NIRMA UNIVERSITY INSTITUTE OF LAW

DISSERTATION

INSTITUTE OF LAW, NIRMA UNIVERSITY, AHMEDABAD AS A PARTIAL FULFILLMENT OF REQUIREMENT FOR THE DEGREE OF MASTER OF LAWS (LL.M)

TOPIC: Defamation On Internet: Comparative Study Of India, United States & United Kingdom

UNDER THE GUIDANCE OF

Prof. NK Indrayan

SUMBITTED BY:

Mr.Chitrajeet Upadhyaya:

20ml004

DECLARATION

I, Chitrajeet Upadhyaya, bearing Roll No.20ml004, do hereby declare that the dissertation submitted is original and is the outcome of the independent investigations/ research carried out by me and contains no plagiarism. The dissertation is leading to the discovery of new facts/ techniques/ correlation of scientific facts already known. This work has not been submitted to any other University or body in quest of a degree, diploma or any other kind of academic award.

I do hereby further declare that the text, diagrams or any other material taken from other sources including [but not limited to books, journals and web] have been acknowledged, referred and cited to the best of my knowledge and understanding.

Date: 30.07.2021

Name: Chitrajeet Upadhyaya
Roll no. : 20ml004
Course: Constitution Law
Institute of Law
Nirma University

CERTIFICATE

This is to certify that the dissertation entitled "**Defamation On Internet: Comparative Study Of India, United States & United Kingdom**" has been prepared by Chitrajeet Upadhyaya under my supervision and guidance. The dissertation is carried out by her after careful research and investigation. The work of the dissertation is of the standard expected of a candidate for Master of Laws [LLM] in Constitutional Law and I recommend it be sent for evaluation.

Date:

Prof. NK Indrayan
ASSOCIATE PROFESSOR
INSTITUTE OF LAW,
NIRMA UNIVERSITY,
AHMEDABAD

ACKNOWLEDGMENT

This is a heartfelt Acknowledgement to all those who have helped me in successful Completion of this Dissertation.

First, I am thankful to Nirma University for giving me such a great chance to work on such emerging issue in the legal field. I am thankful to Prof. NK Indrayan, Associate Professor, Institute of Law, Nirma University for providing me such opportunity to be part of this Master of Laws [LLM] programme. I am thankful Prof. NK Indrayan who have guided me throughout the dissertation.

Further I am thankful to the librarian, Institute of Law, Nirma University for her constant support. Lastly I would like to express my gratitude to all those who have actively or passively aided in the successful completion of this Dissertation.

Date:

Name: Chitrajeet Upadhyaya
Roll No. 20ml004
Course: Constitutional Law
Institute of law
Nirma University

TABLE OF CONTENTS

OBJECTIVE OF THE STUDY

- To understand the problem of Defamation on the Internet
- To understand the case laws related to defamation in different countries.
- To know the liability of Inter Service Provider.
- To decide on the jurisdictional issues associated with the Internet, with a focus on defamation as it arises on the Internet.
- To point out the need of a comprehensive legislation

HYPOTHESIS

- There are instances of defamation via internet which crosses border.
- There is conflict as to which law will be applicable with respect to Jurisdiction, Prosecution & different charges against the defendant who is a foreign national.
- There is high unwillingness amongst the defendant to submit to foreign jurisdiction and foreign laws.
- The legal remedy for this kind of defamation is indeed complex and the courts are also perplexed as to applicability of laws.
- The defendants have find it easier to escape liability in such issues.
- There is no uniformity of law as different countries have applied different laws. The need of the hour is to overhaul the existing loopholes in law and apply standard set of laws uniformly across nations of the globe.
- Most of the cases have been reported from USA and India, whose analysis will make it clear to understand the modern legal trends to such issues.

Research Methodology

- In this research paper the method of doctrine research has been used.
- The data used in this research is collected from primary sources such as,
    - Bare acts, judgments, laws and other
- The most of the data used in this research is collected from secondary sources such as,
    - Publications of central, state and local governments
    - Books, magazines and newspapers

    Reports and journals prepared by research scholars, universities in the said field.

LIST OF CASES

1. *Dow Jones & Company, Inc v Gutnick* [2002] HCA 56.
2. *Reno v ACLU*, 117 S.Ct. 2329, 2334-35 (1997).
3. *Shevill v. Press Alliance S.A,* (C68/93) European Court of Justice.
4. Berezovsky v. Michaels [2000] 1 W.L.R. 1004 (H.L.).
5. New York Times v. Sullivan, 376 U.S. 254 (1964).
6. *Gertz v. Robert Welch Inc.*, 418 U.S. 323 (1974).
7. Tolstoy Miloslavsky v. United Kingdom, 20 EHRR 442 (1995),
8. *Dennis v. Salvation Army Grace General Hospital Board"* (1997), 156 N.S.R. (2d) 372 (C.A.)
9. Spilada Maritime Corporation v. Cansulex Ltd. 1 AC 460. [1987].
10. Pennoyer v. Neff, 95 U.S. 714 (1877).
11. Revell v. Lidov, no. 01-10521 (5th Cir., 2002).
12. Calder v. Jones, 465 U.S. 783 (1984).
13. Vladimir Matusevitch v. Vladimir Ivanovich Telnikoff, 1995 U.S. 702 A.2d 230 (1997).
14. TELCO Communications v. An Apple A day, 977 F. Supp. 404 (E.D. Va. 1997).

15. Zippo Mfg. Co. v. Zippo Dot Com, 952 F. Supp. 1119 (W.D. Pa. 1997).

16. Lane v. Applegate , (1815) 1 Stark 49.

17. George Firth v. State of New York, NY Int. 88 (2002).

18. Playboy Enterprises v. Chuckleberry., 1996 US Dist LEXIS 8435.

19. Young v. New Haven Advocate, 2002 US App. LEXIS 25535 (4th Cir.).

20. Govindacharylulu v Srinivasa Rao, AIR 1941 Mad 860.

21. Narayanan v Mahendra, AIR 1957 Nag 19.

22. *Lunney v. Prodigy* , 94 N.Y.2d 242 (1999).

CHAPTER 1: INTRODUCTION

The *definition* of the Internet is a largely uncontroversial matter. In technical terms, the Internet is essentially "a decentralised, self-maintained telecommunications network."[1] There is, however, nothing ordinary about the *benefits* associated with such a telecommunications network. The Internet provides its users with a previously unprecedented ability to communicate. E-mail provides virtually instantaneous global messaging, and information published on the world-wide-web (a subset of the Internet) is viewable and *usable*[2] upon creation, by any person with a connection to the Internet.[3] In becoming a medium used by hundreds of millions of people[4], the Internet has become an essential tool for commerce.[5] The U.S. Supreme Court provided its impressions of the Internet in 1997, labelling the Internet "a unique medium – known to its users as 'cyberspace' – located in no particular geographical location but available to anyone, anywhere in the world."[6] This description provides but a glimpse of the jurisdictional problems that have arisen as a result of the emergence of such a "revolutionary"[7] medium.

The Internet is a cheap, fast means of international communication of text, sound or image. In other words, an information resource without political or content boundaries; limited only by the extent to which the information providers are willing to disclose their materials and the fruits of their own writing and research. In the present day, web sites displaying information of all kinds are proliferating. These sites are established and controlled by Internet Service Providers (ISPs) or, sometimes, by the company's information technology

---

[1] *Dow Jones & Company, Inc v Gutnick* [2002] HCA 56, para 80. The proceedings in the High Court of Australia will hereafter be called "*Dow Jones v Gutnick*". General reference to the proceedings (including the 22 decision of first instance, the Court of Appeal decision, and the High Court's decision) will hereafter be "*Gutnick*". The full citation for the decision of first instance will be provided where relevant.

[2] 'Usable' means the Internet has the ability to interact with its users. Interaction is an important concept in relation to jurisdiction. See, in particular, section 3(e) below.

[3] The Internet does not require proprietary software for access. Any software platform (including Windows, Macintosh and UNIX) that can 'understand' Internet protocols can establish a connection to the Internet.

[4] United Nations Conference on Trade and Development, *E-Commerce and Development Report, 2002: Executive Summary* (2002) 1.

[5] Ibid

[6] *Reno v ACLU*, 117 S.Ct. 2329, 2334-35 (1997).

[7] "It is indeed a revolutionary leap in the distribution of information … It is a medium that overwhelmingly benefits humanity, advancing as it does the human right of access to information and to free expression." *Dow Jones v Gutnick*, para 164.

department. These sites can be accessed through suitable search engines, which will trace and display information to suit the requirements of the searcher. It is to be remembered that a number of features unique to the internet distinguishes it from any other medium. These features have led to the current re-examination of existing laws relating to defamation, to allow for their possible evolution and ultimately their application in cyberspace. A key feature of the internet is its highly interactive nature. The ease with which users of the internet can access information and communicate with each other has engendered in its users a false sense of freedom in their communications. Accessibility is another feature of the internet, which distinguishes it from traditional print or broadcast media. The relatively low cost of connecting to the internet and even of establishing one's own website means that the opportunity for defamation has increased exponentially. Now, on the internet everyone can be a publisher and can be sued as a publisher. Another key feature of the internet is that users do not have to reveal their true identity in order to send e-mail or post messages on bulletin boards. Users are able to communicate and make such postings anonymously or under assumed names. This feature, coupled with the ability to access the internet in privacy and seclusion of one's own home or office and the interactive, responsive nature of communications on the internet, has resulted in users being far less inhibited about the contents of their messages resulting in cyber space becoming excessively prone to defamation.

Defamation can be understood as the intentional infringement of another person's right to his good name. It is the wrongful and intentional publication of words or behaviour concerning another person, which has the effect of injuring that person's status, good name, or reputation in society. Libel is written defamation and slander is oral defamation. The primary difference is that in libel, damages are presumed, whereas in slander actions, unless the slander falls into a certain category, called slander per se, the plaintiff must prove actual or quantifiable damages. A person's good name can only be damaged if maligning statements are made to someone other than that person; that is, the defamatory statement must be disclosed to a third person, thereby satisfying the requirement of publication. When determining whether or not defamation has taken place, the only issue to consider is whether a person of ordinary intelligence in society would believe that the words would indeed injure the person's reputation.

Thus the law of defamation places a heavy burden on the defendant. All that a plaintiff has to prove, in a defamation action, is the publication of defamatory matter. The onus then lies on the defendant to prove innocence. Once again, most people are unaware of this burden. In essence, the law on defamation attempts to create a workable balance between two equally important human rights: The right to an unimpaired reputation and the right to freedom of expression. In a cyber society, both these interests are increasingly important. Protection of reputation is arguably even more important in a highly technological society, since one may not even encounter an individual or organization other than through the medium of the internet.

The elements of a defamation action can be summarized as follows:

- The plaintiff must prove publication of the defamatory statement;
- The plaintiff must prove that the defamation refers to the plaintiff; and
- The plaintiff must prove that the statement is defamatory.

Upon proof of publication, the law makes several presumptions in favour of the plaintiff:

- That the statement is false;
- That it was published with malice; and
- That in the case of libel or slander per se, the plaintiff has suffered damage.

Defences that can be raised against such a defamation action are as follows:

- Truth.
- Fair comment: The defendant is allowed to comment on facts truly stated, as long as the comment is fair and the defendant is not motivated by actual malice.

- Privilege: On certain occasions, the courts have held that policy and convenience require that a person should be free from responsibility for the publication of defamatory words. These occasions constitute privileges. Privilege may be absolute, such as statements in the House of Commons or the Courts. It may be qualified,

in that it may be lost if the publication is unnecessarily wide or made with malice.

- Innocent dissemination: This last defence is potentially very important in cyber libel.

If a defendant proves that his statements were true and in public interest, then his conduct is regarded as lawful. In addition, if the defendant can show that he had no intention to defame (the plaintiff), then he could avoid liability.

CHAPTER 2: DEFAMATION CASES

The ever increasing importance of the internet has countless legal ramifications. Among them, the internet raises problems of jurisdiction in defamation cases. Plaintiffs seek jurisdictions where the burden of proof for defamation and damages is comparably low while website owners seek jurisdictions that minimize their legal liability. It will often be advantageous for plaintiffs to file internet defamation suits in the United Kingdom when possible because of the structure of United Kingdom defamation laws.

