Chapter 6

JURISDICTION

The Internet has no territorial boundaries. To paraphrase Gertrude Stein, as far as the Internet is concerned, not only is there perhaps 'no there there,' the 'there' is everywhere where there is Internet access.

Nancy Gertner[872]

6.1 Introduction

Enforcement of human rights of cyberspace entities is crucial and without enforcement mechanism the exercise of human rights in cyberspace becomes meaningless. The question to be asked of any law or regulation that purports to govern activity on the Internet is not whether it is applicable, but rather whether it is enforceable? Though it may be vogue to call for regulation, the primary question that should govern whether or how a regulation should be framed is not whether it is applicable- it will almost certainly be so. The question must be whether the regulation is needed, and if so, whether it is enforceable in a coherent and satisfactory manner that satisfactory mechanism yields fruits. If regulations are not needed or do not prove to be enforceable due to the jurisdictional or substantive issues then there is a threat that users of the internet will hold them in contempt[873].
This distinction between applicability and enforceability is fundamental to the future development of Internet law. It is a comparatively easy task for a legislator to draft a law which applies to a particular activity undertaken via the Internet, but much more difficult to frame the law so that it is enforceable in practice. Laws which are unenforceable have two major defects; not only do they fail to deal with the

[872] Judge who delivered the judgment in Digital Equipment Corp. v. Altavista Technology, Inc., 1997 , 960 F. Supp. 456, 462 (D. Mass. 1997), available at http://www.techlawjournal.com/courts/drudge/80423opin.htm , visited on 12 Dec 2003
[873] Lars Davies, A Model for Internet Regulation?- Constructing a Framework for Regulating Electronic Commerce, Society for Computers and Law, London, 1999, available at www.scl.org ,visited on 1 Jun 2003

mischief which the law seeks to remedy, but the knowledge that they are unenforceable weakens the normative force of other laws[874].

In relation to the enforceability of law and regulations, it is important to recognize that compliance with law is not solely dependent on that law's enforcement through the courts. In the vast majority of the instances, the law is complied with because of its normative force, that is, because it is law[875]. Thus most citizens refrain from criminal behaviour because they wish to act lawfully, not because of a fear of prosecution and similarly private law matters such as contracts, the parties adhere to their bargains because that is what they have agreed. However, the ultimate enforceability of a law is important if it is to have normative force. For this reason, a system of law regulation, which is so contradictory that it is in practical terms, impossible to obey is treated here as unenforceable. Because it is impossible or excessively burdensome to act in accordance with the law it loses normative force and ceases to be treated by citizens and businesses as binding on them.

The first problem one would face in enforcement of his right is in relation to jurisdiction of courts and the applicability of procedural and substantive law for the dispute to be resolved. Cyberspace having multijurisdcitionality as its main feature poses several challenges to legal community for the enforcement of basic rights. Interestingly it is human rights issues involving free speech in Yahoo! France case and defamation in Gutnick case highlighted the jurisdictional problems created by cyberspace activities.

6.2 Jurisdiction

Jurisdiction refers to the power of a state to govern persons, property and situations. A number of different categories and types of jurisdiction should be identified from the outset. It is necessary to distinguish between prescriptive jurisdiction, which

[874] Reed Chris, Internet Law- Text and Materials, 2nd Edition, Universal Law Publishing Co.,Delhi,2004

[875] Kelsen , Hans, Pure Theory of law, 2nd Edition, Unviversity of California, Berkeley, 1967, at pp 35-47

indicates the power to prescribe rules, and enforcement jurisdiction, which refers to the power to enforce rules.

International law concerns itself with the propriety of the exercise of jurisdiction. Jurisdiction has primarily and historically been exercised on a territorial basis, but there are occasions when states exercise jurisdiction over people or things outside their own territory. Governmental power gave rise to three types of jurisdiction: prescriptive jurisdiction, adjudicative jurisdiction and enforcement jurisdiction[876]. Prescriptive jurisdiction is the power to apply legal norms to conduct; adjudicative jurisdiction is the power of tribunals to resolve disputes; and enforcement jurisdiction is the power of the jurisdiction to enforce[877].

In addition to jurisdiction exercised on a territorial basis there are a number of other relevant principles, which have been identified, and which have received varying degrees of international acceptance. The commentary on the Harvard Research Draft Convention on Jurisdiction with respect to Crime in 1935 identified five general heads of jurisdiction, namely:

(a) The territorial principle

(b) The passive personality principle

(c) The nationality principle

(d) The protective principle ; and

(e) The universality principle

The heads of traditional jurisdiction may be briefly defined as follows;

(a) **Territorial principle**: The ability of a state to exercise jurisdiction over actions, events and things within its territory is an essential attribute of sovereignty and the territorial principle has received universal recognition. According to this principle, events occurring within a state's territorial boundaries and persons within that territory, albeit temporarily, are subject to local laws and the jurisdiction of the local

[876] Perritt H Henry, Jr, Jurisdiction and the Internet: Basic Anglo/American Perspectives, Internet Law Forum, July 26, 1999, available at http://www.ilpf.org/confer/present99/perrittpr.htm , visited on Feb 26, 2002

[877] ibid

courts. The principle has practical advantages in terms of availability of witnesses[878].

(b) **Passive Personality**: Under this principle, jurisdiction is claimed on the basis of the nationality of the actual or potential victim. In other words, a state may assert jurisdiction over activities which, although committed abroad by foreign nationals, have affected or will affect nationals of that state[879].

(c) **Nationality Principle**: Most civil law system claim a wide jurisdiction to punish crimes committed by their nationals, even on the territory of a foreign state. Those states which make little use of the nationality principle do not appear to protest about its use elsewhere. Although a state may not enforce its laws within the territory of another state, it can punish crimes committed by nationals extra-territorially when the offender returns within the jurisdiction. Jurisdiction based on nationality is less usual in common law countries, although there may be exceptions with regard to serious offences[880].

(d**) Protective or security Principle**: Under this principle, a state can claim jurisdiction over offences committed outside its territory, which are considered injurious to its security, integrity or vital economic interests. The principle remains ill defined and there are uncertainties about how far it can extend. There remains a considerable danger of abuse. Nevertheless, a large number of states have used the principle to a greater or lesser extent. Generally speaking the protective personality principle is most often used in cases involving currency, immigration and economic offences[881].

(e**) Universality Principle**: It has been seen that so far all the bases of jurisdiction have in some way involved a connection with the state asserting jurisdiction; events

[878] Brian Fitzgerald and Anne Fitzgerald, Cyberlaw- Cases and Materials on the Internet, Digital Intellectual Property and Electronic Commerce, LexisNexis, Butterworths,, Australia, 2002 at p 121
[879] ibid at p 122
[880] ibid
[881] ibid

have taken place within the territory of the jurisdictional state or they have been committed by or against nationals or in some other way impinge on the interests of the state claiming jurisdiction. International law further recognizes that where an offence is contrary to the interests of the international community, all states have jurisdiction irrespective of the nationality of the victim and perpetrator and the location of the offence. The rationale behind the universality principle is that repression of certain types of crime is a matter of international public policy[882]. Human rights being universal rights, their violations in cyberspace would be contrary to the interests of the international community.

The non-geographic character of the net makes it very difficult to apply current, territorially based rules to activities online[883]. Sovereign countries may have monopoly on the lawful use of physical force but they cannot control online actions whose physical location is irrelevant or cannot even be established. Majority Jurisdictional issues that have been raised are related to legal disputes in the areas of trademarks, domain names, defamation, free speech, copyright etc.

6.2.1 Personal Jurisdiction, Multimedia and Broadcasting

In evaluating the ability to obtain personal jurisdiction over a defendant due to operation of a Web site, a parallel can be drawn to print publications. Print publications, like Web sites, come into contact with several jurisdictions, based on conduct that occurs primarily in one location. Print publications are created by conduct concentrated at the location of the author and publisher. The activity creating a Web site occurs in the state in which the Web site is developed, and the location of the Web server. However, like a broadly distributed magazine or broadcast, a Web site is accessible everywhere[884].

