EXAMINING JURISDICTIONAL CHALLENGES IN CYBER COMMERCE

Augustine Amoako, Lekubu Bernard Khotso & Mabusela Oupa, Department of Criminal and Procedural Law, College of Law, University of South Africa

ABSTRACT

The background of virtually every E-commerce law issue is the question of jurisdiction. Given the ability to operate without regard for geographic borders on the Internet, the matter of who is entitled to regulate or assert jurisdiction quickly becomes as important as what is being regulated dilemma unresolvable through traditional legal jurisdictional means and thus advocate a unique, Internet-specific solution With each passing day, e-commerce gain a greater foothold within society. It has become so much a part of mainstream commerce that businesses are now often classified alternatively as brick and mortar businesses or e-businesses. For businesses to function effectively online, contractual relationship must be established. Online contracting is clearly central to the e-commerce transaction, since without the ability to create enforceable contract online, e-commerce would grind to a halt.

Keywords: E-commerce, Jurisdiction, Law, Internet, Investigation, Privacy, cybercrime.

INTRODUCTION AND CONSUMER PRIVACY ON THE INTERNET

Chaffey, (2002) claim that a government enacts legislation in order to protect consumer privacy on the internet but it is also worth noting that some individuals and organizations believe that legislation may also be too restrictive. In the United Kingdom, the telecommunication Act and Regulation of Investigatory Powers act (RIP) took several years to enact since companies were concerned to ensure security and to give security forces the ability to monitor all communications passing through Internet Services Providers and this was fiercely contested due to cost burdens placed on infrastructure providers and in particular the Internet Service Providers and many citizens and employees many not be happy being monitored (Chaffey, 2002). Laudon and Traver (2010) posit that, the online industry in the United States has historically opposed privacy legislation, arguing that industry can do a better job of protecting privacy than government hence individual companies or firms such as AOL, Yahoo, Google have adopted policies on their own in an effort to address the concern of the public about personal privacy on the internet. Laudon and Traver (2010) further claim that the online industry formed the Online Privacy Alliance (OPA) in 1998 to encourage self-regulation in part as a reaction to growing public concern and the threat of legislation being proposed by FTC and Privacy advocacy groups. In the United States, the FTC has taken the lead in conducting research on online privacy and recommending legislation to Congress. The Fair Trade Commission is a cabinet – level agency charged with promoting the efficient functioning of the marketplace by protecting consumers from unfair or deceptive practices and increasing consumer choice by enforces existing legislation by suing corporation it believes are in violation of federal fair trade laws.

INVESTIGATIONS OF ONLINE PRIVACY

In 1995, the Fair Trade Commission began a series of investigations of online privacy based on its belief that online invasion of privacy potentially involved deceit and unfair behaviour and 1998 the FTC issued its Fair Information Practice (FIP) Principles, on which it has based its assessments and recommendations for online privacy. The Fair Trade Commission's Fair Information Practice principles set the ground rules for what constitutes due process privacy protection procedures at e-commerce and all over Web-sites – including government and non-profit Web sites in the United States. Many private industries in the United States has come together and created the safe harbor idea from government regulation to enhance their online privacy with their respective organisation or firms. Also, the advertising network industry has

also formed an association called Network Advertising Initiative (NAI), to develop privacy policies. Members includes Advertising.com, Atlas, DoubleClick, Revenue Science, Tacoda and 24/7 Real Media. The Network Advertising Initiative has also developed a set of privacy principles in conjunction with the Fair Trade Commission. The policies develop by the Network Advertising Initiative have two objectives which offer a consumers a chance to opt-out of advertising network programs and to provide consumers redress from abuses Over the past decade E-commerce transactions have grown immensely (Hanefah *et al.,* 2008; Chou, 1999; Li, 2000.