The internet transcends frontiers. It allows a person to publish simultaneously in many countries at low cost. A person can gain reputation over the internet. A person can have reputation harmed over the internet, which raises problems of jurisdiction in defamation cases. In this article, I will analyze what the alternatives of jurisdiction and choice of law are in cases in which defamation through the internet involves more than one state. I will conclude that the United Kingdom is preferable to the United States when considering jurisdiction for plaintiffs in cases of internet defamation. A modern case involving defamation over the internet is the Dontdatehimgirl.com case. Dontdatehimgirl.com is a website where users post warnings on men who are unfaithful.[8] Users upload pictures, write descriptions, and describe how they were wronged, which can significantly diminish the reputation of the men involved. A lawyer from Pittsburgh sued dontdatehimgirl.com for defamation in Pennsylvania because one poster stated that he had a sexually transmitted

[8] Lizette Alvarez, *(Name here) is a liar and a cheat,* N.Y. TIMES, February 16, 2006, *available at* http://select.nytimes.com/gst/abstract.html?res=F60E1EFD385A0C758DDDAB0894 DE404482, (last visited July 29, 2010).

disease,[9] dated two women at the same time, and was bisexual or gay. In April 2007 the case was dismissed for lack of personal jurisdiction over the website's owner, a Florida resident.[10]

The Terms of Use at Dontdatehimgirl.com have the following clause: IT reads as following : **8. JURISDICTION**. This Web site is hosted on servers located in the United States and is intended to be viewed by residents of the United States. In the event of any dispute arising out of or relating to this site, you agree that the exclusive venue for litigating disputes shall be in state or federal court in Miami, Florida.[11] Despite these Terms of Use, I argue that it would be to a plaintiff's advantage to sue Dontdatehimgirl.com for defamation in the United Kingdom, if someone accessed this website in the United Kingdom and if the plantiff suffered damage to his or her reputation within the United Kingdom.

Assuming a plaintiff could sue in any jurisdiction he chose, there are several reasons why he would benefit from suing in the United Kingdom, rather than the United States.

A. DEFAMATION CASES IN THE UNITED KINGDOM

London is considered to be "the libel capital of the world."[12] In the United Kingdom, the test used to determine if a statement is defamatory is whether the statement lowers "the claimant in the estimation of rightthinking people generally."[13] There has to be a false statement that damages a person's reputation. A defamatory statement is one that impugns another person's reputation or adversely affects his or her standing in the community.[14]

---

[9] Moustafa Ayad, *City lawyer sues 'don't date him' Web site*, PITTSBURGH POST-GAZETTE, June 30, 2006, *available at* http://www.post-gazette.com/pg/06181/702314-51.stm, (last visited July 29, 2006); Carl Jones, *Scorned Attorney Sues Kiss-and-Tell Web Site*, DAILY BUSINESS REVIEW, July 5, 2006, *available at* http://www.law.com/jsp/article.jsp?id=1151658319991, (last visited July 29, 2006).

[10] Joe Mandak, *Judge Tosses Date-Dissing Web Suit*, ASSOCIATED PRESS, April 11, 2007, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2007/04/10/financial/f141020D38.DTL, (last visited December 8, 2007). On Novermber 29, 2007 a second lawsuit was filed in a federal court in Florida. David Ardia, , *Hollis v. Cunningham,* Citizen Media Law Project, December 7, 2007 http://www.citmedialaw.org/threats/hollis-v-cunningham (last visited December 8, 2007).

[11] *Terms of Use*, *available at* http://dontdatehimgirl.com/terms.html, (last visited July 29, 2010).

[12] Geoffrey Robertson & Andrew Nicol, *Media Law* 71 (Penguin Books 2002).

[13] *Id.* at 79.

[14] Mark Lunney & Ken Oliphant, *Tort Law*. Text and Materials 581 (Oxford University Press 2000).

Moreover, United Kingdom libel law is biased towards the plaintiff. There is a presumption of falsehood of the statement unless the defendant proves its truth: "defamatory statement is actionable without proof of its falsity, but the defendant has a complete defence of justification if he or she succeeds in demonstrating its truth; the publication of true statements, whether or not it is in the public interest, cannot generally amount to defamation."[15] Other pro-plaintiff features of English libel law are: (a) each communication is treated as a separate libel,[16] (b) publication occurs where the words are heard or read,[17] and (c) the damage is presumed.[18] The test for jurisdiction is that the tort committed must be real and substantial.[19] Given these characteristics, a plaintiff would find it advantageous to attempt to sue Dontdatehimgirl.com in the United Kingdom, as opposed to the United States, if possible, and many foreign plaintiffs do indeed choose to sue in the United Kingdom.[20]

In the United Kingdom, there is double actionability for defamation. The claimant can choose to sue at the place of distribution or where the loss of reputation occurred, but only for the reputation lost in that jurisdiction. This was established in *Shevill v. Press Alliance S.A.*,[21] when a French newspaper published that Fiona Shevill was involved in money laundering for a drug-trafficking network. The newspaper was mainly distributed in France and had minor circulation in the United Kingdom, with 230 copies sold in England and Wales, and only 5 in Yorkshire. The Court held that: On a proper construction of the expression *"place where the harmful event occurred"* the victim of a libel by a newspaper article distributed in several Contracting States may bring an action for damages against the publisher either before the courts of the Contracting State of the place where the publisher of the defamatory publication is established, which have jurisdiction to award

---

[15] *Id.*

[16] Duke of Brunswick v. Harmer, 14 Q.B. 185 (1849); McLean v. David Syme & Co. Ltd., 92 W.N. (N.S.W.) 611 (1970), "The originator of a defamatory statement may be held liable for its foreseeable repetition by a third party." Also see *Slipper v. British Broadcasting Corporation* 1Q.B. 283 (1991), for application to an internet defamation on a newspaper archive. See Loutchansky v. The Times Newspapers Ltd. & Ors EWCA Civ 1805 (2001).

[17] Bata v. Bata, W.N. 366 (1948); Lee v. Wilson and Mackinnon, 51 C.L.R. 276 (1934).

[18] Ratcliffe v. Evans, 2 Q.B. 524, 529 (1892), Bowen L. J. This presumption was eliminated in the United States by *Gertz v. Welch* 418 U.S. 323 (1974). See also *Kroch v. Rossell* 1 All E.R. 725 (1937).

[19] Berezovsky v. Michaels [2000] W.L.R. 1004 (H.L.).

[20] For example, see Berezovsky v. Michaels [2000] 1 W.L.R. 1004 (H.L.); King v. Lewis [2004] E.W.C.A. (Civ. 1329). In both of these cases, Americans sued for defamation in the United Kingdom, despite having no apparent ties to the UK.

[21] (C68/93) European Court of Justice (hereinafter ECJ), March 7, 1995.

damages for all the harm caused by the defamation, or before the courts of each Contracting State in which the publication was distributed and where the victim claims to have suffered injury to his reputation, which have jurisdiction to rule solely in respect of the harm caused in the State of the court seised. The fact that under the national law applicable to the main proceedings damage is presumed in libel actions, so that the plaintiff does not have to adduce evidence of the existence and extent of that damage, does not therefore preclude the application of Article 5(3) of the Convention.[22]

The *Shevill v. Press Alliance S.A.* case established that there is jurisdiction for defamation in both France, the place of publication, and in the United Kingdom, the place of loss of reputation.

Given all of these advantages, when there is damage to a person's reputation in the United Kingdom, there are incentives to sue for defamation in the United Kingdom. Some examples of this practice are presented below, including *Berezovsky v. Michaels*, which describes a similar situation to *Shevill v. Press Alliance S.A.*, but includes an internet component.

In 1996, Forbes Magazine published an article which referred to Mr. Berezovsky, a Russian citizen, as: *"the Godfather of the Kremlin? Power, Politics, Murder. Boris Berezovsky can teach the guys in Sicily a thing or two."*[23] This magazine had most of its circulation in the United States (785,710 copies), some in the United Kingdom (1,915 copies), and almost none in Russia (13 copies). Forbes Magazine was also available on the internet. Mr. Berezovsky claimed to have "extensive personal and business connections with England."[24] However, Forbes argued that the United States and Russia were more appropriate forums. The judge ruled that the case had more connection with Russia and dismissed the action, but the decision was appealed. The court of appeal stated that there was jurisdiction in the United Kingdom to continue the trial. Forbes appealed to the House of Lords. Mr.

[22] Shevill v. Press Alliance S.A., (C68/93) ECJ, March 7, 19 erezovsky v. Michaels [2000] 1 W.L.R. 1004 (H.L.).
[23] Berezovsky v. Michaels [2000] 1 W.L.R. 1004 (H.L.).
[24] *Id.*

Berezovsky countered that he had "extensive contacts with England" and "worked frequently in London and with persons and companies based in London."[25]

The House of Lords concluded that England was the best place for the suit. It dismissed Russia and the United States on the following grounds: The first is that only 19 copies were distributed in Russia. Secondly, and most importantly, on the evidence adduced by Forbes about the judicial system in Russia, it is clear that a judgment in favour of the plaintiffs in Russia will not be seen to redress the damage to the reputations of the plaintiffs in England. Russia cannot therefore realistically be treated as an appropriate forum where the ends of justice can be achieved. In the alternative counsel for Forbes argued that the United States is a more appropriate jurisdiction for the trial of the action. There was a large distribution of the magazine in the United States. It is a jurisdiction where libel actions can be effectively and justly tried. On the other hand, the connections of both plaintiffs with the United States are minimal. They cannot realistically claim to have reputations which need protection in the United States. It is therefore not an appropriate forum.[26]

The subject of the availability on the internet of the magazine, however, was deemed not an issue in the case:

"During the course of interesting arguments it became clear that there is not the necessary evidence before the House to consider this important issue satisfactorily. Having come to a clear conclusion without reference to the availability of the article on the Internet it is unnecessary to discuss it in this case."[27]

[25] *Id.*
[26] *Id.*
[27] *Id.*

The *Berezovsky v. Michaels* case was a closest connection case, determining that there was a closer connection with the United Kingdom than either the United States, the place of publication, or Russia, Mr. Berezovsky's home country. The *Berezovsky v. Michaels* case relates to the internet defamation predicament because it established that country of citizenship is not the relevant question – it does not matter that the plaintiff is from the United States, as it did not matter that Mr. Berezovsky's country of citizenship was Russia. The relevant question here was where the loss of reputation occurred. Therefore, despite Clause 8 of Dontdatehimgirl.com's Terms of Use, a plaintiff could theoretically sue the website in the United Kingdom, despite his residency in the United States and the website servers' location in the United States.

Although the *Berezovsky v. Michaels* case established that country of citizenship is not the relevant question, a connection still needs to exist with the United Kingdom before a person can sue for defamation in that forum, as clearly illustrated in the *King v. Lewis* case. Mr. King has a worldwide reputation in the boxing business. He is a citizen of the United States and lives in Florida, but was involved in a case in New York. The opposing counsel, Mr. Burstein, wrote an article on two websites, fightnews.com and boxingtalk.com, calling Mr. King an anti-Semite. Mr. King chose to sue in London. After citing *Berezovsky v. Michaels*, the court stated:

Thus the starting-point for the ascertainment of what is clearly the most appropriate forum is to identify the place where the tort has been committed. That will, of course, by definition be England in a defamation case where leave to serve out has been obtained on the basis of publication here. But – and here is our second proposition from the cases – the more tenuous the claimant's connection with this jurisdiction (and the more substantial any publication abroad), the weaker this consideration becomes.

In these circumstances there is in our judgment no basis on which this court could properly be invited to ascertain the appropriate *forum* for itself, and for all the reasons we have given the appeal will be dismissed.[28] In the quote above, the judge ruled that Mr. King would not be

[28] King v. Lewis [2004] E.W.C.A. (Civ. 1329).

permitted to sue Mr. Burstein and Mr. Lewis in the United Kingdom because Mr. King's case, despite Mr. King's worldwide reputation in the boxing industry, did not have a strong enough connection to the United Kingdom for jurisdiction in that forum. Mr. King, apparently aware of the many advantages of suing for defamation in the United Kingdom, was ultimately unable to do so, due to a lack of connection there.

Up until now, I have discussed: the *Shevill v. Press Alliance S.A.* case, which covered the place of readership versus the place of publication; the *Berezovsky v. Michaels* case, which considered Mr. Berezovsky's significant connection to the forum; and the *King v. Lewis* case, which examined Mr. King's lack of significant connection to the forum. The next case I will discuss is *Jameel v. Dow Jones*, which also covers defamation over the internet.

The Wall Street Journal (WSJ) Online, owned by Dow Jones & Co., Inc., published an article in which Mr. Jameel, a citizen of Saudi Arabia, was mentioned as a donor of Al Qaeda in the WSJ's "Golden Chain" list. In this case, Mr. Jameel wanted his name removed from being associated with Al Qaeda, in part because the United States' Department of Justice was using this list to investigate people who gave funds to Al Qaeda. The judge ruled, however, that:

Where a defamatory statement has received insignificant publication in this jurisdiction, but there is a threat or a real risk of wider publication, there may well be justification for pursuing proceedings in order to obtain an injunction against republication of the libel. We are not persuaded that such justification exists in the present case. There seems no likelihood that Dow Jones will repeat their article in the form in which it was originally published. It has been removed from the web site and from the archive. If they do publish further material about the Golden Chain list, it is likely to be by way of reports about litigation in which the list features, or statements made about the list by the United States Government or other authorities. It is quite impossible to predict whether any such future publication will be protected by privilege, or calculated to cause significant damage to the claimant's reputation. In these circumstances, if this litigation were to proceed and to culminate in judgment for the claimant, it seems to us unlikely that the court would be able, or prepared, to

formulate and impose an injunction against repetition of the defamation in terms that would be of value to the claimant.[29]

The judge made two significant considerations about this case. First, the judge determined that access to the WSJ's publication online, from the United Kingdom, was not significant enough to establish jurisdiction for defamation in the United Kingdom. Second, there was a low risk of

republication of the "Golden Chain" list by the WSJ Online. Therefore, the judge dismissed Mr. Jameel's case. In the preceding cases about jurisdiction for defamation in the United Kingdom, I have discussed how several plaintiffs have attempted to sue for defamation in the United Kingdom, due to the many advantages that plaintiffs enjoy when suing for defamation in that forum. Relating these cases to the internet defamation predicament, it seems clear that a plaintiff

would benefit from suing Dontdatehimgirl.com in the United Kingdom, if he could establish jurisdiction there. However, if a plaintiff had no connection with the United Kingdom and could not establish jurisdiction there, then he might be resigned to sue in the United States. That would be unfortunate for the plaintiff because there are more limitations imposed on defamation cases in the United States than there are in the United Kingdom.