---

[882] ibid

[883] David R Johnson and David G Post, Law And Borders-Rise of Law in Cyberspace, 48 Stanford Law Review 1367 (1996)

[884] Warren E. Agin of Swiggart & Agin, L.L.C., Coping with Personal Jurisdiction in Cyberspace ABA Subcommittee on Internet Law Liability Report #3, available at http://library.findlaw.com/2000/Dec/20/126993.html , visited on 5 Mar 2005

The United States Supreme Court has held that a state can exercise personal jurisdiction over a publisher accused of publishing libelous material about a resident of that state when the publisher targets its economic activity at that state. In Keeton v. Hustler Magazine, Inc[885] the United States District Court for the District of New Hampshire was able to exercise personal jurisdiction over an Ohio corporation because the defendant's magazine circulation in the state of New Hampshire created minimum contacts with that state. Jurisdiction was appropriate because of the State's interest in discouraging libel by the defendant against its citizens[886].

In a companion case, Calder v. Jones[887], the Supreme Court held that a California court could exercise personal jurisdiction against an author and editor, both resident in Florida, who had libeled a California resident in an article published in the National Enquirer newspaper. The court determined that the defendants had purposefully targeted their libelous activity at California by publishing their article containing libelous material about a California resident in a magazine which they knew was sold and circulated in California and "must reasonably anticipate being haled into court" in California[888].

In these cases, the tortious act is the knowing publication in the state attempting to exercise personal jurisdiction over the defendant. The results differ if the tortious act is unrelated to the act of publication. If, instead of publishing an article in a magazine or newspaper circulated in the forum state, the defendant submits advertising to a nationally circulated magazine or newspaper, the fact of that advertising is generally not sufficient to create jurisdiction, unless the claim arises from the advertising. For example, in IDS Life Insurance Company v. SunAmerica,

---

[885] Keeton v. Hustler Magazine, Inc., 465 U.S. 770, 104 S. Ct. 1473 (1984), available at http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=465&invol=770, visited on 23 Feb 2003
[886] ibid
[887] Calder v. Jones, 465 U.S. 783, 104 S. Ct. 1482 (1984) available at http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=search&court=US&case=/us/465/783.html, visited on 20 May 2004
[888] ibid

Inc[889], the defendant advertised in nationally circulated newspapers and magazines and on national television, and maintained an Internet Web site. The District Court for the Northern District of Illinois held that such advertising did not involve systematic and continuous contact with the forum state, Illinois, and concluded that it did not have personal jurisdiction over the defendant[890]. In another case, Gaingolo v. Walt Disney World Co[891], a district court judge noted that allowing national advertising to make a defendant subject to suit wherever the advertisement appeared would "substantially undermine the law of personal jurisdiction[892]."

6.3 Evolution of Internet Jurisdiction – Case Law Development

While Internet jurisdiction creates significant challenges, courts have not enjoyed the luxury of considering the issue from an abstract, theoretical perspective. Since 1996, courts in the United States have regularly faced litigation that includes an Internet jurisdiction component. As courts grapple with the issue, the jurisprudence has shifted first toward the Zippo passive versus active test, then more recently towards an effects based test with elements of targeting analysis[893].

In International Shoe Co. v. Washington, the US Supreme Court outlined the contemporary basis for jurisdiction[894]. In this case the Court held that, a court could exercise personal jurisdiction over a nonresident defendant if that defendant has "certain minimum contacts with [the forum] such that the maintenance of the suit does not offend 'traditional notions of fair play and substantial justice.'[895] The minimum contacts standard serves two purposes: protecting defendants from

---

[889] DS Life Insurance Company v. SunAmerica, Inc., 958 F. Supp. 1258 (N.D. Ill. 1997), available at http://laws.findlaw.com , visited on 2 Mar 2003

[890] The court stated, in reaching its decision that "It cannot plausibly be argued that any defendant who advertises nationally could expect to be haled into court in any state, for a cause of action that does not relate to the advertisements."

[891] Gaingolo v. Walt Disney World Co., 753 F. Supp. 148 (D.N.J. 1990), available at http://laws.findlaw.com, visited on 2 Mar 2003

[892] ibid

[893] Geist ,A Michael, Is There A There There? Toward Greater Certainty For Internet Jurisdiction**,** Berkeley Technology Law Journal, Vol.16, Issue 16:3, Fall 2001

[894] 326 U.S. 310, 316 (1945) available at http://lwas.findlaw.com/us/326/310.html, visited on 15 May 2003

[895] ibid

burdensome litigation and ensuring that states do not reach too far beyond their jurisdictional limits[896].

Minimum contacts have been defined as "conduct and connection with the forum . . . such that the defendant should reasonably anticipate being haled into court there."[897] A defendant's contacts are sufficient to satisfy the minimum contacts standard where they are "substantial" or "continuous and systematic," such that the defendant "purposefully availed itself of the privilege of conducting activities within the Forum State, thus invoking the benefits and protections of its laws."[898] The plaintiff has the burden of showing that the defendant took action "purposefully directed" at the forum and that the cause of action arises from this action.[899] A defendant "purposefully avails" himself of jurisdiction when "the contacts proximately result from actions by the defendant himself that create a 'substantial connection' with the forum State.'[900]

In determining whether the exercise of jurisdiction comports with notions of fair play and substantial justice, a court must balance several factors. These factors are: (1) the extent of a defendant's purposeful interjection; (2) the inconvenience to the defendant of defending in that forum; (3) the extent of conflict with the sovereignty of the defendant's state; (4) the forum state's interest in adjudicating the dispute; (5) the interstate judicial system's interest in the efficient resolution of conflicts; (6) the plaintiff's interest in obtaining convenient and effective relief; and (7) the existence of an alternative forum[901].

---

[896] World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 291 (1980) available at http://laws.findlaw.com/us/444/286.html , visited on 25 June 2003

[897] ibid

[898] Hanson v. Denckla, 357 U.S. 235, 253 (1958) available at http://supreme.justia.com/us/357/235/case.html, visited on 23 June 2003

[899] Supra Note 887,Calder v. Jones, 465 U.S. 783, 789 (1984) (upholding jurisdiction where conduct was allegedly calculated to cause injuries in the forum state and the cause of action arose from this conduct).

[900] Burger King v. Rudzewicz, 471 U.S. 462, 475 (1985) available at http://supreme.justia.com/us/471/462/case.html, visited on 23 June 2003

[901] ibid

One of the earliest US case in which applications of these principles to the Internet traces back to 1996 and applied by a Connecticut District court in Inset Systems, Inc. v. Instruction Set, Inc.,[902]. In this instance, Inset Systems, a Connecticut company, brought a trademark infringement action against Instruction Set, a Massachusetts company, arising out of its use of the domain name "Inset.com."[903] Instruction Set used the domain name to advertise its goods and services on the Internet, a practice to which Inset objected since it was the owner of the federal trademark "Inset."[904] The legal question before the court was one of jurisdiction. Did Instruction Set's activity, the establishment of a website, properly bring it within the jurisdiction of Connecticut under that state's long-arm statute? Did Inset's conduct meet the minimum contacts standard outlined by the United States Supreme Court in World-Wide Volkswagen?[905].In this case the court concluded that it could properly assert jurisdiction, basing its decision on Instruction Set's use of the Internet[906]. Likening the Internet to a continuous advertisement, the court reasoned that Instruction Set had purposefully directed its advertising activities toward Connecticut on a continuous basis and therefore could reasonably have anticipated being sued there.[907]

The court's decision was problematic for several reasons. First, its conclusion that creating a website amounts to a purposeful availment of every jurisdiction distorts

---

[902] Inset Sys., Inc. v. Instruction Set, Inc., 937 F. Supp. 161 (D. Conn. 1996) available at http://cyber.law.harvard.edu/property00/jurisdiction/insetedit.html, visited 24 June 2003