CHALLENGES OF CYBER COMMERCE TO GOVERNMENT ADMINISTRATION

As Internet law has developed, a two-step analytical approach has emerged. The rise in cyber commerce has imposed a number of challenges to the government administration and regulations in relation to the tax system (Hanfah *et al.,* 2008; Edwards & Waelde, 2000). First, courts, regulators and legal practitioners must determine what law applies. In many instances it is unclear if traditional legal rules can be readily adapted to Internet activity. Although the common law is based on the laws ability to adapt to changing circumstances, in certain fields online commerce or e-commerce represents a paradigm shift of a magnitude not previously contemplated by legislators, thus leaving existing law ill-equipped to handle these emerging legal issues. Assuming the applicable law can be identified, the analysis then shifts to a second step consisting of determining who is entitled to apply the law. The effects of E-commerce activity are global in nature, such that online commerce activity – be it fraudulent conduct or defamatory postings can be accessed worldwide and, therefore, theoretically, subject the party to the legal system of any country worldwide. From a practical perspective, however, there is little risk of being hauled into court in far off jurisdictions where the likelihood of enforcing a judgement is practically nil. For multinational corporations and others operating or travelling within multiple jurisdictions, the concern that E-commerce activity can be subject to legal proceedings in several jurisdictions is nevertheless worrisome, as legal proceedings can be costly and reputational damaging. In certain respects, these concerns are not new. Regulators and courts must always be cognizant of the limitations on their regulatory reach, striving to craft regulations that meet their policy needs yet simultaneously adhering to limitations of their jurisdiction. Whether in real space or online, legal regulations often have a cross-border element that frequently results in some degree of uncertainty as to which rules apply.

CYBER COMMERCE JURISDICTION JURISPRUDENCE

The examination of the law begins with a trilogy of cases from the United States, whose courts have played the leading role in developing Internet jurisdiction jurisprudence. In the case of *Inset Systems, Inc. v Instruction Set, Inc*. The plaintiff, Inset Systems, Inc. ("Inset"), is a corporation organized under the laws of the state of Connecticut, with its office and principal place of business in Brookfield, Connecticut. Inset develops and markets computer software and other related services throughout the world. The defendant, Instruction Set, Inc. ("ISI"), is a corporation organized under the laws of the state of Massachusetts, with its office and principal place of business in Natick, Massachusetts. ISI provides computer technology and support to thousands of organizations throughout the world. ISI does not have any employees, nor offices within Connecticut, and it does not conduct business in Connecticut on a regular basis.

On August 23, 1985, Inset filed for registration as the owner of the federal trademark INSET. On October 21, 1986, Inset received registration number 1,414,031. Thereafter, ISI obtained "INSET.COM" at its Internet domain address. ISI uses this domain address to advertise its goods and services. Inset first learned of ISI's Internet domain address in March, 1995 when attempting to obtain the same Internet domain address. ISI also uses the telephone number "1-800-US-INSET" to further advertise its goods and services. Inset did not authorize ISI's use of its trademark, "INSET", in relation to both its Internet domain address and its toll-free number on June 30, 19.

In Hanson v. Denckla, the Supreme Court noted that as technological progress has increased the flow of commerce between States, the need for jurisdiction has undergone a similar increase. Twenty seven years later, the Court observed that jurisdiction would not avoided "merely because the defendant did not physically enter the forum state. The Court observed that: It is an inescapable fact of modern commercial life that a substantial amount of commercial business is transacted solely by mail and wire communications across states lines, thus obviating the need for physical presence within a State in which business are conducted. Enter the E-commerce, a global super-network of over 15000 computer networks used by over 30 million individual, corporations, organizations, and educational institutions worldwide. In recent years, businesses have begun to use the Internet to provide information and products to consumers and other businesses. E- Commerce makes it possible to conduct business throughout the world entirely from a desktop. With this global revolution looming on the

horizon, the development of the law concerning the permissible scope of personal jurisdiction based on E-commerce use is in its infant stages. Review of the available cases and materials reveals that the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet. This sliding scale is consistent with well-developed personal jurisdiction principles. At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendants enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. At the opposite end are situations where a defendant has simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions. A passive Web site that does little more than make information available to those middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site. Traditionally, when an entity intentionally reaches beyond its boundaries to conduct business with foreign residents, the exercise of specific jurisdiction is proper. Different results should not be reached simply because business is conducted over the Internet.