B. DEFAMATION CASES IN THE UNITED STATES

In the United States, it is relatively difficult for a plaintiff to obtain compensation for defamation.

The Uniform Single Publication Act, adopted by most states,[30] provides that:

No person shall have more than one cause of action for damages for libel, slander, invasion of privacy or any other tort founded upon a single publication, exhibition or utterance, such as any one edition of a newspaper, book or magazine, any one presentation to an audience, any one broadcast over radio or television or any one

[29] *Id.*

[30] See *Dow Jones & Company Inc. v. Gutnick (2002), HCA 56 (provides that "[s]ome 27.* States of the United States, including California, Illinois, New York, Pennsylvania and Texas" have adopted §577A of the Restatement of Torts, 2d (1977)).

exhibition of a motion picture. Recovery in any action shall include all damages for any such tort suffered by the plaintiff in all jurisdictions.[31]

The Uniform Single Publication Act also prevents the reiteration of action:

"A judgment in any jurisdiction for or against the plaintiff upon the substantive merits of any action for damages founded upon a single publication, exhibition or utterance as described in subsection A shall bar any other action for damages by the same plaintiff against the same defendant founded upon the same publication, exhibition or utterance."[32]

In other words, if a person is defamed via most publication methods, then that person can sue for all damage that he or she received from all jurisdictions - but from within only one jurisdiction. For example, suppose Mr. King was defamed by an opinion article in USA Today, which has

worldwide publication. Mr. King could sue USA Today for damage he received to his reputation worldwide. However, he could only do so in one particular state. Also, all acts of defamation - if they occurred via one opinion article - count as one collective act of defamation, rather than

counting each individual newspaper printed that carried the opinion article. The Uniform Single Publication Act has significant implications for this case. Whereas United Kingdom law states that "each communication is treated as a separate libel," the Uniform Single Publication Act lumps together all publications at once. Based on this comparison, a plaintiff could potentially sue in the United Kingdom for defamation every time the Dontdatehimgirl.com website is accessed with defamatory information about him, whereas, in the United States, it is arguable that under the Uniform Single Publication Act only the single act of posting the defamatory information on the host server is libelous.

[31] Restatement Second on Torts §577A (1977), William L. Prosser, *Interstate publication*, 51 Michigan L. Rev. 959 (1953). 25 *Id.*

[32] Id.

The Uniform Single Publication Act was applied to a website in *Firth v. State of New York*.[33] However, it did not designate a particular jurisdiction and, therefore, did not prevent forum shopping.[34] Thus, if Mr. King chose to sue for defamation in the United States, he could choose to sue in New York, California, or any other state where he felt he could obtain sufficient jurisdiction.

In Stratton Oakmount v. Prodigy (1995), the US Supreme Court provided no incentive for online service providers to remove obscene or libelous material from their databases. If any good faith attempt were made to inspect content prior to publication, the online service provider risked liability for any offensive material it missed. This case led to the enactment of the Telecommunications Act of 1996, and was effectively overruled by the said Act.

This Act was signed into law by President Clinton On February 8, 1996, and includes the Communications Decency Act ("CDA")and the Internet Freedom and Family Empowerment Act. The Act recognizes the value of the internet, and declares that the internet has "flourished, to the benefit of all Americans, with a minimum of Government regulation."

Historically, the posture of the United States on defamation is affected by several factors. To begin with, the First Amendment of the Constitution provides strong protection for freedom of expression. Two notable cases, *New York Times v. Sullivan*[35] and *Gertz v. Robert Welch Inc.*,[36] have also established that politicians and public persons receive less protection from defamatory statements, because clear and convincing evidence of actual malice is the standard required for defamation in those cases, a contrast expressed by Justice Eady in *Harrods v. Dow Jones*.[37]

Justice Eady's ruling on the *Harrods v. Dow Jones* case highlights an important difference between the priorities of the United States and the United Kingdom regarding defamation, a person's reputation, and freedom of expression. His ruling established that the priority in

---

[33] George Firth v. State of New York, NY Int. 88 (2002), which holds the opposite from *Duke of Brunswick v. Harmer*: "Thus, a multiple publication rule would implicate an even greater potential for endless retriggering of the statute of limitations, multiplicity of suits and harassment of defendants. Inevitably, there would be a serious inhibitory effect on the open, pervasive dissemination of information and ideas over the internet, which is, of course, its greatest beneficial promise." … "Republication, retriggering the period of limitations, occurs upon a separate aggregate publication from the original, on a different occasion, which is not merely a delayed circulation of the original edition." Rinaldi v. Viking Penguin, Inc., 52 NY 2d at 435.

[34] Restatement of Torts §577A 2d (1977); Berezovsky v. Michaels .

[35] 376 U.S. 254 (1964).

[36] 418 U.S. 323 (1974).

[37] Harrods Ltd. v. Dow Jones & Co. Inc. [2003] (E.W.H.C.) 1162 (Q.B.).

the United Kingdom is to protect and vindicate a defamed person's reputation more than to protect freedom of speech. Thus, plaintiffs suing in the United Kingdom have more rights than in the United States, as Justice Eady also alluded to a judge in New York, implying that in the United States, granting freedom of expression is generally considered to be a higher priority than vindicating the reputation of a defamed person. Not only does the United Kingdom require less evidence than the United States for defamation cases, but also the damages awarded are usually higher.[38] Faced with these incentives, a plaintiff would certainly want to sue in the United Kingdom if he could establish jurisdiction there. The next logical question is whether a plaintiff can establish jurisdiction in that forum.

CHAPTER III: JURISDICTION ON THE INTERNET

Before I examine whether a plaintiff could reasonably sue Dontdatehimgirl.com for defamation in the United Kingdom, I will discuss the concept of jurisdiction on the internet. Jurisdiction can be classified into three types: jurisdiction to prescribe, jurisdiction to adjudicate, and jurisdiction to enforce.[39] In this section, I will focus primarily on the jurisdiction to prescribe and adjudicate. Jurisdiction must be justified by the court exercising it. Jurisdiction is usually based on the principle of territoriality, nationality, effects doctrine, or the protection of national security and interests. The classically accepted principles are territoriality and nationality. However, for defamation cases,[40] the effects doctrine is widely used.

The internet is an international context. Several authors have attempted to apply the aforementioned principles to internet cases in order to justify jurisdiction. Now, I will examine the application of the principles of territoriality and nationality to internet cases.

---

[38] Tolstoy Miloslavsky v. United Kingdom, 20 EHRR 442 (1995), John v. MGN Ltd, 2 All ER 35 (1996). However, the costs may be higher too. Geoffrey Robertson & Andrew Nicol, *Media Law* 76 (Penguin Books 2002).

[39] Restatement (Third) of Foreign Relations Law of the United States § 401 (1987).

[40] And torts in general are guided by the lex loci delicti commssi principle.

One approach of the territoriality doctrine leads to applying the law of the server where the website is stored.[41] That was Dow Jones' contention in Gutnick v. Dow Jones.[42] The court recounted:

"the principal burden of the argument advanced by Dow Jones on the hearing of the appeal in this Court was that articles published on Barron's Online were published in South Brunswick, New Jersey, when they became available on the servers which it maintained at that place."

Using the law of the server would be arbitrary, because the server can be located in a place that has no connection to either the uploader or the downloader. Furthermore, the place of the server will be chosen by the uploader, usually in a country with laws favourable to the owner's

interests.[43] In relating this case to the Dontdatehimgirl.com case, it seems feasible to assume that many servers which contain defamatory statements might be arbitrarily placed in locations with relatively weak connections to either the uploader or the downloader, but which provide greater legal protections for the owner of the website that contains defamatory comments. The law of

the server may explain why Dontdatehimgirl.com's Terms of Use has Clause 8, which again states:

"This Web site is hosted on servers located in the United States and is intended to be viewed by residents of the United States. In the event of any dispute arising out of or relating to this site, you agree that the exclusive venue for litigating disputes shall be in state or federal court in Miami, Florida".[44]

Since the laws governing protection from defamation are relatively weaker in the United States than the United Kingdom, it is arguable that the owner of Dontdatehimgirl.com is attempting to use the law of the server to establish jurisdiction in the United States, in order to avoid being sued for defamation in the United Kingdom, where it is easier to

[41] This can be difficult when a website is stored on more than one server, and when there are mirror websites.
[42] Gutnick v. Dow Jones & Co. Inc.[2002] H.C.A. 56 (H.C. (Aus.)), settled in 2004.
[43] Id.
[44] *Terms of Use,* supra note 4

prove defamation and the penalties are higher, as stated in Section 2 of this article. Another common principle used in conflicts of law is nationality. With nationality, one question is whose nationality should be used to determine jurisdiction: the owner of the server, the author of the website, or the user.

According to Daniel Menthe, nationality should be the principle used to determine jurisdiction in cyberspace. To arrive to this conclusion, he postulated that the internet is an international space. Then he postulated that in the law of the flag of a ship, Antarctica and outer space, which are

international spaces, jurisdiction is determined by the law of nationality. Therefore, he concluded that the nationality of the creator or the person, on whose behalf a website is maintained, should determine the jurisdiction.[45] The internet would appear to be an international space like the high seas, which makes Menthe's theory intuitively attractive. A website can be owned by a company that was created in a country with favourable laws, like a ship displaying a flag of convenience in international waters. If the creator of a website is a company, the principle of nationality may allow it to choose a more convenient jurisdiction. Although the territoriality and nationality principles are significant in defamation cases, the prevailing principle is the effects doctrine: the act occurred where the effects took place. The place of publication is the place of the tort, lex loci delicti. On the internet, the effects of defamation can easily occur in multiple countries simultaneously, which makes it difficult to determine jurisdiction and applicable law, while preventing forum shopping.[46]

As with the case of *Berezovsky v. Michaels*, Mr. Berezovsky was able to demonstrate jurisdiction in the United Kingdom via the effects doctrine, which is present in the United Kingdom law of jurisdiction for torts.

A. JURISDICTION IN THE UNITED KINGDOM

[45] Darrel C. Menthe, *Jurisdiction in Cyberspace: A Theory of International Spaces,* 4 Mich. Telecomm. Tech. L. Rev. 69 (1998).

[46] Forum shopping has been defined as trying to have an "action tried in a particular court or jurisdiction where [the litigant] feels he will receive the most favorable judgement or verdict." Bryan A. Garner, editor in chief, Black's Law Dictionary, abridged (8th ed, St. Paul, MN: Thomson/West, 2005). The line between legitimately choosing a forum and forum shopping is blurry. See *Forum Shopping Reconsidered,* Notes, 103 Harvard Law Review, 7 1677-96 (May, 1990).

In the United Kingdom, defamation is excluded from the Private International Law (Miscellaneous Provisions) Act 1995, which provides that "the applicable law is the law of the country in which the events constituting the tort or delict in question occur," unless there is a more significant connection with another country.[47] Therefore, common law rules still apply to defamation conflict of laws. However article 5(3) of the Brussels Convention states that "in matters relating to tort, delict or quasidelict, in the courts for the place where the harmful event occurred." In *Shevill v. Press Alliance S.A.*,[48] the place where the harmful event occurred was interpreted as either at the place of distribution or at the place where the loss of reputation occurred, with the latter as a more plausible standard for internet cases.

Cheshire and North, in Private International Law, proposed a solution for cases of multi-state defamation:

There is a strong argument for adopting a different rule for multi-state defamation from that applicable in more straightforward cases involving publication in just one country. This could take the form of a special rule defining the place of the tort, not in terms of publication, but in terms of where the claimant suffered the most injury to reputation.

