms and conditions for the provisions of goods or services. The contract should clearly establish the exact time and manner of acceptance of the contract. In the event of dispute or breach of contract, the liability of the owner of the website would be limited only to the extent of the terms of the contract.

b. Statutory liability: Depending on the type of business, a website would have to comply with the provisions of the law, central or state, in that jurisdiction. But various nations differ with respect to statutory compliances and permitted activities. The website would therefore, in addition to the state laws, be required to comply with the provisions of the statutes of the countries in which the website would be vastly accessed. Failure to comply with such foreign laws may lead to liability under such law. For example, an Indian company using comparative advertising on the worldwide web, not knowing that such practices are prohibited in Germany and France may be liable for violation of the laws of Germany or France.

c. Tortuous Liability: Liability under tort may arise due to wrongful interference with the business or wrongful defamation or any remark or action that may cause injury to one's property or reputation. Thus, although no contractual relationship may exist as well as where the interference or damage is unintentional, the website owner may be liable for wrongful injury. The law of torts lays down a duty on every man to take reasonable care to avoid any harm to nay person. The owner of the website also owes a duty to the user and is bound to take reasonable care to avoid any harm that may be done.

8. Taxation

The massive growth of e-commerce business has not gone unseen by the tax authorities. Realising the potential of earning tax revenue from such sources, tax authorities world over are examining the tax implications of e-commerce transactions and resolving mechanisms to tax such transactions. In India the High Powered Committee was

[23] Washington Post Co. v TotalNews, 97 Civ. 1190 cited from Richard D. Harroch, Esq. *Start-up and Emerging Companies: Planning, Financing, and Operating the Successful Business* (Vol 2 Revised Ed.)
[24] New York Times Co. v Sulllivan, 376 US 254 (1964) cited from Richard D. Harroch, Esq. *Start-up and Emerging Companies: Planning, Financing, and Operating the Successful Business* (Vol 2 Revised Ed.).

constituted by the Central Board of Direct Taxes, which submitted its report in September 2001. For a detailed analysis of e-commerce taxation, please refer to Mr. Nishith Desai's paper on "**E-commerceTaxation**" that has been presented to the Confederation of Indian Industries.

[This space is left blank intentionally]

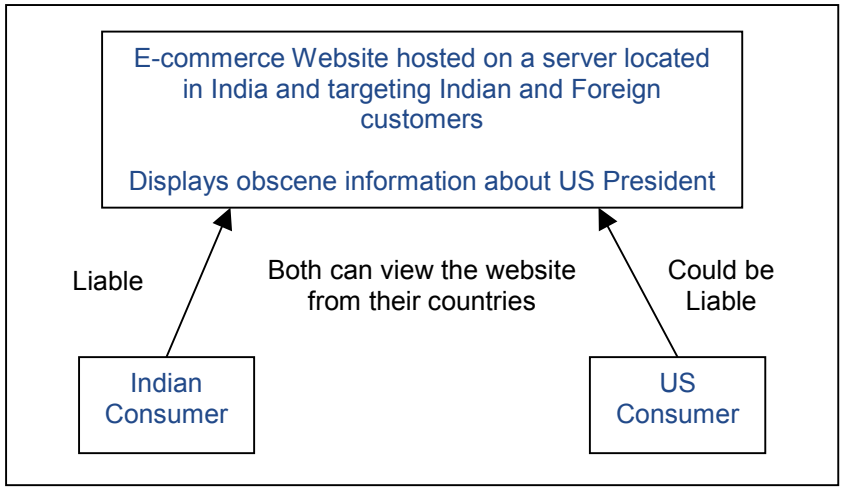
III. OTHER LEGAL ISSUES

The issues dealt with in the above section relate across the board to all e-commerce companies. However, there are certain sector-specific legal issues that need to be kept in mind only be certain companies. This section deals with some of these issues.