In *Compuserve, Inc. v Patterson,* the Sixth Circuit addressed the significance of doing business over the Internet. In that case, Patterson, a Texas resident, entered into a contract to distribute shareware through *compuserve's* Internet server located in Ohio. From Texas, Patterson electronically uploaded thirty two master software files to Compuserve's server in Ohio via the Internet. One of Patterson's software products was designed to help people navigate the Internet. When Compuserve later began to market a product that Patterson believed to be similar to his own, he threatened to sue. Compuserve brought an action in the Southern District of Ohio, seeking a declaratory judgement. The District Court granted Patterson's motion to dismiss for lack of personal jurisdiction and Compuserve appealed. The Sixth Circuit reversed, reasoning that Patterson had purposefully directed his business activities toward Ohio by knowingly entering into a contract with an Ohio resident and then "deliberately and repeatedly" transmitted files to Ohio. In analyzing a defendant's contacts through the use of the Internet, the probability that personal jurisdiction may be constitutionally exercised is "directly proportionate to the nature and quality of commercial activity that an entity conducts over cyber commerce. *Grutkowski v. Steamboat Lake Guides and Outfitters*, Inc. (quoting *Blackburn v. Walker Oriental Rug Galleries, Inc*.). Courts have established three categories of Internet

contacts, each with its own standards governing the propriety of personal jurisdiction based on those contacts. As explained in Blackburn: the first type of contact is when the defendant clearly does business over the Internet. If the defendant enters into contract with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. The second type of contact occurs when a user can exchange determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site. The third type of contact involves the posting of information or advertisements on an Internet Web site which is accessible to users in foreign jurisdictions. Personal jurisdiction is not exercised for this type of contact because a finding of jurisdiction based on an Internet Web site would mean that there would be nationwide personal jurisdiction over anyone and everyone who establishes an Internet Web site. As there is no general personal jurisdiction over defendant under the facts of this case, if personal jurisdiction exists, it must be specific. Specific jurisdiction is invoked when the cause of action arises from the defendant's forum related activities such that the defendant should reasonably anticipate being hauled into court there. To establish specific jurisdiction, the plaintiff must show that the defendant has constitutionally sufficient minimum contacts with the forum. In applying the minimum contacts standard, it is clear that a defendant will not be hauled into a jurisdiction solely as a result of random fortuitous or attenuated contacts. The likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the internet. This sliding scale approach is similar to the approach used to determine whether general jurisdiction can be exercised. At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. At the opposite end are situations where a defendant has simply posted information on a web site which is accessible to users in foreign jurisdictions. Thus, "[a] passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise [of] personal jurisdiction." The middle ground is occupied by interactive web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and the commercial nature of the exchange of information that occurs on the web site. Because the parties have agreed that Defendant's business is carried out exclusively in the British Columbia lower mainland, any claim that this Court has specific jurisdiction over Defendant must be based on the allegation that Defendant's domain name, colorworks.com,

and its web site infringe Plaintiff's trademark in Pennsylvania and that Defendant's web site can be accessed in Pennsylvania. Upon review of recent cases that have addressed the issue of whether a forum can exercise specific jurisdiction over a non-resident defendant based upon a claim that the defendant's web site or domain name infringes the trademark rights of a resident plaintiff, a basic principal emerges: [S]imply registering someone else's trademark as a domain name and posting a web site on the Internet is not sufficient to subject a party domiciled in one state to jurisdiction in another…[T]here must be "something more" to demonstrate that the defendant directed his activity towards the forum state.