More radically, the concept of the place of the tort could be abandoned altogether and replaced in cases of multi-state defamation by a rule applying one of the following:

(i) the law of the claimant's domicile or residence;

(ii) the law of the country which, with respect to the particular issue, has the most significant relationship with the occurrence and with the parties.[49]

At first, Cheshire and North appeared to propose the application of the effects doctrine – applying the law of the country in which the reputation was harmed the most. This approach is consistent with the one adopted in in Shevill *v. Press Alliance S.A.*:[50] the plaintiff can choose between the place of publication or the main place of loss of reputation. As

[47] Private International Law (Miscellaneous Provisions) Act, 42 HL, § 11-13 (1995)
[48] (C68/93) ECJ, March 7, 1995.
[49] Peter North & J.J. Fawcett, Cheshire and North's Private International Law, (Butterworths, Thirteenth Ed, 1999) pg. 660.
[50] (C68/93) ECJ, March 7, 1995

both are essential parts of the tort, they are encompassed in the lex loci delicti principle. The principal place of loss of reputation is nearer to the effects doctrine, without abandoning the lex loci delicti principle. Then, proposing more radical approaches, they proposed the law of the claimant's domicile or residence in

(i). This seems to presuppose that the claimant had most of his or her reputation at the place of his or her domicile or residence, which may not always be true, especially with internet cases, since reputation can be built over the internet.

Option **(ii)** appears to be more equitable.[51] If a case has more points of attachment with a specific country, then the parties and the action must be related to that country, which provides more discretion to judges.[52]

Multiple points of attachment can arise from a defamation case. These can include: the place of first publication, the place of predominant publication, the place of defendant's act, the place of defendant's incorporation, the defendant's principal place of business, the plaintiff's domicile, the plaintiff's principal place of business, the forum, and the state having the largest group of these contacts.[53]

I will now analyze these points of connection. The place of first publication has the same problems as the territoriality principle: it can be chosen by the publisher and is difficult to determine on the internet.[54] The place of the defendant's act refers to the place of publication and would suffer from the same problems. The place of predominant publication is more appropriate, because it points to the place where readers were sought.[55] It is safe to assume that a person would suffer more injury to their reputation in a place

---

[51] Option (ii) is also more intuitive because this is the principle that is often used in contract conflicts of law. See Rome Convention article 4, Restatement (Second) of Conflict of Laws § 188 (1971).

[52] This can be seen as either an advantage or a disadvantage. Some do not believe such judicial discretion should exist. See Dworkin Ronald, Taking Rights Seriously, (Ed: 7th impression. Publisher: London, Duckworth, 1994, c1977). On the other hand, legal realists believe in ample judicial discretion. "The prophecies of what the courts will do in fact, and nothing more pretentious, are what I mean by the law." Oliver Wendell Holmes, Jr., The Path of the Law, 10 Harvard Law Review 457 (1897). An economic analysis of judicial discretion can be found in: Richard S. Higgins & Paul H. Rubin, *Judicial Discretion*, 9 The Journal of Legal Studies, 1 129-38 (January, 1980).

[53] Loid G. Forer, *The Choice of Law in Multistate Defamation: A Functional Approach*, . 77 Harv. L. Rev., 8 1463-84 (June, 1964);,(W. Norton and Co., New York, 1987), pg. 314.

[54] du Pont , George F., *The Time Has Come for Limited Liability for Operators of True Anonimity Remailers in Cyberspace: An Examination of the Possibilities and Perils, 6* J. Tech. L. & Pol'y, 175 (Fall 2001)

[55] This is the approach taken in *Schapira v. Ahronson* EMLR 753[1999] : "Where the tort of libel is allegedly committed in England against a person resident or carrying on business in England by foreigners who were aware that their publication would be sent to subscribers in England, that English resident is entitled to bring proceedings here against those foreigners."

with more readers than a place with less, as long as that person had a reputation to protect there. This approach also assumes that there was a place of predominant publication. On the internet, there is sometimes an intention to pursue readers in a determinate country or region, and sometimes there is not. Clearly, an online edition of a local newspaper is aimed at local readers. Websites with country-specific editions aim at a definite readership as well. Language editions are less clear. The English edition of dontdatehimgirl.com is frequented by users from the United States, the United Kingdom, Canada, Australia, and non- English speaking countries. Additionally, websites that do not specify a readership may or may not have a predominant place of publication, perhaps aiming at international readers with a certain interest. In these cases, the point of attachment of predominant place of publication may not be the most valid point of connection in internet defamation cases. Other points of attachment can be arbitrary as well. Specifically, the place of defendant's incorporation, the defendant's principal place of business, the plaintiff's domicile, and the plaintiff's principal place of business are arbitrary. One could assume that the plaintiff has more of his or her reputation at the place of his or her domicile or principal place of business. However, it is reasonable to consider a person with a worldwide reputation on the internet. A store on eBay,[56] multinational companies, and a frequent poster on a forum are examples of those whose reputations acquired on the internet may be harmed irrespective of domicile or principal place of business. For example, in the case of Bangoura v. Washington Post,[57] Mr. Bangoura was dismissed from his job at the United Nations as a result of an article published by the *Washington Post*. At the time the suit was filed, Mr. Bangoura resided in Ontario, Canada. However, the court stated that:

The connection between Ontario and Mr. Bangoura's claim is minimal at best. In fact, there was no connection with Ontario until more than three years after the publication of the articles in question. Mere residence in the jurisdiction does not constitute a sufficient basis for assuming jurisdiction. See V. Black, "Territorial Jurisdiction Based on the Plaintiff's Residence: *Dennis v. Salvation Army Grace General Hospital Board"* (1997), 14 C.P.C. (4th) 207 at p. 232, 156 N.S.R. (2d) 372 (C.A.), where the author writes: Permitting a plaintiff to

[56] eBay even has a system to measure online reputations with stars, which makes the loss more tangible.
[57] Bangoura v. Washington Post (Unreported, September 16, 2005) (CA (Ont)) at http://www.ontariocourts.on.ca/decisions/2005/september/C41379.htm (last accessed August 18, 2010).

assume a new residence and sue a defendant there in respect of events that occurred elsewhere seems to be harsh to defendants, and this is particularly so when those events comprise a completed tort.[58]

The court refused to accept that the story would follow Mr. Bangoura wherever he resided, illustrating how residence can be arbitrary as a point of attachment.Given the variety of possible circumstances, it is difficult to adhere to one point of attachment exclusively. Therefore, the closest connection[59] approach appears to be the most reasonable. It also appears to be the approach taken in most of the cases in the United Kingdom.[60] If a case has a closer connection with another country, but little connection to the United Kingdom, then a court in the United Kingdom should refuse to adjudicate that case, using the doctrine of forum non coveniens, if there is a forum that is clearly more appropriate for the resolution of that dispute.[61]

B. JURISDICTION IN THE UNITED STATES

Doctrines regarding internet defamation jurisdiction in the United States have evolved over time. Traditional jurisdiction in the United States requires in personam jurisdiction[62] or minimal contacts with the forum.[63] The minimal contacts test was used in an internet case in Zippo

Manufacturing Inc. v. Zippo Dot Com Inc.[64] The judge used a sliding scale to measure the level of activity in the state in question, concluding that: "If Dot Com had not wanted to

---

[58] *Id*

[59] The Rome Convention defines closest connection as "the law of the country with which it is most closely connected" (Art. 4.3). Art. 3 of the proposed Rome Convention for torts reads: "Unless otherwise provided for in this Regulation, the law applicable to a non-contractual obligation arising out of a tort or a delict shall be the law of the country with which the noncontractual obligation is most closely connected".

[60] Berezovsky v. Michaels [2000] 1 W.L.R. 1004 (H.L.); King v. Lewis [2004] E.W.C.A. (Civ. 1329); Jameel v. Dow Jones & Co Inc. [2005] E.W.C.A. (Civ. Div. 75).

[61] Spilada Maritime Corporation v. Cansulex Ltd. 1 AC 460. [1987].

[62] Pennoyer v. Neff, 95 U.S. 714 (1877).

[63] International Shoe v. Washington, 326 U.S. 310 (1945). "[...] to the extent that a corporation exercises the privilege of conducting activities within a state, it enjoys the benefits and protection of the laws of that state. The exercise of that privilege may give rise to obligations; and, so far as those obligations arise out of or are connected with the activities within the state, a procedure which requires the corporation to respond to a suit brought to enforce them can, in most instances, hardly be said to be undue."

[64] Zippo Manufacturing Inc. v. Zippo Dot Com Inc., 952 F. Supp 1119 (WD Pa (United States)) (1997).

be amenable to jurisdiction in Pennsylvania, the solution would have been simple - it could have chosen not to sell its services to Pennsylvania residents."[65] The sliding scale test was refined in *Young v. New Haven Advocate*[66] and *Revell v. Lidov*.[67]

The continuum of the scale was clarified in *Revell v. Lidov*:

A 'passive' website, one that merely allows the owner to post information on the internet, is at one end of the scale. It will not be sufficient to establish personal jurisdiction. At the other end are sites whose owners engage in repeated online contacts with forum residents over the internet, and in these cases personal jurisdiction may be proper. In between are those sites with some interactive elements, through which a site allows for bilateral information exchange with its visitors.[68]

The sliding scale focuses on the readership and customers sought by the website and the level of interaction with them. The judge at *Revell v. Lidov* sustained, as obiter dicta, that the Zippo scale was not in conflict with the effects doctrine.[69]

In the United States, the effects doctrine is used for defamation cases. In *Calder v. Jones*,[70] the National Enquirer had published that actress Shirley Jones was an alcoholic. The Supreme Court held that the California Court of Appeal had jurisdiction, even if the article was written and edited in Florida, because "intentional conduct in Florida calculated to cause injury to respondent in California." This principle was later tested on an internet defamation case, *Griffis v. Luban*,[71] when it was held that publishing on an internet newsgroup did not show intention of publishing

in Alabama. Therefore, the effects doctrine is not applied to internet defamation cases if the intention to publish in a specific place is not demonstrated.

---

[65] *Id*.

[66] Young v. New Haven Advocate, no. 01-2340 (4th Cir. 2002). "The newspapers' websites, as well as the articles in question, were aimed at a Connecticut audience. The newspapers did not post materials on the internet with the manifest intent of targeting Virginia readers. In sum, the newspapers do not have sufficient internet contacts with Virginia to permit the district court to exercise specific jurisdiction over them."

[67] Revell v. Lidov**,** no. 01-10521 (5th Cir., 2002).

[68] *Id*.

[69] *Id*.

[70] Calder v. Jones, 465 U.S. 783 (1984).

[71] Griffis v. Luban, no. C3-01-296 (Minn. 2002).

Some states use interest analysis to determine jurisdiction.[72] Interest analysis involves weighting the interests of each state in applying their own law. Brainerd Currie distinguishes between false conflicts, where the interests of all the states involved can be reconciled, and true conflicts, where the interests cannot be reconciled, and the law of the forum applies. With defamation, states can choose to protect either reputation or uphold freedom of expression. This is a matter of public policy in which states can have a clear policy. For example, in *Matusevitch v. Telnikoff*,[73] the court stated that, while freedom of expression is a public policy of the United States, this was a case between two British residents for an act that took place in England, and thus public policy did not apply to them. However, the court sustained that each case should be examined on its own facts to see if public policy was infringed.[74]

C. JURISDICTION IN INDIA

1. INTRODUCTION

With tremendous rise in the use of the internet as a medium of communication, chances of use of the web as a forum for publication of defamatory content has increased multifold and there is a need for a clear, coherent expression of the law in this area. While the need for a uniform law to govern internet transactions is undoubted, the question is whether the traditional law of defamation can be applied to the internet without any changes.

Defamation traditionally requires the proof of publication of a matter intentionally and with malice, thus lowering the reputation of a person in the eyes of right thinking people. In the context of the internet, the proof of these elements acquires new dimensions: determining the place of publication, establishing what constitutes a publication, ascertaining which country's law applies; and deciding whether an individual can be subject to the jurisdiction

[72] Brainerd Currie, *Notes on Methods and Objectives in the Conflict of Laws*, 2 Duke Law Journal, 1959 171-181 (Spring, 1959). In Zippo Manufacturing Inc. v. Zippo Dot Com Inc., it was held that "[t]here can be no question that Pennsylvania has a strong interest in adjudicating disputes involving the alleged infringement of trademarks owned by resident corporations." Zippo Manufacturing Inc. v. Zippo Dot Com Inc., 952 F. Supp 1119 (1997) (WD Pa (United States)).

[73] Vladimir Matusevitch v. Vladimir Ivanovich Telnikoff, 877 F. Supp. 1; 1995 U.S. 702 A.2d 230 (1997).

[74] Id.

of the court of another country based on a defamatory statement disseminated over the internet.[75]

The law of defamation requires a delicate balance between the right of persons not to be defamed and the right of others to engage in free speech.[76] This is harder to maintain in the case of the World Wide Web. Since internet allows transactions between persons of various jurisdictions, an international agreement (to be crystallised into a convention, later) is required for any regulation governing defamation over the internet.[77] However, in arriving at a uniform law, varying standards adopted by jurisdictions across the world and the point of balance adopted by them have to be kept in mind. The failings of domestic regulation were aptly demonstrated in Playboy Enterprises v. Chuckleberry.[78]

2. WHEN DOES PUBLICATION OCCUR ON THE INTERNET?

The traditional common-law rule is that defamation occurs where the matter is read and comprehended. In the case of internet publication occurs when the material is read by the reader, and the delivery of information occurs before comprehension by the reader. In many cases of internet defamation, users would have accessed the defamatory material only after they request it to be "pulled" from the server. While the article may have been placed by the defendant on the internet, but once a "pull" request is made, the defendant has no control over it.[79] Satellite signals are intentionally transmitted into some jurisdictions.[80] Unlike television, in case of internet, the requirement of intention to transmit to that particular jurisdiction, or at least a minimum contact with that jurisdiction is required to be proved.[81]

---

[75] Tara Blake Garfinkel, Jurisdiction Over Communication Torts: Can You Be Pulled into Another Country's Court System for Making a Defamatory Statement Over the Internet? A Comparison of English and US Law, 9 Transnat'l Law 489, 492.