1. Content Regulation

The Internet offers a quick and cost-effective means of disseminating information. However, the unrestricted flow of content over the Internet through different jurisdictions could raise various concerns. While traditionally there are several restrictions placed on the content of information that is distributed, the challenge lies in evolving similar parameters to regulate the content of information on the Internet. Some issues that e-commerce companies should bear in mind while publishing or displaying content should be as follows:

a. Nature of Content: Different nations have developed certain standards with respect to display, exhibition and dissemination of content. While regulating content transmission over the Internet, diverse cultural and religious issues, national interests and security and global standards of decency and morality would have to be kept in mind. For example, a website that displays certain content which may be objectionable in Country A, but permissible in Country B. In such a case, based upon whether the courts in Country A have jurisdiction or not (as discussed under the "**Jurisdiction"** issue), the website could be restricted from displaying such content. Therefore, if a company's target audience is a large range of countries, the company should ensure that the content on its website is not against the national, security or cultural interests of these countries.



b. Violation of the Statutory Law: An e-commerce company should also bear in mind that content displayed over the Internet could violate provisions of Indian as well as foreign statutes. For instance, as per the IT Act, any person who publishes any obscene

information in any electronic form is liable to be penalised.[25] The IT Act has extra-territorial operation[26] and therefore, even a website outside India could be penalised for publishing obscene information. As per the diagram above, if a company's website displays obscene information about the US President, the company could be sued under Indian law, and possibly in the US if it violates the provisions of any US law. Similarly, publication of obscene information could also violate the provisions of the Indian Penal Code. Further, publishing information that is deprecating upon women could be in contravention of the provisions of the Indecent Representation of Women's Act.

Several countries have enacted legislations to regulate content on the Internet. The US has passed the Communications Decency Act, Australia had introduced the Broadcasting Services (Online Services) Act, 1999 and Malaysia has enacted the Communications and Multimedia Act, 1998.

b. Licensing framework: Licensing is the key regulatory tool through which public authorities can exercise control over their national markets, particularly in relation to telecommunications and broadcasting. Companies must bear in mind that communication and broadcasting of content must be done after securing appropriate licences. The proposed Communications Convergence Bill, 2001 of India ("**Convergence Bill**") mandates that the any service who obtains licences under the Convergence Bill for network infrastructure facilities, networking services, application services, content application services and value added network application services must abide by the codes and standards laid down by the Communications Communication of India ("**CCI**")[27] that is set up under the Convergence Bill.[28] The CCI has to regulate programme codes and standards to ensure *inter alia,* national interests, sovereignty and security of the country, promotion of culture and values, and prevent obscenity or indecent representation of women or offence to religious views. [29]

c. Imposition of Liability: In the event that content regulations are not abided by, different countries would hold different parties liable. Depending upon the liability provisions in different countries, the following parties may be held liable:

i. the network service provider;
ii. the e-commerce company; or
iii. the user / consumer.

There may be instances where more than one party is held liable for an act or one party is liable in more than two countries for the same act. For example, a company that publishes obscene information and pictures on its website could be liable under the IT Act. Simultaneously, the Internet Service Provider could also be held liable for publication of obscene material unless it proves that it had exercised all due diligence or had no knowledge that obscene content was being displayed by one its users. Further, a company's website that provides links to another website that displays obscene or

[25] Section 69 of the IT Act.
[26] Section 75 of the IT Act.
[27] Section 28 of the Convergence Bill.
[28] Section 6 of the Convergence Bill.
[29] Section 20 of the Convergence Bill.

defamatory material could be held liable for violating content regulations. Therefore, it would be the primary duty of every company to take reasonable precautions to ensure that the content on its website is not in violation of any Indian or foreign content regulation law.

2. Advertisement

Many websites advertise goods or services to customers. The traditional laws of advertising, which apply to ordinary sales, are enacted in the interest of all consumers to prevent deceptive and unfair acts or practices. These laws would also be applicable to advertising or marketing on the Internet. The websites may be subject to any liability that may arise due to false designations, origin, misleading description of fact that are likely to cause confusion or misrepresent the nature, characteristics, quality or geographic origin of the goods or services that are offered for sale in an advertisement.[30] In addition to advertising laws, depending on the kind of business, the websites would also have to comply with the laws of applicable to such a business.

Certain countries have introduced legislations that place limitations on Internet advertising. In such a case, would a website owner be subject to liability for violation of the laws of a country even though it was not aware of such limitations or restrictions on advertisement? For example, the courts have in certain cases held a website of another country liable for fraudulent Internet advertising in violation of a state statute.[31]

Further, an advertisement may be exposed to liability under the consumer protection laws since it may be subject to different interpretations by the consumer in different jurisdictions. Certain websites simply display advertisements or banners of other companies. In such a case, would the owner of the website be subject to liability for misleading or fraudulent advertisements that are displayed on its website? The website should contain appropriate disclaimers disclaiming any such liability. Most countries have stringent laws with respect to spamming. Website owners must ensure that they use legal methods of advertisements and that the method used does not amount to spamming.