ZIPPO DOCTRINE AND JURISDICTION IN THE INTERNET CONTEXT

Despite the widespread acceptance of the *Zippo* doctrine (and indeed the export of the test to other countries, including Canada), cracks in the test began to appear late in 1999. In fact, closer examination of the case law indicates that by 2001, many courts were no longer strictly applying the *Zippo* standard but rather were using other criteria to determine when assertion of jurisdiction was appropriate. Numerous judgments reflect that courts in the United States moved towards a broader, effects-based approach when deciding whether or not to assert jurisdiction in the Internet context. Under this approach, rather than examining the specific characteristics of a Web site and its potential impact, courts focused their analysis on the actual effects that the Web site had in the jurisdiction. Indeed, courts are now relying increasingly on the effects doctrine that was established by the U.S. Supreme Court in *Calder v. Jones.* This doctrine holds that personal jurisdiction over a defendant is proper when (a) the defendant's intentional tortious actions expressly aimed at the forum state; (b) causes harm to the plaintiff in the forum state, of which the defendant knows is likely to be suffered. In *Calder*, a California entertainer sued Florida publisher for libel in a California district court. In ruling that personal jurisdiction was properly asserted, the court focused on the effects of the defendant's actions. Reasoning that the plaintiff lived and worked in California, spend most of her career in California, suffered injury to her professional reputation in California, and suffered emotional distress in California, the court concluded that the defendant had intentionally targeted a California resident and thus it was proper to sue the publisher in that state. The application of the Calder test can be clearly seen in an Internet context in *Blakey v. Continental Airlines, Inc*., an online defamation case involving an airline employee, living in Seattle and based out of Houston. The employee filed suit in New Jersey against her co-employees, alleging that they published defamatory statement on the employer's electronic bulletin board, and against her

employer, a New Jersey-based corporation, alleging that it was liable for the hostile work environment arising from the statements. The lower court granted the co-employees' motion to dismiss for lack of personal jurisdiction and entered summary judgement for the employer on the hostile work environment claim.

In reversing the ruling, the New Jersey Supreme Court found that the defendants who published defamatory electronic messages with the knowledge that the messages would be published in the New Jersey could properly be held subject to the state's jurisdiction. The court applied the effects doctrine and held that while actions causing the effects in New Jersey were preformed outside the state, this did not prevent the court from asserting jurisdiction over a cause of action arising out of those effects. The broader effects-based analysis can also be seen moving beyond the defamatory tort action at issue in *Calder* and *Blakey* to range of disputes, including intellectual property and commercial activities. On the intellectual property front, *Nissan Motor Co. Ltd.* v. *Nissan Computer Corporation* typifies the approach. The plaintiff, an automobile manufacturer, filed a complaint in California district court against a Massachusetts-based computer seller, alleging tht the defendant's "nissan.com" and "nissan.net" Internet domain names infringed on its "Nissan" trademark. Prompting the complaint was an allegation that the defendant altered the content of its "nissan.com" Web site to include a logo that was similar to the plaintiff's logo, as well as to include links to automobile merchandisers and auto related portions of search engines. In October 1999 the parties met to discuss the possibility of transferring the nissan.com domain name. These negotiations were ultimately unsuccessful. The defendant brought a motion to dismiss for lack of personal jurisdiction and improper venue, and the plaintiff brought a motion for a preliminary injunction in March 2000.

In considering the defendant's motion, the court relied on the effects doctrine to assert jurisdiction, ruling that the defendant had intentionally changed the content of its Web site to exploit the plaintiff's goodwill and to profit from consumer confusion. Moreover, since the plaintiff was based in California, the majority of the harm was suffered in the forum state. The court rejected the defendant's argument that it was not subject to personal jurisdiction because it merely operated a passive Web site. Although the defendant did not sell anything over the internet, it derived advertising revenue through the intentional exploitation of consumer confusion. This fact, according to the court, satisfied the *Cybersell* requirement of "something more" in that it established that the defendant's conduct was deliberately and substantially directed toward the forum state. Courts have also refused to assert jurisdiction in number cases