[903] Internet domain names, which have become a ubiquitous part of commercial advertising, enable users to access websites simply by typing in a name such as "www.inset.com" in their web browser. The "www" portion of the address identifies that the site is part of the World Wide Web; the "Inset" portion is usually the name of a company or other identifying words; and "com" identifies the type of institution, in this case a company. Domain names, the subject of several other litigated cases, are administered in the United States by a government appointed agency, Network Solutions Inc. (NSI) and are distributed on a first come, first served basis. *See* Cynthia Rowden & Jeannette Lee, Trademarks and the Internet: An Overview, Nov. 4, 1998, available at http://www.bereskinparr.com/art-pdf/TM&InternetOverview.pdf. visited on 23 Apr 2003

[904] Supra Note 902, Inset Sys., Inc. v. Instruction Set, Inc., 937 F. Supp. 161

[905] World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 291 (1980) available at http://laws.findlaw.com/us/444/286.html, 13 July 2003

[906] Supra Note 902, Inset Sys., Inc. v. Instruction Set, Inc., 937 F. Supp. 161

[907] ibid

the fundamental principle of jurisdiction[908]. Second, the court did not analyze the Internet itself, but merely drew an analogy between the Internet and a more traditional media form, in this case a continuous advertisement[909]. If the court was correct, every court, every-where, could assert jurisdiction where a website was directed toward its forum. This approach would stifle future Internet growth, as potential Internet participants would be forced to weigh the advantages of the Internet with the chances of being subject to legal jurisdiction throughout the world. Third, the court did not assess Instruction Set's actual activity on the Internet[910]. The mere use of the Internet was sufficient for the court to hold that jurisdiction was established[911]. In fact, the court acknowledged that Instruction Set did not maintain an office in Connecticut nor did it have a sales force or employees in the said state[912]. This principle would affect the interest of cyberspace entities severely restricting their free speech as standards of free speech scrutiny vary from country to country.

In Bensusan Rest. Corp. v. King[913], a New York district court created an important exception to the rule created in Inset Systems[914]. The Blue Note was a small Columbia, Missouri club operated by the defendant (King). King promoted his club by establishing a website that included information about the club, a calendar of events, and ticketing information[915]. New York City was also home to a club named The Blue Note, this one operated by the Bensusan Restaurant Corporation, who owned a federal trademark in the name[916]. King was familiar with the New York Blue Note as he included a disclaimer on his website that stated: "The Blue Note's

---

[908] Supra Note 902,Inset Sys., Inc. v. Instruction Set, Inc., 937 F. Supp. 161, 165

[909] Geist A Michael,, Is There A There There? Toward Greater Certainty For Internet Jurisdiction , Berkeley Technology Law Journal, Vol.16, Issue 16:3, Fall 2001

[910] ibid at p 25

[911] ibid at p 26

[912] ibid at p 26

[913] 937 F. Supp. 295 (S.D.N.Y. 1996), available at http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=2nd&navby=docket&no=969344 , visited on 15 Aug 2003

[914] Supra Note 902

[915] Supra Note 913,Bensusan Rest. Corp. v. King, 937 F. Supp. 295 (S.D.N.Y. 1996)

[916] ibid

Cyberspot should not be confused with one of the world's finest jazz clubs, the Blue Note, located in the heart of New York's Greenwich Village..."[917]

Within months of the establishment of King's Blue Note website, Bensusan brought a trademark infringement and dilution action in New York federal court[918]. Once again, the court faced the question of personal jurisdiction in a trademark action arising out of activity on the Internet. Unlike the Inset systems line of cases, however, the court considered the specific uses of the website in question. It noted that King's website was passive rather than active in nature, that is, several affirmative steps by a New York resident would be necessary to bring any potentially infringing product into the state[919]. Specifically, tickets could not be ordered online, so that anyone wishing to make a purchase would have to telephone the box office in Missouri, only to find that the Missouri club did not mail tickets[920]. The purchaser would have to travel to Missouri to obtain the tickets[921]. Given the level of passivity, the court ruled that the website did not infringe Bensusan's trademark in New York[922]. The court observed that "the mere fact that a person can gain information on the allegedly infringing product is not the equivalent of a person advertising, promoting, selling or otherwise making an effort to target its product in New York."[923]

The decision in Bensusan case, which the Court of Appeals for the Second Circuit affirmed in September 1997[924], provided an important step toward the development of deeper legal analysis of Internet activity. Although the decision did not attempt to reconcile the *Inset* line of cases, it provided the groundwork for a new line of

[917] ibid
[918] ibid
[919] ibid
[920] ibid
[921] ibid
[922] ibid
[923] ibid
[924] Supra Note 913,Bensusan Rest. Corp. v. King, 126 F.3d 25, 29 (2d Cir. 1997)

cases[925]. By the end of 1996, however, the majority of Internet related decisions evidenced little genuine understanding of activity on the Internet. Rather, most courts were unconcerned with the jurisdictional implications of their rulings and instead favored an analogy based approach in which the Internet was categorized en masse[926]. This analogy-based approach by courts was ignoring the fact that Internet technology has offered a great platform for expressing one's view in an inexpensive way. In all these cases courts were interested in resolving jurisdictional problems and were unable to consider the rights of the cyberspace entities.

6.4 The Rise and fall of Zippo Test – Passive versus Active Test

A new approach to internet jurisdiction emerged with the decision of Pennsylvania district court decision in Zippo Manufacturing Co. v. Zippo Dot Com, Inc[927].It was with this decision that courts gradually began to appreciate that activity on the Internet was as varied as that in real space, and that all encompassing analogies could not be appropriately applied to this new medium. This realization again reinforces Lawrence Lessig argument for separate study for cyberlaw. In the above case, Zippo Manufacturing was a Pennsylvania based manufacturer of the well-known "Zippo" brand of tobacco lighters[928]. Zippo Dot Com was a California based Internet news service that used the domain name "Zippo.com" to provide access to

---

[925] For example in Hearst Corp. v. Goldberger, 15 (S.D.N.Y. Feb. 26, 1997), available at http://www.internetlibrary.com/cases/lib_case172.cfm , visited on 2 Feb 2003, the court relied heavily upon the Bensusan analysis in refusing to assert personal jurisdiction in a trademark infringement matter involving the domain name "Esqwire.com."In this case the court carefully reviewed Internet case law to that point, noted its disagreement with decisions such as Inset Systems etc cautioned that:

"Where, as here, defendant has not contracted to sell or actually sold any goods or services to New Yorkers, a finding of personal jurisdiction in New York based on an Internet website would mean that there would be nationwide (indeed, worldwide) personal jurisdiction over anyone and everyone who establishes an Internet website. Such nationwide jurisdiction is not consistent with traditional personal jurisdiction case law nor acceptable to the court as a matter of policy."

[926] Geist A,Michael , The Reality of Bytes: Regulating Economic Activity in the Age of the Internet, 73 WASH. L. REV. 521, 538 (1998).

[927] 952 F. Supp. 1119, 1126 (W.D. Pa. 1997) available at http://people.hofstra.edu/peter_j_spiro/cyberlaw/zippo.htm , visited on 17 Sep 2003

[928] ibid

Internet newsgroups[929]. Zippo Dot Com offered three levels of subscriber service—free, original, and super[930]. Those subscribers desiring the original or super level of service were required to fill out an online application form and submit a credit card number through the Internet or by telephone[931]. Zippo Dot Com's contacts with Pennsylvania occurred almost exclusively on the Internet because the company maintained no offices, employees, or agents in the state[932]. Dot Com had some success in attracting Pennsylvania subscribers; at the time of the action, approximately 3,000, or two percent of its subscribers, resided in that state[933]. Once again, the issue before the court was one of personal jurisdiction arising out of a claim of trademark infringement and dilution[934].

Rather than using Internet analogies as the basis for its analysis, the court focused on the prior, somewhat limited Internet case law[935]. The court, which clearly used the *Bensusan* decision for inspiration, determined that, although few cases had been decided, 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[936].