[76] Bryan P. Werley, Aussie Rules: Universal Jurisdiction over Internet Defamation, 18 Temp. Int'l & Comp. L.J. 199, 219.

[77] Para 1.16 of the British Law Commission Report on Defamation and the Internet, cited from (visited on 7th August,2010)

[78] 1996 US Dist LEXIS 8435 (SDNY 19 June, 1996), cited from R. Matthan: The Law Relating to Computers & the Internet, p. 2 (New Delhi: Butterworths, 2000). In this case, the defendant was an Italian, who had, using an Italian server, set up a website, under the name "Playmen". The court had earlier issued a permanent injunction against the defendant from using that name in any magazine sold, published or distributed in USA. The court accepted that it could not order the website to be shut down as that would amount to asserting that every court in the world had jurisdiction over all information providers on the internet.

[79] Gutnick v. Dow Jones & Co. Inc., 2002 HCA 56, 73 Hereinafter Gutnick.

[80] No Bad Puns: A Different Approach to the Problem of Personal Jurisdiction on the Internet, 116 HARV. L. REV. 1821, 1821-22. (Hereinafter "No Bad Puns")

[81] Ibid. at pp. 1821-22.

3. TESTS FOR DETERMINING JURISDICTION

3.1 TOTALITY OF CONTACTS

In totality of contact analysis[82], the court gathers and weighs all online contacts that the defendant has with the forum, electronic or non-electronic, to determine whether sufficient minimal contacts exist to assert specific jurisdiction.[83] In Rubbercraft Corpn. of California v. Rubbercraft, Inc.,[84] the court, after explaining that a passive website alone is insufficient to convey jurisdiction in the forum, identified Rubbercraft's contacts like advertisement by web page and a nationally circulated periodical, operation of a web page and sales in the forum of about $20,000 in that year, as being sufficient to convey jurisdiction to the forum.

3.2 EFFECTS TEST

The effects test approach as enunciated in Calder v. Jones,[85] essentially inquires whether the forum State is the focal point of the defamatory story and the harm suffered. The inquiry requires an examination of whether the defaming party had the intent to cause injury in the forum or whether knowledge could be reasonably presumed that injury would be caused in the forum. In California Software, Inc. v. Reliability Research[86], the court explained that even if defendant did not send a tangible object into the forum or was not present in the forum, he is not at liberty to use the unique characteristics of internet technology to avoid jurisdiction. The test was further clarified in Young v. New Haven Advocate[87], where the court held that jurisdiction would be established if the publisher's intent was to reach the readers in the forum.

---

[82] B.J. Waldman, A Unified Approach to Cyber-Libel: Defamation on the Internet, A Suggested Approach, 6 RICH. J.L. & TECH. 9, 11.
[83] Supra note 6, at p. 1824.
[84] 1997 WL 835442 (C.D. Cal.).
[85] 465 US 783. In this case, the Court found jurisdiction to have been properly asserted in California when the libellous material was produced in Florida because the subject of the defendant's article was in California and it injured the plaintiff's reputation in California.
[86] 631 F. Supp. 1356 (C.D. Cal. 1986).
[87] 2002 US App. LEXIS 25535 (4th Cir.).

3.3 KEETON TEST

The Keeton test approach[88] transports a traditional multi-State defamation jurisdictional analysis into cyber-libel thus allowing exercise of jurisdiction where the defamatory statement is published and delivered to the forum.

In TELCO Communications v. An Apple A day[89], the court held that even though the evidence showed that the defendant had no other actual contacts with the forum apart from a defamatory statement on a passive website, it was subject to the exercise of jurisdiction. In Gutnick5 the High Court of Australia held that a court in Victoria could exercise jurisdiction over an American defendant who had defamed an Australian resident. While it is true that Gutnick5 is unlikely to have succeeded in the USA, where defamation laws are much less strict, the Court failed to recognise that such a decision may result in Australians being cut off from internet contents due to the fear of an unfriendly forum. The decision makes it necessary for internet publishers to have contemplated the defamation laws of all countries where there is a reasonable likelihood of access, especially if the laws are stricter than where the server is based. The alternative is to erect firewalls around countries where the person resides, so that residents there have no access to the site.

The Court recognised that the public interest in the free flow of information and opinion stands in broad opposition to the private interest in the security of reputation.[90] The problem arises when international disputes involve choice of law concerns between competing forums that strike different balances between these interests.[91] However, the broad approach of the Commonwealth countries, focussing on the harm caused to the plaintiff[92] is entirely at variance with the approach adopted by the American Courts.

3.4 NATURE OF THE WEBSITE OR ZIPPO APPROACH

---

[88] Laid down in Keeton v. Hustler Magazine, Inc., 465 US 770 (1984).

[89] 977 F. Supp. 404 (E.D. Va. 1997), cited from D.L. Kidd, Casting the Net: Another Confusing Analysis of Personal Jurisdiction and Internet Contacts in TELCO Communications v. An Apple A Day, 32 U.RICH.L.REV. 505, 509.

[90] Adrian Briggs, The Duke of Brunswick and Defamation by Internet, 119 Law Quarterly Review 119, 210-15

[91] B.P. Werley, Aussie Rules: Universal Jurisdiction over the Internet, 18 Temp.Int'l & Comp.L.J. 199, 219-20.

[92] Supra note 5, at p. 80; Berezovsky v. Michaels, (2000) 1 WLR 1004 (HL), at p. 1008.

A distinction relevant in law, but not addressed in the Gutnick case5, is the difference between paid and subscription sites. Moderators of paid sites have control over who accesses the site and its material. However, publication within a jurisdiction may nevertheless have occurred, despite the exercise of control, as the website may have been accessed by someone in the plaintiff's country who has a credit card registered in another country. In such a case, the requirement of intent to publish is not satisfied.

A fourth approach, embodied in Zippo Mfg. Co. v. Zippo Dot Com[93] contemplates that it is not sufficient to show that it is possible for someone to reach into cyberspace and bring the materials on to the screen in that particular jurisdiction ;there has to be evidence that the defendant used the internet for a commercial purpose to enter that particular jurisdiction.[94]

Where a defendant clearly does business over the internet, personal jurisdiction is proper. On the other hand, a passive website that does little more than make information available to those who are interested in it does not create grounds for the exercise of personal jurisdiction. The middle path is occupied by interactive websites where a user can exchange information with the host computer. Reasonableness of the forum depends on the level of interactivity and the commercial nature of the information exchanged. This is somewhat similar to the totality of contacts approach, but that approach takes into account electronic as well as non-electronic contacts with the forum, while only electronic contacts are considered here.

The Keeton approach has to be discounted altogether because of manifest unreasonableness. The Zippo approach and the totality of contacts approach are similar, but the Zippo approach should be considered to be superior, as it does not take extraneous factors such as non-electronic contact into account. However, in the absence of an international agreement, the effects approach seems to be the best.

[93] 952 F. Supp. 1119 (W.D. Pa. 1997).
[94] Braintech Inc. v. Kostiuk, (1999), 63 B.C.L. R 3d, 156 cited from www.lawsonlundell.com

CHAPTER IV: FRAMEWORK IN INDIA

Reputation is a jus in rem, a right absolute and against the world and a person's reputation is his/ her property. Thus, no one can defame a person i.e. use his freedom of speech or expression so as to injure another's reputation. The essence of defamation is its tendency to cause that description of pain which is felt by a person who knows himself to be the object of the unfavourable sentiments of his fellow- mates and those inconveniences to which a person who is the object of such unfavourable sentiments is exposed. In general, there are four requirements for liability for defamation to arise. A false and defamatory statement must be made about another's reputation or business. What is necessary in a case of defamation is that the statement made is understood by others to be "of or concerning" the plaintiff. If the individual who is the subject of defamation is deceased, no cause of action lies for defamation. The publication should be made out to a third party. Generally, there is no liability if the defendant did not intend the publication to be viewed by anyone other than the plaintiff. However, most defamatory material on the internet is accessible to millions worldwide. Therefore, it is unlikely that a defendant would be able to argue that he or she did not intend that others should view the statements. The plaintiff must establish some extent of fault or negligence on the part of the defendant in publishing the statements. Thus, a plaintiff who is a public figure will have to show that the statements were made out of malice. The burden of proof is less demanding in case of a private individual. The statements must result in actual or presumed damage. The permanent nature of libel coupled with the ability to distribute it widely especially through the internet have led courts to allow for recovering damages for libel without actually proving damage caused.

India is the only country which has both civil as well as criminal defamation in its legal books. That is another reason why rights of the people should clearly be laid down. People in India are liable for defamation not just to the extent of payment of damages but also undergoing imprisonment. Millions of people could be charged for defamation just by giving their opinion which in the eyes of some may be defamatory.

The problems for ISP's are just beginning. Some sites have already been blocked due to government directives. Bloggers in India are getting together to protest against the sudden blocking of popular Google-owned blog-hosting site Blogger by some (ISPs) like Spectranet, Mahanagar Telephone Nigam Limited (MTNL), Reliance Powersurfer, Airtel Broadband and Sify.

On July 15, the Department of Telecommunications (DoT) had sent ISPs a list of sites to be blocked. R H Sharma, senior engineer with MTNL, said the list ran into some 22 pages. Now, several bloggers have organized themselves into a Blogger's Collective and are planning to file a Right to Information application to obtain the list.

Under the Information Technology Act, 2000, a body called the Computer Emergency Response Team, or CERT-IN, was created along the lines of similar authorities the world over. Although its main task is in the domain of Internet security, it also oversees Internet censorship under a clause that seeks to ensure 'balanced flow of information.' Any government department seeking a block on any web site has to approach CERT-IN, which then instructs the DoT to block the site after confirming the authenticity of the complaint. In 2003, one of the first things CERT-IN did was to approve the blocking of an obscure mailing list run by a banned militant outfit, the Hynniewtrep National Liberation Council (HNLC) of the Khasi tribe in Meghalaya. Ironically, the popularity and visibility of the list went up by leaps and bounds, despite it being blocked by all ISPs. Many could still see the list via email or proxy surfing.

Whether such blocking is arbitrary, unreasonable and unfair and in violation of Articles 14, 19 and 21 of the Constitution of India is a question, which remains to be answered by the Indian Courts

IPC ON DEFAMATION:

Chapter XXI of the IPC exclusively talks of defamation. Section 499 prescribes the offence: "*Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said . . . to defame that person".*

EXPLANATION 2. - It may amount to defamation to make an imputation concerning a company or an association or collection of persons as such.

Section 500 prescribes the punishment in such cases:

"Whoever defames another shall be punished with simple imprisonment for a term, which may extend to two years, or with fine, or with both."

EMPLOYER'S LIABILITY

A company can be held liable for the conduct of its employees. If an employee, during working hours, e-mails a defamatory remark about a competitor company to a colleague, the firm could be held liable for defamation even if the employee's actions were not authorised or expressly prohibited.

For instance, in a dispute, which arose in the United Kingdom between the Western Provident Association (WPA) and Norwich Union, it was suggested that Norwich Union staff were spreading e-mail rumours amongst their sales force that WPA was more or less insolvent and under investigation by the Department of Trade and Industry. WPA sued Norwich Union, alleging that the latter was responsible for the communications made by its employees, even though the allegations were made without the instructions or knowledge of the management. The case was settled out of court but it is believed that Norwich Union paid approximately half a million pounds to WPA in settlement.

In fact, Asia's first case of cyber defamation has been filed in India in the case of SMC Numatics Ltd. v. Jogesh Kwatra . Defamatory emails were allegedly sent to the top management of SMC Numatics by the defendant, who has since been restrained by the

Delhi High Court from sending any form of communication to the plaintiff. This order of Delhi High Court assumes tremendous significance as this is for the first time that an Indian Court assumes jurisdiction in a matter concerning cyber defamation and grants an ex-parte injunction restraining the defendant from defaming the plaintiffs by sending derogatory, defamatory, abusive and obscene emails either to the plaintiffs or their subsidiaries.

An important test in determining whether a company can be held responsible for its employees' actions is to decide whether the actions were to the benefit of the company. An employer would be held vicariously liable in case of an employee promoting his own interests. The Australian judgment could impact freedom of speech of media organisations and expose publishers to legal actions all over the world. The judgment has raised complex global issues regarding internet publications, which could develop over time. The principle enunciated by the Australian Apex court is likely to stand in conflict with emerging jurisprudence relating to jurisdiction. Such an approach is likely to undermine the global nature of the internet, because it could make online publishers cautious and may deny access of their web sites to readers in countries where they fear litigation. This judgment will certainly have an impact on the Indian web publishing industry. It could open up the ground of misuse of law as Indian web publishers would be amenable to defamation laws not only in India but outside.