based on what is best described as insufficient commercial effects. For example, in the case of *People Solutions Inc. v. People Solutions, Inc.* the defendant, a California-based corporation, moved to dismiss a trademark infringement suit brought against it by a Texas-based corporation of the same name. The plaintiff argued that the suit was properly brought in Texas since the defendant owned a Web site that could be accessed and viewed by Texas residents. The site featured several interactive pages that allowed customers to take and score performance test, download product demos, and order products online. The court characterized the site as interactive but refused to assert jurisdiction over the matter. Relying on evidence that no Texans had actually purchased from then Web site, the court held that "[p]ersonal jurisdiction should not be premised on the mere possibility, with nothing more, that Defendant may be able to do business with Texans over it Web site. Instead, the plaintiff had to show that the defendant had 'purposefully availed itself on the benefits of the forum state and its laws."

In copyright dispute over craft patterns yielding a similar result in *Winfield Collection, ltd.* v. *McCauley*. The plaintiff, a Michigan-based manufacturer of craft patterns, filed a complaint in Michigan district court accusing the defendant, a resident of Texas, of infringing copyrighted craft patterns that it had supplied to the defendant. The defendant moved to dismiss the suit for lack of the personal jurisdiction. The plaintiff argued that the court could exercise personal jurisdiction because (a) the defendant had sold crafts made with the plaintiff's patterns to Michigan residents on two occasions, and (b) the defendant maintained an interactive Web site that could send and receive messages. The court refused to assert jurisdiction, dismissing both arguments. With respect to the plaintiff's first argument, the court focused on the fact that the sales were in fact concluded on eBay, an online auction site. Since the items were sold to the highest bidder, the defendant had no advance knowledge about where the products would be sold.

Cyber Commerce and Criticism of the Zippo Doctrine

One of the strongest criticisms of the Zippo doctrine can be found in *Millenium Enterprises, Inc v. Millenium Music. L.P,* another case in which the court found insufficient commercial effects and therefore declined to assert jurisdiction. The defendant, a South Carolina corporation, sold products both offline and on the Web. The plaintiffs, an Oregon-based corporation, sued the defendants in Oregon district court for trademark infringement. The defendant filed a motion to dismiss for lack of personal jurisdiction. After canvassing numerous Internet Jurisdiction cases decided by the Ninth Circuit, as well as Zippo, the court stated: The

middle interactive category of Internet contacts as described in Zippo needs further refinement to include the fundamental requirement of personal jurisdiction: "deliberate action" within the forum state in the form of transaction between the defendant and resident of the forum or conduct of the defendant purposefully directed at residents of the forum state. Although the case law illustrates that there was no single reason for the courts to shift away from the *Zippo* test, a number of themes do emerge. First, the test simply doesn't work particularly well in every instance. For example, with courts characterizing chat room postings as passive in nature, many might be inclined to dismiss cases involving allegedly defamatory or harassing speech on jurisdictional grounds. Such speech may often be targeted toward a particular3 individual or entity located in a jurisdiction different from that of the poster or the chat site itself.

The *Zippo* test also falls short when active sites are at issue, as the court in people *solutions* recognized. That court is request for evidence of actual sales within the jurisdiction illustrates that the mere potential to sell within a jurisdiction does not necessarily make a web site active. While the active web site may want to sell into every jurisdiction, the foreseeability of a legal action is confined primarily to those places where actual sales occur. The *Zippo* test does not distinguish between actual and potential sales, however, but rather provides that the mere existence of an active site is sufficient to assert jurisdiction. Again, the problem with the *Zippo* test is not limited to inconsistent and often undesirable outcomes. The test also encourages a perverse behavior that runs contrary to public policy related to the Internet and e-commerce. Most countries have embraced the potential of e-commerce and adopted policies designed to encourage the use of the Internet for commercial purposes. The *Zippo* test, however, inhibits e-commerce by effectively discouraging the adoption of interactive Web sites. Prospective Web sites owners who are concerned about their exposure to legal liability will rationally shy away from developing active Web sites since such sites increase the a likelihood of facing lawsuits in far-off jurisdictions. Instead, the test encourages passive Web sites that feature limited legal exposure and therefore present limited risk. Since public policy aims are to increase interactivity and the adoption of e-commerce (and in doing so, enhance consumer choice and open new markets for small and medium sized businesses), the *Zippo* test acts as a barrier to that policy approach. One of the primary reason for the early widespread support for the *Zippo* test was the desire for increased legal certainty for internet jurisdiction issues. While the test may not have been perfect, supporters felt it offered a clear standard that would allow businesses to conduct effective legal risk analysis and make rational choices with regard to their approach to the internet. In the final analysis, however, the *Zippo* test simply does not