3. Electronic Payment Issues

The instrumental growth in e-commerce activities has necessitated the evolution of electronic payment mechanisms. In addition to normal currencies, e-financial instruments / digital currencies such as cybercash[32] and e-cash[33] can be used for the purchase of current as well as capital assets over the Internet and for carrying on other commercial activities. Before regulating the use of such financial instruments, it would be essential to identify the issues that these instruments pose. Some of these issues are:

---

[30] FTC v Consumer Credit Advocates P.C., 96 Civ. 1990 cited from Richard D. Harroch, Esq. *Start-up and Emerging Companies: Planning, Financing, and Operating the Successful Business* (Vol 2 Revised Ed.).

[31] People v Lipsitz, IA, P.8, (N.Y. Sup. June 24, 1997) cited from Richard D. Harroch, Esq. *Start-up and Emerging Companies: Planning, Financing, and Operating the Successful Business* (Vol 2 Revised Ed.) .

[32] CyberCash Inc created a system called CyberCash which permits secure transactions through complex routing transaction.

[33] DigiCash, a Netherlands based Company has formed an electronic payment system known as e-cash. The system involves purchasing 'units' or 'credits' from a bank to a particular value in a particular currency which can be used to trade on Internet. The seller of the goods can take e-cash units and either use it to buy some other goods on the Internet or redeem it at participating banks for its own country's currency. Mark Twain Bank in the US issues e-cash on Internet.

a. Secure Credit Card Transactions: An e-commerce website that accepts online credit card payments must ensure that it has adequate security measures to safeguard confidential customer data that is provided on the site. In the event that credit card numbers are leaked on the Internet, the website could be held liable for damages caused to the consumers.

b. Recognition of digital currencies: To be effective, existing laws would need to recognise the payment of digital currencies, as enforceable consideration against obligations undertaken by the other parties. Further, the extent to which these digital currencies are "valid tender" would also need to be examined. [34]

c. Determining the relevant jurisdiction: This would mean determining the relevant law that parties will be governed by in respect of electronic transactions (whether by the contract, or in its absence, by general principles of law). This may create problems, especially when the laws in Country A, where the company is registered permit electronic payment contracts, whereas the laws in Country B, where the consumer is located, do not regulate electronic payment contracts.

d. Risk of Regulatory Change: The regulatory environment for electronic payment is likely to change with technological innovations in modes of payment.[35] Therefore, any form of legislation made in this regard should be technologically neutral. Pursuant to the IT Act the Reserve Bank of India ("**RBI**"), in consultation with the National Payment Council is in the process of giving final touches to the draft of the Payment Systems Regulations Act. This proposed legislation will bring in all electronic fund transfers in the country, such as money orders, settlements at payment gateways, stock and commodity exchanges and clearing houses under the jurisdiction of the RBI.

e. Transaction risks: These include the liability for security failures in the system of transaction and the relevant standard of care for system security. [36]

f. Consumer-oriented risks: These include risks concerning privacy, consumer protection, money laundering, tax avoidance, online fraud and crime. [37]

g. Disabling IT Act: The IT Act does not apply to negotiable instruments which is likely to create problems in the growth of electronic payment mechanisms.

h. No virtual banks: The recently announced Internet Banking Guidelines in India, which stipulate that purely virtual banks on the Internet are not allowed, may be a hindrance in maximising the potential of the Internet for electronic payments. However, existing banks are not prevented from setting up e-commerce operations for their customers.

[34] Simon Pollard, "Electronic Payment Systems: The Legal Perspective".
[35] Simon Pollard, "Electronic Payment Systems: The Legal Perspective".
[36] Simon Pollard, "Electronic Payment Systems: The Legal Perspective".
[37] Simon Pollard, "Electronic Payment Systems: The Legal Perspective".

4. Foreign Direct Investment

In the recent past, the Indian Government has considerably liberalised foreign direct investment ("**FDI**") in India. As per the regulations formed under the Foreign Exchange Management Act, 1999, ("**FEMA**") FDI is allowed on an automatic basis, (i.e. without any prior approval of the Ministry of Commerce and Industry) upto a certain limit or fully, in most sectors. In July 2000, vide Press Note No. 7 (2000 Series), the Government has also allowed 100% FDI in e-commerce activities. However, this investment is subject to the following conditions:

i. FDI is allowed only in companies engaged in B2B e-commerce activities and not in retail trading; and
ii. 26% of the FDI has to be divested in favour of the Indian public within a period of five years, if the companies are listed in other parts of the world.