The court proceeded to identify a sliding scale based on Internet commercial activity:

"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 the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. At the opposite end are situations

---

[929] ibid
[930] ibid
[931] ibid
[932] ibid
[933] ibid
[934] ibid
[935] In Zippo case the court relied on court was Compuserve Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996). Although the *Zippo* court refers to the decision as an Internet case, in fact, the activity in question did not involve the use of the Internet. Rather, Patterson used Compuserve's proprietary network to dis-tribute certain shareware programs. Accordingly, Patterson's contacts with Ohio, Compuserve's headquarters and the location of the litigation, were confined to an offline contractual agreement and the posting of shareware on a Compuserve server that was avail-able to users of its proprietary network (not Internet users at large).

[936] 952 F. Supp. 1119, 1126 (W.D. Pa. 1997) available at http://people.hofstra.edu/peter_j_spiro/cyberlaw/zippo.htm, visited on 17 Sep 2003

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 who are interested in it is not grounds for the exercise of personal jurisdiction. The middle ground is occupied by interactive Web sites where users 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."[937]

Although the court may have conveniently interpreted some earlier cases to obtain its desired result, its critical finding was that the jurisdictional analysis in Internet cases should be based on the nature and quality of the commercial activity conducted on the Internet. There is a strong argument that prior to Zippo, jurisdictional analysis was based upon the mere use of the Internet. Courts relying solely on the inappropriate analogy between the Internet and advertisements developed a legal doctrine poorly suited to the reality of Internet activity. In the aftermath of the Zippo decision, Internet legal analysis underwent a significant shift in perspective[938].

The test laid down by the court in Zippo fails on many counts. First, the majority of websites 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 website.

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 data collection technologies behind the scenes without the knowledge of the individual

---

[937] ibid

[938] Geist A Michael , Is There A There There? Toward Greater Certainty For Internet Jurisdiction , Berkeley Technology Law Journal, Vol.16, Issue 16:3, Fall 2001 at p 27

user[939]. Given the value of personal data, its collection is properly characterized as active, regardless of whether it occurs transparently or surreptitiously[940]. Similarly, sites such as online chat rooms may appear to be active, yet courts have consistently characterized such sites as passive[941].

Third, it is important to note that the standards for what constitutes an active or passive website are constantly shifting. When the test was developed in 1997, an active website 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 with improved technology. In fact, it can be credibly argued that owners of websites must constantly reevaluate their positions on the passive versus active spectrum as web technology changes[942].

Fourth, the Zippo test is ineffective even if the standards for passive and active sites remain constant. With the expense of creating a sophisticated website being high, few organizations will invest in a website without anticipating some earning potential. Since revenue is typically the hallmark of active websites, most new sites are likely to feature interactivity, and therefore be categorized as active sites. 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 website because virtually all sites will meet the Zippo active benchmark[943].

In light of the ever changing technological environment and the shift toward predominantly active websites, the effectiveness of the *Zippo* doctrine is severely undermined no matter how it develops. If the test evolves with the changing

---

[939] Kang ,Jerry , Information Privacy in Cyberspace Transactions, 50 STAN. L. REV. 1193, 1226-29 (1998).

[940] Supra Note 921,Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1126 (W.D. Pa. 1997)

[941] Barrett v. Catacombs Press, 64 F. Supp. 2d 440 (E.D. Pa. 1999) , available at http://www.findlaw.com, visited on 18 May 2003

[942] Geist A Michael , Is There A There There? Toward Greater Certainty for Internet Jurisdiction, Berkeley Technology Law Journal, Vol.16, Issue 16:3, Fall 2001 at p 39

[943] ibid at p 45

technological environment, it fails to provide much needed legal certainty. On the other hand, if the test remains static to provide increased legal certainty, it risks becoming irrelevant as the majority of websites meet the active standard.[944]Therefore, we need to look for alternative tests.

The limitation of the Zippo doctrine was highlighted in Millennium Enterprises, Inc. v. Millennium Music L.P.,[945] a 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[946]. After canvassing numerous Internet jurisdiction cases decided in 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: that is, "deliberate action" within the forum state in the form of transactions between the defendant and residents of the forum or conduct of the defendant purposefully directed at residents of the forum state. This, in the court's view, is the "something more" that the Ninth Circuit intended in Cybersell and Panavision cases.[947]

6.5 The Effects-doctrine for Internet Jurisdiction

Another important doctrine used by US courts for the determination of personal jurisdiction is known as effects doctrine.

In the application of "effects doctrine" to the cases, the US Supreme Court asserted jurisdiction on the principle that the defendant knew that his action would be injurious to the plaintiff, therefore he must reasonably anticipate being haled into court where the injury occurred. The "effects" cases are of particular importance in

[944] ibid at p 64
[945] 33 F. Supp. 2d 907 (D. Or. 1999), available at http://www.internetlibrary.com/cases/lib_case178.cfm , visited on 20 May 2004
[946] ibid
[947] ibid

cyberspace because conduct in cyberspace often has effects in various jurisdictions[948].

Under this "effects" test approach, rather than examining the specific characteristics of a website and its potential impact, courts focused their analysis on the actual effects that the website had in the jurisdiction. Indeed, courts are now relying increasingly on the effects doctrine established by the United States Supreme Court in Calder v. Jones[949].

The effects doctrine holds that personal jurisdiction over a defendant is proper when: a) the defendant's intentional tortious actions b) expressly aimed at the forum state and c) cause harm to the plaintiff in the forum state, which the defendant knows is likely to be suffered[950]. In Calder case, a California entertainer sued a Florida publisher for libel in a California district court[951]. In ruling that personal jurisdiction was properly asserted, the Court focused on the effects of the defendant's actions[952]. Reasoning that the plaintiff lived and worked in California, spent most of her career in California, suffered injury to her professional reputation in California, and suffered emotional distress in California, the Court concluded that

---

[948] Kesan Jay, Personal Jurisdiction in Cyberspace: Brief Summary of Personal Jurisdiction Law, Learning Cyberlaw in Cyberspace available at http://www.cyberspacelaw.org/kesan/kesan1.html , visited on Mar 22, 2004

[949] 465 U.S. 783 (1984) available at http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=search&court=US&case=/us/465/783.html, visited on 23 May 2004.In this case the actress Shirley Jones who worked and lived in California brought a libel suit in California against a reporter and executive for the National Enquirer. The defendant had only been to California twice, and neither of these visits was connected in any manner with the Jones claim of libel. However, the court held that because Jones caused the story to the published which he knew would have a "potentially devastating impact . . the brunt of that injury would be felt by [plaintiff] in the state in which she lives and work and in which the National Enquirer has its largest circulation," the defendant must "reasonably anticipate being haled into court there." 465 U.S. at 784, 104 S.Ct. at 1484. The court in *Calder* emphasized was this was a case of an intentional tort that was highly foreseeable to cause damage in California. The court also found significant that the effects of the article were centered in California, both in the content of the story as well as where the harm would be suffered. Thus the *Calder* case is considered a classic effects case, because jurisdiction was based on the effects of the defendants conduct

[950] ibid
[951] ibid
[952] ibid

the defendant had intentionally targeted a California resident and thus it was proper to sue the publisher in that state[953]. Thus in effect doctrine court considered the effects created on defendant to assert personal jurisdiction over the plaintiff.

The application of the Calder test can be seen in the Internet context in Blakey v. Continental Airlines, Inc.,[954] an online defamation case involving an airline employee. The employee filed suit in New Jersey against her co-employees, alleging that they published defamatory statements 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[955]. The lower court granted the co-employees' motion to dismiss for lack of personal jurisdiction and entered summary judgment for the employer on the hostile work environment claim[956].

In reversing the ruling, the New Jersey Supreme Court found that defendants who published defamatory electronic messages with the knowledge that the messages would be published in New Jersey could properly be held subject to the state's jurisdiction[957]. The court applied the effects doctrine and held that while the actions causing the effects in New Jersey were performed outside the state, this did not prevent the court from asserting jurisdiction over a cause of action arising out of those effects[958].

The broader effects based analysis has moved beyond the defamatory tort action at issue in Calder case to a range of disputes including intellectual property and commercial activities. On the intellectual property front, Nissan Motor Co. Ltd. v.