deliver the desired effect. First, the majority of Web sites are neither entirely passive nor completely active. Accordingly, they fall into the "middle zone" that requires courts to gauge all relevant evidence and determine whether the site is "more passive" or "more active." With many sites falling into this middle zone, their legal advisors are frequently unable to provide a firm opinion on how any given court might judge the interactivity of the Web site. Second, distinguishing between passive and active sites is complicated by the fact that some sites may not be quite what they seem. For example, sites that feature content best characterized as passive may actually be using cookies or other at collection technologies behind the scenes unbeknownst to the individual user. Given the value accorded to personal data, its collection is properly characterized as active, regardless of whether it occurs transparently or surreptitiously. Third, it is important to note that the standards for what constitutes and active or passive Web site are constantly shifting. When the test was developed in 1997, an active Web site might have featured little more than an email link and some basic correspondence functionality. Today, sites with that level of interactivity would likely be viewed as passive, since the entire spectrum of passive versus active has shifted upward together with improved technology. In fact, it can be credibly argued that sites must constantly re-evaluate their position on the passive versus active spectrum as Web technology changes. Fourth, the effectiveness of the *Zippo* test is no better even if the standards for passive and active sites remain constant. With the expense to create a sophisticated Web site now easily in excess of $100,000, few organizations will invest without anticipating some earning potential for their Web-based venture. Since revenue is typically the hallmark of active Web sites, most new sites are likely to feature interactivity and be categorized as active site. From a jurisdictional perspective, this produces an effect similar to that found in the Inset line of cases – any court anywhere can assert jurisdiction over a Web site, since virtually all sites will meet the *Zippo* active benchmark. In light of the ever-changing technological environment and the shift toward predominantly active Web sites, the effectiveness of the *Zippo* doctrine is severely undermined regardless, of how it develops. If the test evolves with changing technological environment, it fails to provide much needed legal certainty and if the test remains static to provide increased legal certainty, it risks becoming irrelevant as the majority of Web sites meet the active test standard. Given the inadequacies of the *Zippo* passive versus active test, it is now fitting to identity a more effective standard for determining when it is appropriate to assert jurisdiction in cases involving predominantly Internet-based contacts. With the benefit of the *Zippo* experience, the new test should remain technology neutral so as to (a) remain relevant despite ever-changing Web technologies, (b) create incentives that, at a minimum, do not discourage online interactivity, and (c) provide