Therefore, companies engaged in B2C e-commerce activities cannot obtain FDI on an automatic basis. They would have to seek prior approvals from the Foreign Investment Promotion Board under the Ministry of Commerce and Industry, which would consider such applications on a case-to-case basis.

5. Corporate Structure and Funding

Like in every other business, an important issue that needs to be addressed is the nature of the entity most suited to the business to be undertaken on the Internet. Establishing an e-business entails a host of decisions to be taken in structuring how the business should be organised, how the members will share the company's interests and the rights and liabilities of each party. Additionally, while structuring the business, one should also evaluate the need to set -up entities in different nations, if the business is to be conducted in different nations. Such an entity may be set up as branch office, liaison office or a representative office. The pros and cons of each such entity also entails a decision making process. For example, a branch office would be entitled to carry on certain activities, whereas a liaison office cannot undertake commercial operations on behalf of the Company.

a. Structure: The first step would be to determine whether the start-up company should be a partnership firm, a private company or a public company. The pros and cons of each structure should be evaluated in relation to the nature of business to be conducted.

(i) *Partnership Firm:* A partnership firm may be formed under the provisions of the Indian Partnership Act, 1932. This structure offers maximum flexibility in structuring economic participation by the founders and investors, as the members of the firm can dispose of the property and incur any liability within the scope of the business. This flexibility facilitates quick decisions. However, since a partnership firm is not a separate legal entity from its members, the partners may be personally liable for any loss that may occur. Additionally, the partnership firm cannot make a public offering and the partners

incur personal liability for any loss that may occur.

(ii) *Private Company:* A private company may be incorporated under the provisions of the Companies Act, 1956 ("**Companies Act**") with a minimum paid-up capital of Rs.1,00,000.[38] One of the main advantages of a private company is that the shareholders can restrict the transfer of shares.[39] This provides the shareholders with greater control on the affairs of the company. However, the liability of the shareholders in a private company is limited to the extent of their share in the company. Also, the company is prohibited from making an invitation to the public for shares or debentures.[40]

(iii) *Public Company:* A public company may be incorporated with a minimum paid-up capital of Rs. 5,00,000 under the provisions of the Companies Act.[41] A public company may make an offering of shares to the public. Also, the liability of the shareholders is limited to the extent of their share in the company. However, the shareholders cannot place restrictions on the right to transfer of shares.

b. Financing: There is relatively a higher degree of flexibility in terms of investment in a private company or a partnership firm, as the members can take quick decisions with respect to the amount and manner of investment to be made in the company. A public company, on the other hand, is required to follow the relevant procedures as detailed in the Companies Act. In the event that foreign equity participation or investment is proposed to be made in the company, the provisions of the Foreign Exchange Management Act, 1999 in this regard would have to be complied with as discussed in the "**Foreign Direct Investment**" issues.

c. Contractual relationships: The company or firm would need to enter into appropriate contractual relationships which would govern the rights, liabilities, manner of investments to be made etc. The contractual arrangements should set forth the shareholding of the promoters, strategic investors and lenders, as the case may be. The rights such as veto rights *etc.,* obligations, amount of profits of the promoter need to be specifically provided for. The agreements should also determine the stage at which the strategic investor can make investments in the company and the rights of such an investor. A lender to the company is usually granted a right under the agreement to nominate a person to act as a director on the Board of the company. Such agreements also lay out the clauses on the manner in which profits would be distributed, the grounds on which the parties may terminate the agreements etc.

Having discussed the various legal issues that an in e-commerce company must bear in mind, we have provided two imaginary case studies to see how various issues may emerge in specific situations. The first case study is industry-specific and relates to issues that may come up in case of an e-commerce bank. The second case study is transaction-specific and deals with problems that may crop up in a webcasting transaction.

[38] Section 3 (1)(iii) of the Companies Act.
[39] Section 3(1)(iii)(a) of the Companies Act.
[40] Section 3(1)(iii)(c) of the Companies Act.
[41] Section 3(1)(iv) of the Companies Act.

IV. CASE STUDIES

CASE STUDY 1: BANKING INDUSTRY

Newbank was established in 1952 in Mumbai, India under the provisions of the banking Regulation Act, 1949, with a branch in USA. The bank offers services in retail banking, investment banking and NRI services. The bank would like to set up a wholly owned subsidiary in India to offer Internet banking facilities to its customers.