---

[953] ibid

[954] 751 A.2d 538 (N.J. 2000) , available at http://lawlibrary.rutgers.edu/courts/supreme/a-5-99.opn.html, visited on 10 June 2004

[955] ibid

[956] ibid

[957] ibid

[958] ibid

Nissan Computer Corp[959] typifies the approach. The plaintiff, an automobile manufacturer, filed a complaint in a California district court against a Massachusetts based computer seller. In the complaint there was an allegation that the defendant altered the content of its "nissan.com" website to include a logo that was similar to the plaintiff's logo and links to automobile merchandisers and auto related portions of search engines. In considering the defendant's motion, the court relied on the effects doctrine, ruling that the defendant had intentionally changed the content of its website to exploit the plaintiff's goodwill and to profit from consumer confusion[960]. Moreover, since the plaintiff was based in California, the majority of the harm was suffered in the forum state[961]. The court rejected the defendant's argument that it was not subject to personal jurisdiction because it merely operated a passive website[962]. 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 decision in *Cybersell* and the requirement of "something more," . The court held that the defendant's conduct was deliberately and substantially directed toward the forum state[963].

Courts have also refused to assert jurisdiction in a number of cases where insufficient commercial effects were found. For example, in People Solutions, Inc. v. People Solutions, Inc.[964], 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 because the defendant owned a website that could be accessed and viewed by Texas residents[965]. The site featured several interactive pages that

---

[959] 89 F. Supp. 2d 1154 (C.D. Cal. 2000) ,available at http://www.internetlibrary.com/cases/lib_case292.cfm, visited 25 June 2004

[960] ibid
[961] ibid
[962] ibid
[963] ibid
[964] Quoted from Michael A. Geist , Is There A There There? Toward Greater Certainty for Internet Jurisdiction**,** Berkeley Technology Law Journal, Vol.16, Issue 16:3, Fall 2001 at p 30

[965] ibid at p 31

allowed customers to take and score performance tests, download product demonstrations, and order products online[966].

The court characterized the site as interactive but refused to assert jurisdiction over the matter[967]. Relying on evidence that no Texans had actually purchased from the website, the court held that "personal jurisdiction should not be premised on the mere possibility, with nothing more, that defendant may be able to do business with Texans over its website."[968] Instead, the plaintiff had to show that the defendant had "purpose-fully availed itself of the benefits of the forum state and its laws."[969]

Effects doctrine has its own limitations and hence cannot be applied to cyberspace under all circumstances. A country cannot enforce conduct occurring outside its borders without the willingness of other countries to cooperate or the ability to exercise its own coercive power to extraterritorially enforce its laws. To do so would create inter-sovereign conflict and technology enabled countries may be able to extend their enforcement jurisdiction beyond persons, things or activities that are present in the enforcing jurisdiction[970].

6.6 The Yahoo! France Case

The Yahoo case serves as an example of a nation struggling to exercise its laws in cyberspace[971]. Yahoo Inc., a California based company, provides internet users with access to online resources, including various communication tools, online forums, shopping services, personalized content and branded programming through its network properties. 'Yahoo auctions', is one of the applications offered through the service; it allows users to communicate through the use of service[972], to buy and sell

---

[966] ibid at 31
[967] ibid
[968] ibid
[969] ibid
[970] Adria,Allen , Internet Jurisdiction Today, Northwestern Journal of International Law & Business, Fall 2001, 82, 1

[971] See generally , Nazis, Libel, Porn- The Web's Legal Minefield, Reuters, Aug 11, 2000, available at http://www.zenet.com/intweek/stories/new/0,41586,261456,00.html, visited 10 Oct 2003
[972] Yahoo! Terms of Service, available at http://www.docs.yahoo.com/info/terms, visited on 4 Feb 2002

items in an online auction[973]. Auction items range from baseball collections, to antiques, to electronics, to automobiles and, until, recently to Nazi memorabilia[974].

Few cyber law cases have attracted as much attention as the *Yahoo! France* case, in which a French judge ordered the world's most popular and widely visited website to implement technical or access control measures blocking auctions featuring Nazi memorabilia from French residents[975]. Yahoo! reacted with alarm, maintaining that the French court could not properly assert jurisdiction over the matter[976]. Yahoo! noted that the company maintains dozens of country-specific websites, including a Yahoo.fr site customized for France that was free of Nazi-related content. These country specific sites target the local population in their local language, and endeavor to comply with all local laws and regulations[977].

The company argued that its flagship site, Yahoo.com, primarily targeted a United States audience. Since United States free speech laws protect the sale of Nazi memorabilia, the auctions were entirely lawful[978]. Moreover, the Yahoo.com site featured a terms of use agreement, which stipulated that the site was governed by United States law[979]. Since the Yahoo.com site was not intended for a French audience, and users implicitly agreed that United States law would be binding, the company felt confident that a French judge could not credibly assert jurisdiction over the site.

---

[973] An auction is a public sale in which the price is determined by bidding, and the item is sold to the highest bidder. A potential buyer participates by bidding on an item that the seller has listed. The person who has offered the highest bid at close of auction wins the right to purchase the item at that price. What is an Auction? Yahoo! Auctions Tour, at http://www.auctions.yahoo.com.phtml/auc/us/tour/0-1-whatis.html, visited on 21 Feb 2003

[974] See Yahoo! Auctions , available at http://www.list.auctions.yahoo.com, visited on 21 Feb 2003

[975] *See* Jim Hu & Evan Hansen, Yahoo Auction Case May Reveal Borders Of Cyberspace, CNET NEWS.COM, Aug. 11, 2000, at http://news.cnet.com/news/0-1005-200-2495751.html , visited o 11 Sep 2005 ("A warning to Internet companies doing business abroad: Local governments may have the power to impose restrictions even if your servers are in the United States.");

[976] ibid

[977] *See* Yahoo! Terms of Service, *at* http://docs.yahoo.com/info/terms , visited on 26 Nov 2003.

[978] Brendon Fowler et al., Can You Yahoo!? The Internet's Digital Fences, 2001 DUKE L. & TECH. REV. 12, 1, available *at* http://www.law.duke.edu/journals/dltr/articles/-2001dltr0012.html ,Visited on 25 Feb 2003

[979] See Yahoo! Terms of service at http://docs.yahoo.com/info/terms

Judge Jean-Jacques Gomez of the County Court of Paris disagreed, ruling that the court could assert jurisdiction over the dispute since the content found on the Yahoo.com site was available to French residents and was unlawful under French law[980]. Before issuing his final order, the judge commissioned an international panel to determine whether the technological means were available to allow Yahoo! to comply with an order to keep the prohibited content away from French residents. The panel reported that though such technologies were imperfect, they could accurately identify French Internet users at least seventy percent of the time[981]. Based on this report, Judge Gomez ordered Yahoo! to ensure that French residents could not access content that violated French law on the site. Failure to comply with the order would result in fines of 100,000 francs per day after a three month grace period[982].

Soon after, Yahoo! removed the controversial content from its site, but the company proceeded to contest the validity of the French court's order in a California court. In November 2001, the California court ruled in favor of Yahoo!, holding that the French judgment was unenforceable in the United States[983].

Yahoo argued and continues to argue that the auction sites involved in the Yahoo case were aimed at the American market and the US First amendment governing freedom of speech prevented it from shutting them down[984]. Though Yahoo later removed Nazi artifacts from its internet auction sites, it had decided not to drop its US suit over French ruling[985].