Further, the offence of defamation as defined in the IPC when extended to cyberspace may not achieve desired results. However, the Australian Judgment can be cited as a precedent and that will have persuasive value in India. Hence if defamatory material is downloaded by someone in India, that will be enough cause for action even if the servers of such site are located outside India.

THE INFORMATION TECHNOLOGY ACT, 2000

In May 2000, at the height of the dot-com boom, India enacted the IT Act and became part of a select group of countries to have put in place cyber laws. In all these years, despite the growing crime rate in the cyber world, only less than 25 cases have been registered under the IT Act 2000 and no final verdict has been passed in any of these

cases as they are now pending with various courts in the country. Although the law came into operation on October 17, 2000, it still has an element of mystery around it. Not only from the perception of the common man, but also from the perception of lawyers, law enforcing agencies and even the judiciary. The prime reason for this is the fact that the IT Act is a set of technical laws. Another major hurdle is the reluctance on the part of companies to report the instances of cyber crimes, as they don't want to get negative publicity or worse get entangled in legal proceedings. A major hurdle in cracking down on the perpetrators of cyber crimes such as hacking is the fact that most of them are not in India. The IT Act does give extra-territorial jurisdiction to law enforcement agencies, but such powers are largely inefficient. This is because India does not have reciprocity and extradition treaties with a large number of countries.

What India needs to do in this backdrop, is to be a part of the international momentum against cyber crimes. The only international treaty on this subject is the Council of Europe's Convention on Cyber Crime, formulated primarily by the European Union. By signing this treaty, member countries agree on a common platform for exchange of information relating to investigation, prosecution and the strategy against cyber crime, including exchange of cyber criminals. At the last count, there are 43 member countries, including the US and South Africa. India is not yet a part of this group and being a member would go a long way in addressing this issue of cross-border cyber terrorism.

The Indian IT Act also needs to evolve with the rapidly changing technology environment that breeds new forms of crimes and criminals. We are now beginning to see new categories and varieties of cyber crimes, which have not been addressed in the IT Act. This includes cyber stalking, cyber nuisance, cyber harassment, cyber defamation and the like. Though Section 67 of the Information Technology Act, 2000 provides for punishment to whoever transmits or publishes or causes to be published or transmitted, any material which is obscene in electronic form with imprisonment for a term which may extend to two years and with fine which may extend to twenty five thousand rupees on first convection and in the event of second may extend to five years and also with fine which may extend to fifty thousand rupees, it does not expressly talk of cyber defamation. The above provision chiefly aim at curbing the increasing number of child pornography cases and does not encompass

other crimes which could have been expressly brought within its ambit such as cyber defamation.

DEFENCES FOR DEFAMATION

Defamation is defined as "the publication of a statement which reflects on a person's reputation and tends to lower him in the estimation of right-thinking members of society generally or tends to make them shun or avoid him." The Indian Penal Code, 1860 defines defamation as the wrong done by a person to another's reputation by words, signs or visible representation (S. 499) . The aim of the law of defamation is to protect one's reputation, honour, integrity, character and dignity in the society. Defamation is both a crime and a civil wrong. An aggrieved person may file a criminal prosecution as well as a civil suit for damages for defamation.

There is no statutory law of defamation in India except the Chapter XXI (Section 499 -502) of the Indian Penal Code. As far as civil liability of defamation is concerned, it has been long settled in the country that an action for damages would lie in proper cases. A large number of artificial and technical rules have grown around this branch of law in England. Though courts in India are not bound by them however, the dicta may be helpful in that they can be applied to Indian cases as principles of equity, justice and good conscience. Under common law there are some general defenses available to all torts like consent, apology, accord, limitation and previous judgments. Another defence, 'Secondary Responsibility which was earlier embedded in the defence of 'innocent disseminators' is also being discussed.

ACCORD –

Accord signifies the presence of assent from the plaintiff. In Lane v. Applegate[95] the defendant burnt libelous papers on plaintiffs agreeing not to sue if that was done. The court held that as there was a prior accord from the plaintiff he could now not claim for damages.

[95] (1815) 1 Stark 49

APOLOGY –

An apology is not under the common law, a defence to an action for defamation but it is only a circumstance in mitigation of defences. However, in England under the Libel Act of 1943 this defence is available under certain circumstances. For example- Apology is available as a defence in actions for libel against newspapers and other periodical publications if the newspaper inserts a sufficient apology and adheres to certain other conditions. When there is an apology and an acceptance there of the defendant can resist the plaintiff's suit for reimbursement for defamation. Nevertheless, there has been no similar legislation in India. In past judgments the court has held that even if the plaintiff accepted an apology and withdrew a criminal prosecution for defamation he can still sue the defendant in a civil suit Govindacharylulu v Srinivasa Rao[96] This ratio was reiterated in Narayanan v Mahendra[97].

CONSENT –

As observed by Salmond if the plaintiff has expressly or impliedly consented to the publication complained of or if it had invited the defendant to repeat those words before witness the defendant can use this defence. If a person telephones a newspaper with false information about himself, he would not be able to sue in defamation when the newspaper publishes it.

LIMITATION –

In India, the right to take legal action for defamation is restricted in accordance with the Limitation Act, 1963 to a period of one year. (Section 75 and Section 76 of the Limitation Act limit the period of filing a suit for compensation of libel and slander respectively to one year).

SPECIALIZED DEFENCE TO DEFAMATION

- Justification by Truth
- Fair (and bona fide) Comment
- Privilege (which may be either absolute or qualified)

JUSTIFICATION BY TRUTH

[96] AIR 1941 Mad 860.
[97] AIR 1957 Nag 19

In a defamation suit it is not required from the claimant to prove the falsity of the statement for the reason that the law assumes that in his favour. Nevertheless the defendant can plead justification (the technical expression for truth). Truth of defamatory expression is an absolute defence in a civil action. The law has recognized this defence for the reason that since defamation is essentially an injury to a man's reputation, when it is shown that what is spoken of person is true it means only that his reputation has been brought down to its proper level and there is no reason for him to complain. M'Pherson v. Daniels (1829 10 B & C 263) embodies this principle commenting that "the law will not permit a man to recover damages in respect to an injury to a character which he either does not or ought not to possess." The motive or maliciousness is immaterial to the extent the charges are correct. It would make no difference in law that the defendant had made a defamatory statement devoid of any belief in its truth, if it turned out afterwards to be true when made. Whenever this plea of justification is raised by a defendant the burden is cast upon him to prove that precise imputation complained of. If the words impute a definite offence, e.g. stealing a watch, it is not enough to prove that the plaintiff was guilty of another offence though of the same character, e.g. stealing a sunglass. According to the rules of common law in case of multiple and distinct charges, each charge must be proved to be true to avail the defence. This rule has somewhat been amended and relaxed. If the defendant is successful in proving the truth regarding some of the charges only, the defence of justification will still be available if the charges not proved do not materially injure the reputation. The defendant must show that the imputation made or repeated by him was true as a whole and in every part thereof. The defendant need not show that the charge he seeks to justify is precisely true in every particular: what matters is whether it is substantially true. If the statement is to a large extent true but false in certain minor aspects, the protection will still be accessible. But if there is gross exaggeration, the plea of justification will fail. In Gulf Oil v Page (1988 Ch. 327) it has been held that the Fourth Estate is authorized a degree of overstatement or exaggeration even in the context of factual assertions.

Where the words complained of add up to specific statements of a fact, for example, the plaintiff stole a car from the defendant's premises, it is adequate to plead that the said words are true. On the other hand if, the words convey a general charge, for example the

plaintiff is a swindler or pickpocket, it is not adequate to plead merely that the said words are true, but the defendant must give particulars of facts on which the charge is based and plead that those facts are true. In a case of innuendo, the defendant must plead the truth of the words both in the natural and alleged hidden meaning. In criminal law truth is not an absolute justification. It can only be availed if it is shown that the publication was for public benefit or public good. In accordance to the Exception 1 of Section 499 of the Indian Penal Code (It is not defamation to impute anything which is true concerning any person, if it be for the public good that the imputation should be made or published. Whether or not it is for public good is a question of fact.), it is not enough that the words complained of are true, the defendant must then be prepared to go further and prove that not only are the words true, but that it is also for the public benefit that they should be published.

Before proving the case of defamation guidelines mentioned in Panday Surinder Nath Sinha v. Bageshwari Prasad, case can be considered. Where distinction between absolute and qualified privilege was brought out as under:

(i) In absolute privilege, it is the occasion which is privileged and when once the nature of the occasion is shown, it follows, as a necessary inference, that every communication on that occasion is protected; in qualified privilege, the occasion is not privileged, until the defendant has shown how that occasion was used. It is not enough to have an interest or a duty in making a statement the necessity of the existence of an interest of duty in making the statement complained of, must also be shown.

(ii) In absolute privilege, the defendant gets absolute exemption from liability; in a qualified privilege, the defendant gets a conditional exemption from liability.

(iii) In absolute privilege, the defendant is exempted from liability even when there is malice on his part; in qualified privilege, the defendant is exempted from liability only when there is no malice on his part.

(iv) In absolute privilege, statements are protected in all circumstances, irrespective of the presence of good or bad motives; in qualified privilege, even after a case of qualified privilege has been established by the defendant, it may be met by the plaintiff proving in reply improper or evil motive on the part of the defendant, in which case defense of qualified privilege vanishes and the plaintiff succeeds; and

(v) In absolute privilege as well as in qualified privilege, the defendant has to prove his plea of privilege, but with this difference that in absolute privilege the

defense is absolute and irrefutable by plaintiff, whereas in qualified privilege the defense is not absolute but reputable by the plaintiff.

ABSOLUTE PRIVILEGE

In matters of absolute privilege, no action lies for the defamatory statement even though the statement is false or has been made maliciously. In these cases, the public interest demands that the individual's right to reputation should give way to the freedom of speech. Absolute privilege is recognized in the case of parliamentary proceedings, judicial proceedings, State communications and Military and Naval Proceedings. Thus statements made by an officer of the state to another in course of official duty are absolutely privileged for reasons of public policy. An absolute privilege extends to statement and words used in the proceedings which have relevance to the matter before the court. These words should not cross the limits of relevance. In Pukhraj v State of Rajasthan[98] it was held that the words (sale, gunde, badmash) and actions (kicking the plaintiff) of postal authorities had no link to the discharge of their duties. An action for defamation therefore was valid.

QUALIFIED PRIVILEGES

A privileged occasion in reference to a qualified privilege is when a person who makes a communication has an interest or a duty – legal, social or moral – to make it to the person to whom it is made has a corresponding interest or duty to receive it. The test for this defence is requirement of public interest. In certain cases the speaker is prevented if there is absence of malice. In Radheshyam Tiwari v Eknath[99] the defendant who was the editor of a local Marathi Weekly published a series of articles mentioning that the plaintiff, who was a BDO, issued false certificates, accepted bribe, adopted corrupt and illegal means to mint money and was a 'Mischief Monger'. In an action for defamation, the defendant pleaded all three defences. The defence of Justification was discarded as truth of facts mentioned could not be proved. The defence of Fair Comment was not accessible because

[98] 1973 SCC (Cri) 944
[99] AIR 1985 Bom 285

there was a statement of fact, rather than an expression of opinion. The defence of qualified privileges could also be not availed because the publications were mala fide.

CHAPTER V: LIABILITY OF INTERNET SERVICE PROVIDERS

The law of defamation addresses harm to a person's reputation or good name through slander and libel. The Internet has made it easier than ever before to disseminate defamatory statements to a worldwide audience with impunity. For some time, courts have struggled with remedies for Web defamation. The problem has been magnified by the difficulty in identifying the perpetrator, and the degree to which Internet Service Providers (ISP's) should be held accountable for facilitating the defamatory activity.

LUNNEY V. PRODIGY

One of the most recent cases addressing Internet defamation is the New York case of *Lunney v. Prodigy.*[100] In Lunney, an imposter opened several Prodigy accounts under different versions of Alexander Lunney's name. He then transmitted threatening e-mail messages to the local Boy Scout master threatening to kill him, molest his sons and "show your wife how a real Boy Scout pitches a tent." The Scout master alerted the police who reported that Mr. Lunney was not the perpetuator. Prodigy then terminated Lunney's account because of the transmission of "obscene, abusive, threatening and sexually explicit materials through the Prodigy service." When Lunney advised Prodigy that it was an imposter who had opened the accounts, Prodigy apologized and notified Lunney it had uncovered four additional accounts under his name without Prodigy's knowledge.

Lunney sued Prodigy seeking, among other things, damages for defamation by Prodigy inasmuch as Lunney was portrayed as the author of vulgar and threatening material due to Prodigy's negligence. In its analysis of whether Prodigy was liable, the court was required to determine whether Prodigy was a "publisher" or merely a "distributor" of e-mail messages.