However, various legal, technological and operational issues with respect to Internet banking would need to be addressed by the bank in this regard.

a. Regulatory issues:

Only banks that are licensed under the Banking Regulation Act, 1949 are permitted to offer Internet banking services. Under the Internet Banking Guidelines ("**Guidelines**") issued by the RBI on June, 14, 2001, virtual banks and banks incorporated outside India and having no physical presence in India are currently not permitted to offer Internet banking products and services to residents of India. Therefore, Newbank is not permitted to establish a virtual bank. It may however set up a division within the existing bank, which could offer Internet services to the customers of Newbank in India. Newbank will have to approach the RBI, as per the Guidelines, to obtain approval for offering Internet banking services in India. As per the Guidelines, Newbank can offer its services only to account holders in India and not in other jurisdictions. Additionally, these services and products can be offered only in local currency.

b. Legal compliances:

Currently, the legal framework for banking in India is provided in the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1934 and the FEMA. In addition to the provisions of these Acts, the Newbank would have to comply with the Guidelines.

c. Security and privacy issues:

As per the Guidelines, the banks are under an obligation to maintain secrecy and confidentiality of the customer's account. In the Internet banking scenario, the risks of banks in this respect is higher on account of several factors like the customers not being careful about their passwords, PIN and other personal identification details, the bank's website being hacked despite all precautions. Newbank should ensure that it has adequate security measures such as firewalls, secured socket layer to ensure authentication, 128-bit encryption and other net security devices. It should also enter into contractual relationships with the customers, services providers and the employees of the bank to limit their liability that may arise due to breach of security and confidentiality of the information of the customers of the bank.

It is mandatory for the bank to make the customer aware of the risks, responsibilities and

liabilities of doing business on the Internet, through a disclosure template.

d. Operational Risks:

Operational risk is one the most common issues in Internet banking. These issues arise due to inaccurate processing of transactions, non-enforceability of contracts, intrusion in the bank's systems *etc.* To safeguard against such risks, Newbank would have to strengthen the design, implementation and monitoring of the bank's information systems. In the event that the bank uses a service provider that is located in a country other than India, it would be difficult to monitor it, thus causing operational risks.

e. Money Laundering issues:

The Report of the Working Group on Internet Banking discussed the issues of money laundering that could arise due to the very nature of Internet transactions. The Working Group was of the view that since Internet banking transactions can be conducted from remote locations, the bank may find it difficult to detect criminal activities. The Guidelines impose an obligation on the bank to verify the credibility of the customer before opening an account. Therefore, Newbank would have to guard against the risk of being exposed to money laundering, which may result in legal sanctions for non-compliance with "know your customer" laws.

f. Cross-border issues:

With respect to cross-border transactions where banking services are offered by Indian banks to foreign residents and where Indian residents are offered services by foreign banks, the RBI has clarified that existing restrictions would continue to apply except where permitted by the FEMA. Therefore, Newbank would have to ensure that the services offered to the Non Resident Indians comply with the restrictions as detailed in the FEMA. However, overseas branches of Indian banks are permitted to offer Internet banking services to the overseas customers subject to their satisfying, in addition to the host supervisor, the home supervisor. Therefore, the US branch of Newbank should restrict its services only to the US customers.

Further, the legal requirements differ from country to country. This could expose the banks to legal risks associated with non-compliance with foreign law, including consumer protection laws, privacy rules and money laundering rules.

g. Hyperlinking:

Hyperlinking from a bank's website, also raises issues of reputational risk. Such links should not mislead the customers in to believing that they sponsor any particular product or any business unrelated to banking. Newbank would have to ensure that such hyperlinking from its website is confined to only those portals with which it has a payment arrangement, in addition to other security measures. In addition, it should also display the terms of the contract prominently on the website and should clearly get an acceptance from the customer before proceeding with any part of the transaction.

CASE STUDY 2: WEBCASTING

Filmiduniya.com, a web-portal ("**Portal**") webcasts Hindi films on the Internet. The Portal has gained tremendous popularity and receives about 100,000 hits per day.

A distribution agent, Mr. X, who owns the distribution rights in a Bollywood blockbuster approaches the Portal to exhibit the film on the Internet.