---

[980] The sale of Nazi items violates Article R645-1 of the French Penal Code. For translation of Article R645-1 of the French Penal Code see http://www.laores.net/html/codpen.html, visited on 25 Oct 2003

[981] UEJF et LICRA v. Yahoo! Inc. et Yahoo France, T.G.I. Paris, Nov. 20, 2000, N° RG: 00/05308 quoted from Michael A. Geist , Is There A There There? Toward Greater Certainty for Internet Jurisdiction**,** Berkeley Technology Law Journal, Vol.16, Issue 16:3, Fall 2001

[982] ibid

[983] Yahoo!, Inc. v. LICRA, C-00-21275 JF, 2001 U.S. Dist. LEXIS 18378 (N.D. Cal. Nov. 7, 2001), available at www.findlaw.com , visited on 20 Jan 2003

[984] Lawsuit Accuses Yahoo of justifying war crimes, REUTERS, 22 Jan. 2003 available at http://news.cnet.com/news/0-1007-200-4560537.html, visited 2 Mar 2003

[985] Lori Enos, Holocaust Survivors sue Yahoo! Over Nazi Auctions, E-commerce Times, 23 Jan 2003, available at http://www.ecommercetimes.com/perl/story/6923.html, visited 24 Feb 2003

Further Yahoo contended that Judge Gomez's order violates the First Amendment and the Communication Decency Act's (CDA) immunization of ISPs from liability to third party content[986]. The fact that Yahoo decided to remove Nazi items from its auction sites, thus appeasing the plaintiffs and the court order in the Yahoo case, does not mean that Yahoo has backed down from its original position: Yahoo will fight the ruling that threatens to pin "frontier-free internet back beyond international boundaries."[987]

The French government found Yahoo guilty of violating French law. In doing so, the French court took the position that 'no one should gain or lose rights merely by going online'[988]. According to this view, 'if Nazi artifacts cannot be sold offline, they should not be sold online'[989]. All existing legislation applies to internet users and a racist message circulated on the web is an offense just as it would be in a newspaper or on radio or television[990]. Because internet users in France have access to Yahoo's US site, indeed all websites, they must follow French law[991]. The problem that arises from this "when-in-Rome"[992] perception of internet jurisdiction is that it could lead to the conclusion that any court anywhere in the world has adjudicative jurisdiction over the author, publisher or provider of a web page[993]. Unlike traditional jurisdictional problems that might involve two or three conflicting jurisdictions, cyberlaw jurisdictional theorists are faced with the reality that a simple

---

[986] ibid
[987] Hate Foes Praise Yahoo Move, REUTERS, 3 Jan 2003 available at, http://www.wirednews.com/news/politics/0,1283,4095,00.html, visited on 25 Feb 2003
[988] Ariel Tam, Online Free of Speech is not So Free, ZDNet ASIA, Jan 22, 2001, available at http://www.ZDNET.com/zdnn/stories/news/0,4586,2677192,00.html, visited on 4 Feb 2002
[989] ibid
[990] David McGuire, Yahoo Decision Won't End Online Speech Debate, NEWSBYTES, 4 Jan 2002, available at http://www.newsbytes.com/news/01/16002.html, visited on 5 Feb 2002
[991] Pimm Fox, News Analysis: Can French Law be Imposed on an Internet Company? COMPUTERWORLD, Nov.28, 2000 , available at http://www.computerworld.com/cwi/s, visited on 4 Feb 2002
[992] The "when-in-Rome" rule refers to the concept that a country can have jurisdiction overall websites merely because they are accessible from the country
[993] Peritt H Henry, Jr., Jurisdiction and the Internet: Basic Anglo/American Perspectives Projects in the coming 2000's, Internet law and Policy Forum, available at http://www.ilpf.org/confer/present99/perrittpr.htm visited Feb 16, visited on 23 July 2003

web page could be subject to jurisdiction by all of the nearly three hundred sovereigns around the world[994].

If we were to apply traditional jurisdictional principles to the Yahoo case, the case satisfies many of the bases for French perspective jurisdiction. According to the facts of the Yahoo case, France has the authority to prescribe its laws on cyberspace. First, subjective territoriality exists because Nazi items, in violation of Article R645-1, were being offered in France[995]. Second, objective territoriality is satisfied because, even if it was determined that the sale of Nazi items took place either in cyberspace, or the location of the seller, the primary effect of the transaction was felt in France[996]. Third, France has jurisdiction over French citizens that are buying Nazi memorabilia[997]. Fourth, the passive nationality theory applies because the victims of a breach of Article R645-1 are thought to be French citizens, some of which are holocaust survivors, offended by the sale of Nazi artifacts[998].Fifth, the victim in the Yahoo! case could be viewed not only as French citizens, but also as France itself, giving France jurisdiction to prescribe its laws over the internet based on the protective principle theory[999]. Finally, though it is not applicable to this case, universal interest jurisdiction could be expanded to Internet law to deal with such areas as internet piracy, computer hacking and viruses[1000].

The traditional model of international jurisdiction would validate the French Tribunals order in the Yahoo! case. A conclusion, such as this, could have far reaching implications for the development of the internet and the future of cyber law. Internet jurisdiction is a subject of increasing debate. Opinions worldwide are "split between civil libertarians who want to uphold the freedom of internet speech

---

[994] Menthe Darrel, Jurisdiction in Cyberspace: A theory of International Spaces, 4 Mich.Telecom.Tech.L.Rev. 69(1998) available at http://www.mttlr.org/volfour/menthe.html, visited on Feb 25, 2004

[995] The sale of Nazi items violates Article R645-1 of the French Penal Code. For translation of Article R645-1 of the French Penal Code see http://www.laores.net/html/codpen.html, visited on 25 Oct 2003

[996] Menthe Darrel, Jurisdiction in Cyberspace: A theory of International Spaces, 4 Mich.Telecom.Tech.L.Rev. 69(1998) available at http://www.mttlr.org/volfour/menthe.html, visited 25 on Feb 2004

[997] ibid

[998] ibid

[999] ibid

[1000] ibid.

at all costs and lawyers and governments trying to find practical compromise that respects the open nature of the web whilst protecting vulnerable people."[1001] The internet's extraordinary growth and distinct ability to make information available to anyone, anywhere in the world with Internet access, has taken traditional national sovereignty by surprise[1002]. While nations are trying to maintain sovereignty in cyberspace, companies, such as Yahoo, fear that the Yahoo case will be used as precedent, forcing web sites to "self-police all online content and activities and make them comply with any number of laws from any country or community."[1003]

6.7 Tackling Internet Jurisdictional Problems

Goldsmith asserts that regulation of cyberspace is both feasible and legitimate from the perspective of traditional jurisdiction and choice of law[1004].He claims that enforceability will operate for cyberspace in the same way as in real space. Rather than being simultaneously subjects to all national regulations, internet users will have to concern themselves with countries that are able to enforce their laws across geographic boundaries[1005]. In the Yahoo case, the California based corporation has a subsidiary company operating in France, which could be used by France to enable enforcement of French law. However, as seen by the expert's proposal in the Yahoo case, as technology increases, the threat of liability will lesson[1006]. As we have seen in Napster case, court order was enforced but in the Grokster case court order can not be enforced because of lack of physical location.

[1001] Adria, Allen , Internet Jurisdiction Today, Northwestern Journal of International Law & Business, Fall 2001, 22, 1

[1002] See generally Reno V ACLU, 521 US 844(1997)

[1003] Kenneth N Cukier, Virtual Exceptionalism: Cyberspace Meets Sovereignty, Wall Street Journal, Aug 6, 2000 at page 6

[1004] Goldsmith L Jack., Against Cyberanarchy, 65 U.Chi.L.Rev 1199 (1998), available at http://eon.law.harvard.edu/property00/jurisidction/cyberanarchy.html, visited on 20 Feb 2004. Though Goldsmith argues that regulation from the perspective of jurisdiction and choice of law is "legitimate and feasible", he does not argue that it is a good idea, and does not take a position on the merits beyond their jurisdictional legitimacy. Further, Goldsmith does not rule out the fact that the new cyberspace will lead to changes in governmental regulation in the same way that the radio , television and satellite gave way to social and regulatory change.

[1005] ibid

[1006] ibid, "The threat of liability will lessen as content providers continue to gain means to control information flows" at, 1221

Skeptics overstate the challenges posed on traditional international jurisdiction by the Internet[1007]. First, the practical problems of jurisdiction will diminish when the substantive content of law in different sovereigns is the same. When harmonization is not an option, the problems may be complex and genuine[1008]. However, Goldsmith asserts that they are not unique to cyberspace. Though the new medium is 'richer, more complex and much more efficient, it is not different than other forms of transnational communication[1009]. Transactions over the internet either involve real people in one territorial jurisdiction transacting with real people in other territorial jurisdictions, or engaging in activity that causes real world effects in another territorial jurisdiction[1010].