sufficient certainty so that the legal risk of operating online can be effectively assessed in advance. Unlike the Zippo approach, a targeting analysis would seek to identify the intentions of the parties and to assess the steps taken to either enter or avoid a particular jurisdiction. Targeting would also lessen the reliance on effect-based analysis, the source of considerable uncertainty, since Internet-based activity can ordinary be said to create some effects in most jurisdictions. Zippo analysis is presently utilized to serve the U.S. court as an inquiry tool for the jurisdiction of non-resident based online activity, however, it is likely additional analyzing of the issues particularly where a defendant's website would involve a tort claim or modestly interactive or passive website. With such cases the analyzing would apply the effects test. Attorneys supporting jurisdiction, must be mindful to use both tests, neither the effects test like the zippo test is free from subjectiveness. The Zippo sliding-scale might not be successful, the effects test may prove successful. Decisions are often made at the threshold of litigation. Inferences on the pleadings are drawn from the pleadings and often pose an issue. Facts which could lead one court to conclude a defendant to purposefully intend to cause an effect within a specific jurisdiction might lead to two differing conclusions in court. Furthermore, courts are not equal in stringent requirements targeted at the forum itself with the purpose to invoke the effects test. Impacting to some courts means "targeting" implies an effort specifically to reach a person who resides in the forum, rather than to generate impact in that area. Ultimately the ending results are the cases convey results that show the predictability of the outcome is possibly only marginally greater under the effects test than the sliding-scale test. A targeting approach is not a novel idea. Several U.S. courts have factored targeting considerations into their analysis of the appropriateness of asserting jurisdiction over Internet- Based activities. For example, in *Bancroft and Masters, Inc. v. Augusta National Inc*., a dispute over the "masters.com" domain name, the Ninth Circuit of Appeal noted that the effect test, the defendant must have (1) committed an intentional act, which was (2) expressly aimed at the forum state, and (3) caused harm, the brunt of which is suffered and which the defendant knows is likely to be suffered in the forum state. Now, to the courts it may insinuate that the effects within the forum were foreseeable results. Whilst a defendant's intent to inflict injury within the forum ought to be determining specifics in facts and cases, numerous factors are necessary in gauging the intent. Essentially, the courts should contend beyond the accessibility matter of the defendant's website. Allegations of specific intent should be present of damage inflicted at the plaintiff within the forum where he (plaintiff) resides. Impact of the content in question should be shown upon at least a critical mass of viewers in the jurisdiction.

CONCLUSION

With governments and regulators generally frustrated with their lack of control over the internet activities, the potential for Internet Service Providers to carry out the regulatory function is viewed by some as a possible solution to Internet regulation. Particularly if one accepts the important role that technology can play in regulating internet activity, then the role of the ISPs becomes quite crucial.

REFERENCES

1. Ayres I, Braithwaite J (1992) Responsive Regulation: Transcending the Deregulation Debate. Oxford University Press, Oxford.
2. Barlow J.P. (1996) A Declaration of the Independence of Cyberspace. [Last accessed 20 June 2015]. Available from URL: https://projects.eff.org/~barlow/Declaration-Final.html
3. Chatterjee C. (2002) *e-Commerce Law for business Managers*, Financial World Publishing, Canterbury.
4. Efraim T. et al (2010) *Electronic Commerce: A managerial Perspective* Sixth Edition, Prentice Hall, New Jersey.
5. Geist M. (2002) *Internet Law in Canada* Third Edition, Captus Press Inc., Ontario.
6. Kenneth C. and Carol G. (2010) *E-Commerce, Business Technology Society* Sixth Edition, Prentice Hall, New Jersey.
7. Shon H. (2005) *CISSP All-in-One Exam Guide*, Third Edition McGraw-Hill, California.
8. Bennett C. J. (2004) Privacy Self-Regulation in a Global Economy: A Race to the Top, the Bottom or Somewhere Else? In: Webb K (ed), Voluntary Codes: Private Governance, the Public Interest and Innovation, pp. 227-249. Carleton University, Ottawa.
9. Bonnici M.J.P. (2008) Self-regulation in Cyberspace, T.M.C. Asser Press, The Hague.
10. Bowman D.M., Hodge G.A. (2009) Counting on codes: An examination of transnational codes as a regulatory governance mechanism for nanotechnologies, Regulation & Governance 3(2), pp. 145164.
11. Li, J. (2000). E-Commerce Tax Policy in Australia, Canada and the United States. University of New *South Wales Law Journal, 23*(2), 313-329.
12. Li, J. (2003). International Taxation in the Age of Electronic Commerce: A comparative Study, Toronto: Canadian Tax Foundation
13. Hanefah, H.M.M., Hassan, H. & Othman, Z. (2008). E-commerce implications: Potential problems and challenges in Malaysia, *International Business Research,* vol.1 (1); pp.43- 57.