At the time of entering into the agreement, the Portal considers the following issues:

a. The Portal determines that the Censor Board as per the provisions of the Cinematograph Act, 1952, has certified the film.
b. The Portal determines that the first owners of the film have assigned Mr. X the rights in the film. The Portal also determines the rights of the first owners of the film.
c. The time period for which the rights have been assigned is determined at five years from the date of signing the assignment agreement.

After the Portal procures the rights to webcast the film, it charges a viewership fee of Rs. 100 for the film from each consumer. At the time of paying the viewership fee, the consumers have to register by reading and accepting certain terms and conditions and filling in certain personal details. One of the details relates to the type of Hindi films that they like. This helps the Portal in marketing new films to potential customers.

One day, the Portal receives notices from three parties:

a. Mr. A, a foreign citizen, who claims that he has paid Rs. 100 to view the film, but the film was not webcast. He wants a refund of his money, or a chance to view the film on another occasion. He also complains that he periodically receives e-mails from the Portal regarding their forthcoming webcasts and he finds these emails to be a nuisance. He asks the Portal to discontinue sending these unsolicited e-mails.
b. Mr. B, who is a foreign citizen and who states that the content of the film is against the national interests of his country. He serves a notice upon the Portal to stop webcasting the film, failing which he would be forced to take legal action.
c. StarBollywood Pvt. Ltd., who claims that the film is exactly similar to another film which it has produced and therefore has infringed its copyrights. It seeks to restrain the Portal from showing the film and also sues the Portal for copyright infringement.

Let us discuss what could be the possible conclusions to the above three issues:

a. The first instance deals with the contractual relationship between Mr. A and the Portal. As mentioned earlier, at the time of registering, Mr. A would have accepted the terms and conditions and is therefore, as per the law of contracts, would be bound by them. The terms and conditions that Mr. A has accepted may or may not make the Portal liable. If the terms provide immunity to the Portal from a failure to webcast a film under certain circumstances, the Portal could disclaim any liability. But if the terms and conditions are silent regarding the same, the Portal may be liable, as the object of the contractual relationship is to webcast the film and provide the consumer with an

opportunity to the view the film. In the latter case, the Portal may have to refund the money or provide Mr. A the right to see the film on another occasion.

With respect to the spam e-mails, once the Portal has been asked to stop sending the e-mails, it would be the duty of the Portal to cease this activity. Even though there may not be any privacy policy, nor does any Indian law make such activity objectionable, Mr. A's country may have certain laws protecting his privacy rights. In that case, Mr. A may be able to sue the Portal for violating his privacy right, if the courts in Mr. A's country establish jurisdiction over the Portal.

b. In the second instance, the Portal may have to discontinue webcasting the film to nationals of Mr. B's country or the Telecommunications Authority in Mr. B's country may block the access to the Portal. The Portal may also face penal consequences depending upon the laws of Mr. B's country. Alternatively, the Portal may put adequate disclaimers that warn future consumers of the content of the film. However, the effectiveness of disclaimers in rebutting any form of liability is debatable.

c. In the event that StarBollywood can successfully prove a case of infringement, the Portal may be restricted from webcasting the film. This is because, if the film which is being webcasted, is an infringement of another film, then the first owner of the film would be an infringer and have no legal right over the film. In that event, if the first owner has no good title on the film, the distributor and in turn the Portal would not get a good title on the film. In that case the Portal could be restrained from webcasting the film, but may be sued for infringement of copyrights. The Portal could however be entitled to claim damages from the distributor of the first owner for misrepresentation.

[This space is left blank intentionally]

V. CONCLUSION

The bursting of the dotcom bubble has made several companies realise that doing business on the Internet is not as easy at it sounds. Undoubtedly, the power of the Internet to reach any part of the world holds tremendous potential for enhancing international trade and boosting global economy. However, just as every coin has a flip side, we have seen that doing business on the Internet also has risks and legal issues associated with it.

The rapid pace of e-commerce development has generally left the legal system struggling to keep up and gasping for breath. In much the same way as companies doing e-commerce must invent new business procedures and rules, the legal system is trying to adapt existing laws to fit new settings where it is simply unclear how these laws will apply. In the midst of this legal turmoil, India is one of the few countries across the globe that has enacted an e-commerce legislation. However, much more is needed to effectively regulate the tangled web.

Effective risk management strategies coupled with adequate legal documentation will go a long way in protecting e-commerce companies. As someone had rightly said, though the Internet is a goldmine, without adequate legal protection it could become a landmine.

[This space is left blank intentionally]