6.7.1 Targeting Test for Internet jurisdiction

Targeting test can be used to resolve internet jurisdictional problems. It focuses on three factors: contract, technology and actual or implied knowledge[1011].

A targeting approach is not a novel idea. Several United States courts have factored targeting considerations into their jurisdictional analysis of Internet-based activities. For example, in Bancroft & Masters, Inc. v. Augusta National Inc[1012]., a dispute over the "masters.com" domain name, the Ninth Circuit considered targeting to be the "something more" required when applying an effects based analysis:

> We have said that there must be "something more," but have not spelled out what that something more must be. We now conclude that "something more" is what the Supreme Court described as "express aiming" at the forum state. Express aiming is a concept that in the jurisdictional context hardly defines itself. From the available cases, we deduce that the requirement is satisfied when the defendant is alleged to have engaged in

[1007] ibid at p 1240
[1008] ibid
[1009] ibid
[1010] ibid
[1011] Geist A Michael A. , Is There A There There? Toward Greater Certainty for Internet Jurisdiction**,** Berkeley Technology Law Journal, Vol.16, Issue 16:3, Fall 2001 at p 56
[1012] 223 F.3d 1082 (9th Cir. 2000) available at http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=9th&navby=case&no=9915099, visited 6 Jan 2005

> wrongful conduct targeted at a plaintiff whom the defendant knows to be a resident of the forum state.[1013]

Targeting based analysis has also become increasingly prevalent among international organizations seeking to develop global minimum legal standards for e-commerce. The OECD Consumer Protection Guide-lines refer to the concept of targeting, stating that "business should take into account the global nature of electronic commerce and, wherever possible, should consider various regulatory characteristics of the markets they target."[1014]

Similarly, a recent draft of the Hague Conference on Private International Law's Draft Convention on Jurisdiction and Foreign Judgments includes provisions related to targeting[1015]. During negotiations over the e-commerce implications of the draft convention in Ottawa in February 2001, delegates focused on targeting as a means of distinguishing when consumers should be entitled to sue in their home jurisdiction. Version 0.4a of Article 7 (3)(b) includes a provision stating, "activity by the business shall not be regarded as being directed to a State if the business demonstrates that it took reasonable steps to avoid concluding contracts with consumers habitually resident in that State."[1016]

Targeting also forms the central consideration for securities regulators assessing online activity. As the United States Securities and Exchange Commission stated in its release on the regulation of Internet based offerings:

> "We believe that our investor protection concerns are best ad-dressed through the implementation by issuers and financial service providers of precautionary measures that are reasonably de-signed to ensure

---

[1013] ibid

[1014] Organization for Economic Cooperation and Development, Recommendation of the OECD Council Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce, at 5, *at* http://www.oecd.org/dsti/sti/it/consumer/prod/-CPGuidelines_final.pdf, visited 26 Nov 2004

[1015] Hague Conference on Private International Law, Preliminary Draft Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters, Oct. 30, 1999, available *at* http://www.hcch.net/e/conventions/draft36e.html, visited on 2 Jul 2003

[1016] ibid

> that offshore Internet offers are not targeted to persons in the United States or to U.S. persons"[1017]

The American Bar Association Internet Jurisdiction Project, a global study on Internet jurisdiction released in 2000, also recommended targeting as one method of addressing the Internet jurisdiction issue[1018]. It was noted in the report:

> "Entities seeking a relationship with residents of a foreign forum need not themselves maintain a physical presence in the forum. A forum can be "targeted" by those outside it and desirous of benefiting from a connecting with it via the Internet . . . . Such a chosen relationship will subject the foreign actor to both personal and prescriptive jurisdiction, so a clear understanding of what constitutes targeting is critical"[1019].

It is the ABA's last point that a clear understanding of what constitutes targeting is critical that requires careful examination and discussion. Without universally applicable standards for assessment of targeting in the online environment, a targeting test is likely to leave further uncertainty in its wake. For example, the ABA's report refers to language as a potentially important determinant for targeting purposes. That criterion overlooks the fact that the development of new language translation capabilities may soon enable website owners to display their site in the language of their choice, safe in the knowledge that visitors around the world will read the content in their own language through the aid of translation technologies[1020].

[1017] ibid

[1018] *See* American Bar Association, Achieving Legal and Business Order in Cyber-space: A Report on Global Jurisdiction Issues Created By the Internet , available at www.abanet.org, visited on 2 Feb 2003

[1019] ibid

[1020] ibid

6.8 Components of Targeting Test

Targeting as the litmus test for Internet jurisdiction is only the first step in the development of a consistent test that provides increased legal certainty. The second, more challenging step is to identify the criteria to be used in assessing whether a website has indeed targeted a particular jurisdiction. This step is challenging because the criteria must meet at least two important standards. First, the criteria must be technology neutral so that the test remains relevant even as new technologies emerge. This would seem to disqualify criteria such as a website language or currency, which are susceptible to real time conversion by newly emerging technologies. In the case of real time conversion language, a Greek website, which might otherwise be regarded as targeting Greece, could be instantly converted to English, and therefore rendered accessible to a wider geographic audience[1021].

Second, the criteria must be content neutral so that there is no apparent bias in favor of any single interest group or constituency. Several business groups are currently lobbying for a "rule of origin" approach under which jurisdiction would always rest with the jurisdiction of the seller[1022]. Consumer groups, meanwhile, have lobbied for a "rule of destination" approach that ensures that consumers can always sue in their home jurisdiction[1023]. The origin versus destination debate has polarized both groups, making it difficult to reach a compromise that recognizes that effective consumer protection does not depend solely on which law applies, while also acknowledging, as the court did in Stomp Inc. v. Neato L.L.C[1024]., that business must shoulder some of the risk arising from e-commerce transactions.

[1021] Geist A Michael A., Is There A There There? Toward Greater Certainty for Internet Jurisdiction**,** Berkeley Technology Law Journal, Vol.16, Issue 16:3, Fall 2001 at p 64

[1022] See for example,, Global Business Dialogue on Electronic Commerce, available *at* http://www.gbde.org, visited 26 Nov. 2005

[1023] See, for example,, Consumers International, *at* http://www.consumersinternational.org , visited on 16 Oct. 2005

[1024] 61 F. Supp. 2d 1074, 1080-81 (C.D. Cal. 1999) available at http://www.ecjlaw.com/CM/InternetandTechnologyLawReporter/InternetandTechnologyLawReporte

To identify the appropriate criteria for a targeting test, we must ultimately return to the core jurisdictional principle, foreseeability. Foreseeability should not be based on a passive versus active website matrix. Rather, an effective targeting test requires an assessment of whether the targeting of a specific jurisdiction was itself foreseeable. Foreseeability in that context depends on three factors: contracts, technology, and actual or implied knowledge. Forum selection clauses found in website terms of use agreements or transactional clickwrap agreements allow parties to mutually determine an appropriate jurisdiction in advance of a dispute. They therefore provide important evidence as to the foreseeability of being haled into the courts of a particular jurisdiction. Newly emerging technologies that identify geographic location constitute the second factor. These technologies, which challenge widely held perceptions about the Internet's architecture, may allow website owners to target their content to specific jurisdictions or engage in "jurisdictional avoidance" by "de-targeting" certain jurisdictions. The third factor, actual or implied knowledge, is a catch-all that incorporates targeting knowledge gained through the geographic location of tort victims, offline order fulfillment, financial intermediary records, and web traffic[1025].

Although all three factors are important, no single factor should be de-terminative. Rather, each must be analyzed to adequately assess whether the parties have fairly negotiated a governing jurisdiction clause at a private contract level, whether the parties employed any technological solutions to target their activities, and whether the parties knew, or ought to have known, where their online activities were occurring. While all three factors should be considered as part of a targeting analysis, the relative importance of each will vary. Moreover, in certain instances, some factors may not matter at all. For example, a defamation action is unlikely to

---

r206.asp , visited on 24 Feb 2004; See generally for clickwrap contracts, Rowland, Diane, Information Technology Law, Cavendish Publishing Ltd, London, 1997

[1025] Geist A Michael , Is There A There There? Toward Greater Certainty for Internet Jurisdiction, Berkeley Technology Law Journal, Vol.16, Issue 16:3, Fall 2001 at p 60

involve a contractual element, though evidence from the knowledge factor is likely to prove sufficient to identify the targeted jurisdiction[1026].