[100] 94 N.Y.2d 242 (1999)

The court concluded that although commercial on-line services like Prodigy transmit e?mail, they do not exercise any editorial control. The court stated:

Prodigy's role in transmitting e-mail is akin to that of a telephone company, where one neither wants nor expects to superintend the content of its subscribers' conversation. In this respect, an ISP, like a telephone company, is merely a conduit.

Bulletin board postings, as opposed to e-mail, however, pose a special problem. Prodigy, as other ISP's, monitors and edits bulletin board content, thereby theoretically causing them to fall into a category of a "publisher" for purposed of defamation analysis. If Prodigy took on the responsibility of monitoring and censoring its bulletin board postings, then it would also be liable for allowing the vulgar content that injured Lunney's reputation to be published. The court, in a questionable analysis, concluded that Prodigy's power to exert editorial control did not alter its essentially passive posture as a mere conduit of information so as to render it a "publisher" of bulletin board messages. The court's choice to avoid ISP liability for the content of bulletin board messages and e-mail distributed by its members is consistent with prior cases on the topic. It does not, however, resolve the issue of how the member of an ISP such as like Mr. Lunney can obtain a remedy for defamation on the Internet against the true perpetrator.

SUING UNKNOWN DEFENDANTS AS "JOHN DOE"

Although ISP's under current case law are theoretically not liable for posting and transmitting defamatory information, they nevertheless are frequently joined as defendants in defamation lawsuits. The reason is purely a practical one that uses the "John Doe" method of suing an unknown wrongdoer.

E-mail addresses on their face do not necessarily identify the origin of the message. Domain name registration services, however, can be used to identify at least the identity of the perpetrator's own ISP. By entering the upper level domain name on a registrar's Website, the identity of the ISP of origin can usually be determined. But even if a victim is successful in identifying the wrongdoer's ISP, ISP's are reluctant to disclose the identities of

their members. To do so may expose them to claims of breach of contract, violation of privacy rights, and negligence. A controversial litigation tactic now comes into play.

Once the ISP has been identified, Internet attorneys will frequently file a lawsuit for defamation against the ISP, knowing full well that it cannot be held liable. The lawsuit also names an unknown co-defendant as "John Doe." Once the lawsuit is initiated, the attorneys are then permitted to make discovery demands on the identified ISP to obtain records and information that will reveal the true identity of the ISP's member who has been sending the offending e-mail. Once "John Doe" has been identified with the help of his own ISP, the ISP is usually dismissed from the lawsuit. The plaintiff then proceeds against the wrongdoer as the only defendant.

The laws regarding defamation differ from state to state. This poses interesting questions of jurisdictions, conflict of laws and choice of laws. As a general rule, courts apply the laws of the area where the impact and injurious effects of the defamatory statements are most felt. However, there are three general rules that courts consider for determining a court's authority to exercise jurisdiction over a person of another state who posts defamatory statements online. These are :

a) Whether there was a direct electronic activity into the state
b) An intent to conduct business or other interactions in the state
c) The activity must create in a person within a state a cause of action recognizable by the courts of that state.

POSITION IN UNITED KINGDOM:

Under English law, anyone who participates in the publication of a defamatory statement will be held liable for defamation. On the other hand, a person who merely facilitates, as opposed to participate, in the publication of the statement shall not be held liable. With respect to the internet, this distinction becomes important so as to draw a line between authorising or participating in publication on the one hand, and mere facilitation on the other. The position of passive facilitators, who provide a connection to the internet, is that it did not render the provider a publisher at common law of a statement transmitted across

the connection. The crucial consideration was whether the person had "a knowing involvement in the process of publication of the relevant words." Thus, it is essential to show that they had a degree of awareness that such words existed, or atleast an assumption of general responsibility.

Section 1 of the Defamation Act, 1996 lays down that to escape liability for defamation, the person has to show that he took reasonable care in relation to its publication and that he did not know, and had no reason to believe that what he did caused or contributed to the publication of the defamatory statement. Godfrey v. Demon Internet Ltd. is authority for the proposition that all three elements have to be satisfied in order to apply this defence. In this case, the defendant was an ISP who provided services for publication of material on the internet. The claimant, about whom defamatory material was published on the defendant's service, informed the defendant of the material on gaining knowledge of the same. However, the defendant took no care in removing the material. Morland J. rejected the contentions of the defendants that they were merely owners of an electronic device through which postings were transmitted and held them liable as they exercised sufficient degree of control over the content. This case is the only reported case in England concerned with the extent of ISP defamation liability.

As with other Commonwealth countries, Canada also follows United Kingdom law on defamation issues. Recently the Supreme Court of Canada in the case, Hill v. Church of Scientology of Toronto (1995), has reviewed the relationship of the common law of libel and its relation to the Canadian Charter of Rights and Freedoms. The reasoning in this case specifically rejects the actual malice test in New York Times Co. v. Sullivan citing criticism of it, not only in the United States, but in other countries as well.

Theoretically, damages could be very large as a publication on the internet potentially reaches millions of people. In practice, however, it is unlikely that millions of people will actually view each particular publication. In any event, publication on the internet will generally be larger than in all but the largest print or broadcast media outlets.

A company could also be held liable, as a Web site host/owner, or as an ISP, for any defamatory statement published on its site. If a hacker breaks into a Web site and publishes

a defamatory statement, the Web site host or ISP could be held liable. However, if a defendant can show that the publication of the defamatory matter was not intentional, he can escape liability proceedings. The question that will have to be decided by courts is whether a Web site host can be equated to a distributor of published matter such as a library, or whether it should simply be equated to an institution such as a telephone firm, which is a mere passive conduit for the information which it carries and over which it has no effective control.

POSITION IN UNITED STATES:

As noted before, one of the most debated issues in litigation has been determining whether online service providers and internet service providers are common carriers, distributors or publishers for the sake of defamation. In Lunney v. Prodigy, the court held that an ISP was merely a conduit and not a publisher of defamatory statements posted on its bulletin board by an imposter, and therefore was no more liable for messages than a telephone company. Thus, the position in the US is that, while publishers, who have discretion over content published, can be held liable for defamation, distributors of published material cannot be held liable. The two landmark cases that set the trend for future decisions on liability of ISPs in the US are Cubby, Inc. v. CompuServe and Stratton Oakmont v. PRODIGY Services Company.

In Cubby Inc., the court held that the defendant ISP exerted no control or knowledge regarding what was published and was, thus, merely a distributor and could not be held liable. However, in Stratton, the defendant, who owned a widely read financial bulletin board, had employed an agent and software-screening programs for monitoring purposes and thus could be considered a publisher rather than a mere distributor.

The position on ISP liability sought to be made clear by the Congress by the passing of the Communications Decency Act, 1996. Under this Act, Sec.230 provides complete immunity to ISPs by stating that "no provider or user of an interactive computer service shall be treated as publisher or speaker of any information provided by another information

content provider." By its plain language, the section creates an immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service. While various options were available to the congress, it chose to "promote the continued development of the Internet and other interactive computer services and other interactive media". In recognition of the speed with which information may get disseminated and the near impossibility of regulating information content, Congress decided not to treat providers of interactive services like other information providers such as newspapers, magazines, or television and radio stations. However, despite the good intentions with which the legislation was framed, the provision has been misused by internet service providers as one that authorizes a blanket immunity to them. This can clearly be seen in the case of Sidney Blumenthal v. Matt Drudge and America Online Inc. In this case, AOL had entered into an agreement with Drudge by which Drudge would provide all AOL members with a report on all gossip from Hollywood and Washington D.C. from his report called the Drudge Report. Drudge was alleged to have posted defamatory material about the plaintiff, who then sought to hold AOL liable. However, due to the immunity provided by Sec.230, AOL was able to escape liability despite having appointed Drudge themselves.

However, though most courts follow the precedents set by the above cases, some have recently qualified the section by taking a closer look at the responsibility of ISPs for content control. This can be seen from the case of Carafano v. Metrosplash.com, Inc., where the defendant, who operated an online matchmaking or dating service, was held liable for defamation of the plaintiff, as on examination, it was found that he exercised a great degree of control over content of the services provided by him. He could not claim immunity under Sec.230.

Thus, we see that, the law on defamation and the liability of ISPs is different in both these jurisdictions. The general practice in England is to remove a site from their service once they are informed that it contains defamatory material. Otherwise, they may held liable for defamation. In the US on the other hand, complete immunity has been provided to any secondary publisher of defamatory material. The UK approach may have a far more limiting effect on the freedom of speech on the internet than on the freedom of speech by press

or media. This is because it is unlikely that an ISP would be able to defend as strongly a suit for libel as would the press of media, as the latter are far more confident of their publishings. However, the US approach may leave individuals without an effective remedy to protect their reputation against defamatory material. It would be wrong to confer unconditional immunity to ISPs as is the current position.

POSITION IN INDIA:

To deal with the contentious issue of ISP liability in India, provision has been made in the Information Technology Act, 2000. Sec. 79 of the Act reads:

"79. NETWORK SERVICE PROVIDERS NOT TO BE LIABLE IN CERTAIN CASES."

For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him 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.

Explanation.- For the purposes of this section,-

(a) "network service provider" means an intermediary;

(b) "third party information" means any information dealt with by a network service provider in his capacity as an intermediary.

The reason for providing internet intermediaries with safe harbours is that given the obvious technical and economic impracticalities, intermediaries cannot be expected to monitor or regulate the vast amount of content that they host on their servers. The immunity is provided by the Act based on knowledge and due diligence. However, the section has been criticised on many grounds as being ambiguous and unclear. The section is silent on whether the knowledge required is actual knowledge or constructive knowledge. Further, there exist different standards of due diligence, and which standard is to be adopted is not specified in the section. Also, the scope of the section is highly limited to the term

'message', which again is not defined in the Act anywhere. This leads to ambiguity in the interpretations attached to the term. The same is true of the term 'intermediary'. Lastly, the extent of the safe harbours is limited to "this Act, rules or regulations made thereunder". This opens various litigation possibilities against service providers under civil and criminal liabilities. Thus, at best, the safe harbour provided to intermediaries under the Act proves sketchy and inadequate.

This section seeks to restrict the liabilities of a network service provider in certain cases. Let us first understand the term "network service provider" (NSP). Section 79 says that an NSP is an intermediary. The IT Act has defined the term "intermediary".

According to section 2(1)(w) of the IT Act "intermediary" with respect to any particular electronic message means any person who on behalf of another person receives,stores or transmits that message or provides any service with respect to that message;

An NSP, in respect of a particular electronic message, therefore has the following characteristics:

3. It **receives** the message on behalf of another person, or
4. It **stores** the message on behalf of another person, or
5. It **transmits** the message on behalf of another person, or
6. It **provides any service** with respect to that message.

The term "electronic message" has not been defined in the IT Act. The UNCITRAL Model Law on Ecommerce defines a **data message** as "information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy".

Note: The IT Act has been based largely on the UNCITRAL Model Law on Ecommerce.

The IT Act has inserted section 88A into the Indian Evidence Act. This section relates to an electronic message forwarded through an electronic mail server. After considering the definition of data message under the UNCITRAL Model Law and the context of electronic

message under section 88A of the Indian Evidence Act, it may be concluded that the term NSP is a narrow term that relates to electronic message service providers only (such as email service providers). It does not apply to other service providers such as search engines, auction websites etc. Even for Internet Service Providers (ISP), the benefits of this section would extend only to the email, voicemail, telephony etc services provided by them and not to the Internet connection services offered by them.

However, this section must be read in conjunction with section 85 of the IT Act that relates to liabilities of companies. This is discussed in the next chapter of this book.

Now let us examine the restrictions on the liabilities of NSPs. An NSP is not liable for any third party information or data made available by him if:

1. the NSP proves that the offence or contravention was committed without his knowledge, or
2. the NSP proves that he had exercised all due diligence to prevent the commission of such offence or contravention. The important terms used in this section are:

Knowledge implies "clear perception of a fact" or "specific information".

Illustration 1

Noodle Ltd is an email service provider. The Noodle management has read several articles in the newspapers that many people use email accounts to store and distribute pornography. Sameer has signed up for an email account provided by Noodle Ltd. He is arrested by the police for suspected publication of cyber pornography. In this case Noodle Ltd will not be liable for the offence. The Noodle management did not have specific knowledge about Sameer's misuse of the email account. They only had a vague and general knowledge about email accounts being misused by some unidentified people.

Illustration 2

Noodle Ltd is an email service provider. Sameer has signed up for an email account provided by Noodle Ltd. Another Noodle subscriber sends an email to the Noodle Customer Service department stating that Sameer is misusing his email account for spreading cyber pornography.

Noodle does not take any action. Many days later Sameer is arrested by the police for suspected publication of cyber pornography. In this case, Noodle Ltd will be liable for the offence. Noodle Ltd had specific knowledge about Sameer's misuse of the email account.

All due diligence implies "such caution and foresight as the circumstances of the particular case demand".

Illustration

Noodle Ltd is an email service provider. Sameer has signed up for an email account provided by Noodle Ltd. Another Noodle subscriber sends an email to the Noodle Customer Service department stating that Sameer is misusing his email account for spreading cyber pornography.

Noodle Ltd immediately verifies the genuineness of the complaints and deactivates Sameer's account. It also keeps a check on new email accounts being created from the IP addresses previously used by Sameer to create and access his account.Many days later Sameer is arrested by the police for suspected publication of cyber pornography. He was using a Noodle account that he had created from a cyber café using a fictitious name. In this case Noodle Ltd will not be liable for the offence. Noodle Ltd had taken all due diligence.

LIABILITY OF ISPS IN INDIA

In respect to ISPs in India, their liabilities are also determined by the **License for Internet Services** based on guidelines dated 24th August, 2007.

"**FUNDAMENTALS OF CYBER LAW**".

According to **clause 33** of this license:

1. ISPs must prevent unlawful content, messages or communications from being carried on their network. This includes objectionable, obscene, unauthorized and other content.
2. Once specific instances of such content are reported to the ISP by the enforcement agencies, they must immediately prevent the carriage of such material on their network.

3. ISPs must ensure that content carried by them does not infringe "international and domestic cyber laws".

4. The use of ISP networks for anti-national activities would be construed as an offence punishable under the Indian Penal Code or other laws.

5. ISPs are required to comply with the IT Act provisions. They are responsible for any damages arising out of default in this compliance.

6. ISPs must ensure that their networks cannot be used to endanger or make vulnerable a networked infrastructure.

7. ISPs must ensure that their services are not used to break-in or attempt to break-in to Indian networks.

8. ISPs must provide, without any delay, all the tracing facilities to trace nuisance, obnoxious or malicious calls, messages or communications transported through their equipment and network. These tracing facilities are to be provided to authorized officers of Government of India including Police, Customs, Excise, Intelligence Department officers etc.

9. ISPs must provide necessary facilities to the Government to counteract espionage, subversive acts, sabotage or any other unlawful activity.

According to **clause 34** of this license:

1. Government can monitor telecommunication traffic in the ISP network. The ISP has to pay for the necessary hardware and software for this monitoring.

2. ISPs must maintain a log of all users connected and the service they are using (mail, telnet, http etc.).

The term **telnet** can be explained through a simple illustration. Sameer runs a telnet program on his computer. Using the program he connects to Pooja's computer using a valid username and password. He then enters commands through the telnet program and these commands are executed directly on Pooja's computer. **http** (hypertext transfer protocol) is the standard method for transferring websites on the Internet.

3. ISPs must also log every outward login or telnet through their computers. These logs, as well as copies of all the packets originating from the Customer Premises Equipment of the ISP, must be available in real time to the Telecom Authority.

Logs are computer based records of activities e.g. a log of a web server may contain details of the users who visited the website, their IP addresses, the Internet browsers used by them etc.

Data travels on the Internet in the form of **packets**. Each packet carries information that will help it get to its destination. This information includes:

a. the sender's IP address,
b. the intended receiver's IP address,
c. how many packets this e-mail message has been broken into
d. identification number of the particular packet.

Customer Premises Equipment (CPE) is the equipment and inside wiring located at a subscriber's premises and connected with the ISPs channels. E.g. Pooja has signed up for Noodle's Internet services. Noodle has placed a telephone, a modem and some wiring at Pooja's house. This equipment is for use with Noodle's services and is CPE.

Real time means instantaneous. In the current context it means that the packets and logs must be made available at the very instant that they are generated or transmitted.

4. ISPs must ensure privacy of communication on their network.
5. ISPs must ensure that unauthorized interception of messages does not take place on their networks.
6. The Government can takeover the service, equipment and networks of ISPs in case of emergency, war etc.
7. The complete and updated list of the ISP's subscribers must be available in a password protected portion of the ISP's website. This is for the use of authorized Intelligence Agencies.

8. In case of dedicated line customers, the ISP must maintain logs in the following format:
9. The Chief Officer-In-Charge of technical network operations and the Chief Security Officer of the ISP should be a resident Indian citizen.
10. ISP must ensure that the information transacted by the subscribers is secure and protected.
11. The ISP officials dealing with the lawful interception of messages must be resident Indian citizens.
12. The majority Directors on the Board of the ISP must be Indian citizens.
13. Ministry of Home Affairs will regularly do security vetting in case foreigners are holding the positions of the Chairman, Managing Director, Chief Executive Officer (CEO) and/or Chief Financial Officer (CFO) of the ISP.
14. ISPs are required to physically monitor, on a monthly basis, those customers who have a high UDP traffic value. UDP (user datagram protocol) is generally used for transmitting voice, streaming video, IP TV, voice over IP and online games.

CHAPTER VI: CONCLUSION

A plaintiff would enjoy more advantages as a plaintiff in an internet defamation case in the United Kingdom than in the United States. Foreigners are allowed to file a defamation suit

in the United Kingdom if there is a real and substantial connection with that forum. However, in

internet defamation cases, it is difficult to determine whether there is a substantial connection with a particular forum and which points of attachment are relevant.

As technology evolves, and people become more involved with internet communities, it will be more difficult to determine jurisdiction in defamation cases on the internet. A person can acquire and lose his or her reputation online. A dispute resolution mechanism for online defamation

cases,[101] with online procedures, could be implemented more frequently when disputes arise. Online solutions to online problems are more cost efficient and accessible for international parties. There is, however, still a problem with choice of law, especially when defamation impacts issues concerning public policy. Few websites, for example, would willingly choose British law, if possible, to minimize costly litigation risks. Whether the suit is brought within the court system or whether alternative methods of dispute resolution are attempted, enforcement considerations may become an issue. Even if a plaintiff in a defamation suit is allowed to choose a forum, a foreign judgement may not always be enforceable. For example, in Matusevitch v. Telnikoff,[102] enforcement of a judgement from the United Kingdom was denied in the United States on public policy grounds. Furthermore, in Ehrenfeld v. Khalid Salim A. Bin Mahfouz,[103] the plaintiff sought to serve the defendant in Saudi Arabia by email and was denied that option. Instead, the plaintiff was forced to comply with the difficult task of serving Mahfouz's company's Post Office Box within a 30 day term.[104] For future consideration, an international treaty on internet defamation could be a solution to disputes that arise over which jurisdiction should apply. Based on the cases cited in this article, particularly Berezovsky v. Michaels and King v. Lewis, when Americans sued for defamation in the United Kingdom despite having no apparent ties to the UK, such a treaty could adjudicate jurisdiction and choice of law for all cases, taking into

[101] For example, the WIPO Arbitration and Mediation Center, which is widely used for domain disputes, at http://arbiter.wipo.int/center (last accessed August 22, 2006).
[102] Vladimir Matusevitch v. Vladimir Ivanovich Telnikoff, 877 F. Supp. 1; 1995 U.S. 702 A.2d 230 (1997).
[103] Rachel Ehrenfeld v. Khalid Salim A. Bin Mahfouz WL 696769 (S.D.N.Y. 2005) no. 04 Civ. 9641(RCC) March 23, 2005.
[104] Ehrenfeld was also denied the possibility of serving Malfouz's company by courier.

account the ties to specific countries. Such a treaty, however, would likely be difficult to negotiate, due to fundamental differences between countries' legislations.[105] Nevertheless, international problems require international solutions. Internet law is not the "law of the horse."[106] Internet law is related to the corpus of law as a whole. I predict that there will be an increase in legislation, such as international treaties, that would better regulate jurisdiction in internet defamation. This, in turn, would result in these types of cases being resolved with less uncertainty regarding which jurisdiction should apply.

Defamation laws should be sufficiently flexible to apply to all media. A balance will always need to be struck between freedom of expression and reputation. The difficulty is that the defamation laws world over were principally framed at a time when most defamatory publications were either spoken or the product of unsophisticated printing. Hence it is not practical to apply the principles derived from 18th and 19th century cases to the issues that can arise on the internet in the 21st century. The ultimate aim of legislation world-wide should be to reduce the costs of world trade by issuing out inconsistencies and uncertainties resulting from differences in national laws. The intense volume of information and the simplicity of its transfer make Internet a very critical source of defamation, while the electronic based trading systems are affecting all aspects of commercial and business entities. The IT revolution is sprawling new business and forcing the old modes to either change or die out. Hence most commercial organizations around the globe will be affected in some significant manner by the internet and therefore crimes in cyber space as well. It may be noted here that there has been an increasing awareness among law enforcement agencies on the need to set up special cells to handle cyber crimes. The CBI has a well-established cyber crime cell. The first such cyber crime police station has also come up in Bangalore. As the network environment becomes more pervasive and easier to use, it will also be a

[105] As noted previously, the United Kingdom and the United States have very different approaches to defamation law.

[106] Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 Harv. L. Rev., 2 501-49 (December, 1999). In his paper, Lawrence Lessig was analogizing the internet to horses. The "law of the horse" debate has two principal arguments. First, that there is a specific area of law that applies to horses, and one could study the law that only applies to horses. Second, that multiple areas of law apply to horses, and one could not only study one area of law (e.g., torts) and be familiar with all laws that apply to horses. Specifically, Lessig replied to Frank Easterbrook's lecture at the University of Chicago, "The Law of the Horse", in which Easterbrook, citing Llewellyn, denied that there was a law of cyberspace – the second argument as stated above. Easterbrook then compared the law of cyberspace to "the law of the horse." Lessig argued that cyberlaw is not the "law of the horse," but rather a distinct subject of law that is worthy of analysis – the first argument as stated above.

medium through which crime and fraud can take place. It is therefore necessary to review the current legislative provisions to ensure that the network environment is adequately protected against criminal activities. Under the current legislation there is no definition of damage and it is consequently difficult for the current enhanced penalties to be imposed.

In the short term, the following may be likely:

Ж **The** old laws will prevail until more cases and legislation emerge to provide a more refined and a more contemporary application of libel laws to the Internet.

Ж **All** Internet users will be exposed to liability for libel on the Internet, whether they are e-mail publishers, owners and/or operators of bulletin boards or home page operators. Individuals or corporate organizations who establish bulletin boards on their web sites are particularly vulnerable.

Ж **There** is unlikely to be an explosion of libel actions against individuals for several reasons.

a) The cost of libel actions.
b) The jurisdictional problems.
c) The unlikelihood of recovering many assets.
d) The opportunity and ease of immediate reply.

Ж **There** are likely to be more lawsuits against the operators of bulletin boards, whether they are corporations, organizations or individuals.

Ж **There** will be actions against owners and/or operators of web sites for statements made by their employees or their organizations.

In our opinion the Law Commission should take up the brave task of analyzing such crimes, which are at the threshold and come up with recommendations in order to equip the existing legal machinery against such offences. For the said purpose necessary amendments could be brought to Section 67 of the Information Technology Act, 2000 and also to

Section 499 of the Indian Penal Code, by expressly bring within their ambit offences such as defamation in cyber space, which is certainly a socio-economic offence.

BIBLIOGRAPHY

REPORTS & ARTICLES

- William L. Prosser, *Interstate publication*, 51 Michigan L. Rev. 959 (1953).
- Darrel C. Menthe, *Jurisdiction in Cyberspace: A Theory of International Spaces*, 4 Mich. Telecomm. Tech. L. Rev. 69 (1998).
- George F., The Time Has Come for Limited Liability for Operators of True Anonimity Remailers in Cyberspace: An Examination of the Possibilities and Perils, 6 J. Tech. L. & Pol'y, 175 (Fall 2001)
- B.P. Werley, Aussie Rules: Universal Jurisdiction over the Internet, 18 Temp.Int'l & Comp.L.J.
- J Goldsmith, "Unilateral Regulation of the Internet: A Modest Defence", 11 *EJIL* (2000) 135, at 147.
- D Post, "Against 'Against Cyberanarchy'", 17 *Berkley Technology Law Journal* (2002) 1371.
- D Menthe, "Jurisdiction in Cyberspace: A Theory of International Spaces", 4 *Mich. Telecomm. Tech. L. Rev* 69 (1998).
- M Collins, *The Law of Defamation and the Internet* (New York: Oxford University Press, 2001).
- Adrian Briggs, The Duke of Brunswick and Defamation by Internet, 119 Law Quarterly Review 119, 210-15.
- M Collins, "Defamation on the Internet After *Dow Jones & Company Inc v Gutnick*", (2003) 8 *Media & Arts Law Review* 3, 181.
- B.P. Werley, Aussie Rules: Universal Jurisdiction over the Internet, 18 Temp.Int'l & Comp.L.J. 199, 219-20.
- No Bad Puns: A Different Approach to the Problem of Personal Jurisdiction on the Internet, 116 HARV. L. REV. 1821, 1821-22.
- Para 1.16 of the British Law Commission Report on Defamation and the Internet.

WEBISTES

- www.jstor.com
- www.westlaw.com
- www.manupatra.com
- www.practicallawyer.com
- www.legaljuuris.com
- www.lexsite.com
- www.india.gov.in
- www.indiankanoon.org
- www.google.com