It is important to also note that the targeting analysis will not determine exclusive jurisdiction, but rather identify whether a particular jurisdiction can be appropriately described as having been targeted. The test does not address which venue is the most appropriate of the jurisdictions that meet the targeting threshold[1027].

Contract is the first of the three factors for the recommended targeting test considers whether either party has used a contractual arrangement to specify which law should govern. Providing parties with the opportunity to limit their legal risk by addressing jurisdictional concerns in advance can be the most efficient and cost effective approach to dealing with the Internet jurisdiction issue. The mere existence of a jurisdictional clause within a contract, however, should not, in and of itself, be determinative of the issue, particularly when consumer contracts are involved. In addition to considering the two other targeting factors, the weight accorded to an online contract should depend upon the method used to obtain assent and the reasonableness of the terms contained in the contract.

Courts in the United States have upheld the per se enforceability of an online contract, commonly referred to as a click-wrap agreement[1028]. These agreements typically involve clicking on an "I agree" icon to indicate assent to the agreement. Given their ubiquity, it should come as little surprise to find that courts have been anxious to confirm their enforceability. For example, in the 1999 Ontario case of Rudder v. Microsoft Corp.,[1029] the court upheld a forum selection clause contained in an electronic ISP Terms of Service Agreement. The court feared that not upholding the clause would not only fail to advance the goal of "commercial

[1026] ibid
[1027] ibid
[1028] Gringras , Clive, The Laws of the Internet, Butterworth, London, 1997

[1029] Rudder V Microsoft , NO. 97-CT-046534CP,Ontario Superior Court Of Justice, available at http://aix1.uottawa.ca/~geist/microsoft.htm , visited on 24 Feb 2004; But contrary to this Indian courts have taken the view that the parties to the suit cannot confer jurisdiction on courts. Either it must be through the Constitution or statutory enactment.

certainty," but would also move this type of electronic transaction into the realm of commercial absurdity. The court further feared that it would lead to chaos in the marketplace, "render ineffectual electronic commerce and undermine the integrity of any agreement entered into through this medium."[1030]

Contracts must clearly play a central role in any determination of jurisdiction targeting since providing parties with the opportunity to set their own rules enhances legal certainty. As the cases decided by US courts suggest, however, contracts do not provide the parties with absolute assurance that their choice will be enforced, particularly in a consumer context. Rather, courts must engage in a detailed analysis of how consent was obtained as well as consider the reasonableness of the terms. The results of that analysis should determine what weight to grant the contractual terms when balanced against the remaining two factors of the proposed targeting analysis.

Technology as the second targeting factor focuses on the use of technology to either target or avoid specific jurisdictions. Just as technology originally shaped the Internet, it is now reshaping its boundaries by quickly making geographic identification on the Internet a reality[1031]. The rapid emergence of these new technologies challenges what has been treated as a truism in cyber law- that the Internet is borderless and thus impervious to attempts to impose on it real space laws that mirror traditional geographic boundaries[1032].

Courts have largely accepted the notion that the Internet is borderless as reflected by their reluctance to even consider the possibility that geographic mapping might be

---

[1030] ibid

[1031] Software companies like Infosplit and NetGeo claims to have the ability to accurately pinpoint the location of any IP address using a proprietary set of techniques and algorithms. The technology provides instant and precise geographic identification and page routing in a process invisible to the web user. The companies maintain that its technology accurately determines the country of origin with 98.5% accuracy, the state or province with 95% accuracy, and the city with 85% accuracy, and that it can even accurately determine user location for users of national or global ISPs such as AOL. *See* Infosplit, *at* http://www.infosplit.com , visited Nov. 26, 2004 and NetGeo, *at* http://www.netgeo.com , visited 26 Nov. 2004.

[1032] David R. Johnson & David G. Post, *Law and Borders*: *The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

possible online. In American Libraries Association v. Pataki[1033], a Commerce Clause challenge to a New York state law targeting Internet content classified as obscene, the court characterized geography on the Internet and observed as follows;

> "The Internet is wholly insensitive to geographic distinctions. In almost every case, users of the Internet neither know nor care about the physical location of the Internet resources they access. Internet protocols were designed to ignore rather than document geographic location; while computers on the network do have "addresses," they are logical addresses on the network rather than geographic addresses in real space. The majority of Internet addresses contain no geographic clues and, even where an Internet address provides such a clue, it may be misleading"[1034].

Although the court's view of the Internet in the above case may have been accurate in 1997, the Internet has not remained static. Providers of Internet content increasingly care about the physical location of Internet resources and the users that access them, as do legislators and courts who may want real space limitations imposed on the online environment[1035]. A range of companies have responded to those needs by developing technologies that provide businesses with the ability to reduce their legal risk by targeting their online presence to particular geographic constituencies. These technologies also serve the interests of governments and regulators who may now be better positioned to apply their offline regulations to the online environment[1036].

Given the development of new technologies that allow for geographic identification with a reasonable degree of accuracy, a targeting test must include a technology component that places the onus on the party contesting or asserting jurisdiction to demonstrate what technical measures, including offline identifiers, it employed to

---

[1033] American. Libraries Ass'n v. Pataki, 969 F. Supp. 160 (S.D.N.Y. 1997) , available at www.findlaw.com , visited on 24 Feb 2004;

[1034] ibid

[1035] Bob Tedeschi, E-commerce: Borders Returning to the Internet, N.Y. TIMES, Apr. 2, 2001 visited on 24 Feb 2004

[1036] Goldsmith L Jack & Sykes O,Alan s, The Internet and the Dormant Commerce Clause, 110 YALE L.J. 785, 810-12 (2001).

either target or avoid a particular jurisdiction. The suitability of such an onus lies in the core consideration of jurisdiction law—that is, whether jurisdiction is foreseeable under the circumstances. Geography identifying technologies provide the party that deploys the technology with a credible answer to that question at a cost far less than comparable litigation expenses. Since parties can identify who is accessing their site, they can use technical measures to stop people from legally risky jurisdictions, including those jurisdictions where a site owner is reluctant to contest potential litigation or face regulatory scrutiny. Fair and balanced targeting jurisdiction test demands it as a requirement.

Actual or implied knowledge of parties is the third and last factor that can be used to identify the jurisdiction based upon targeting. This factor assesses the knowledge the parties had or ought to have had about the geographic location of the online activity. Although some authors have suggested that the Internet renders intent and knowledge obsolete by virtue of the Internet's architecture[1037], the geographic identification technologies available nowadays do not support this view. This factor ensures that parties cannot hide behind contracts and/or technology by claiming a lack of targeting knowledge when the evidence suggests otherwise.

The relevance of a knowledge based factor extends beyond reliance on contracts that the parties know to be false. In an e-commerce context, the knowledge that comes from order fulfillment is just as important. For example, sales of physical goods such as computer equipment or books, provide online sellers with data such as a real space delivery address, making it relatively easy to exclude jurisdictions that the seller does not wish to target. Courts have also begun to use a knowledge based analysis when considering jurisdiction over intellectual property disputes. In

[1037] *See, e.g.,* Martin H. Redish, Of New Wine and Old Bottles: Personal Jurisdiction, The Internet, and the Nature of Constitutional Evolution, 38 JURIMETRICS J. 575 (1998). Redish notes: The most effective defense of an Internet exception to the purposeful availment requirement is not that state interest should play an important role only in Internet cases, but rather that the technological development of the Internet effectively renders the concept of purposeful availment both conceptually incoherent and practically irrelevant. An individual or entity may so easily and quickly reach the entire world with its messages that it is simply not helpful to inquire whether, in taking such action, that individual or entity has consciously and carefully made the decision either to affiliate with the forum state or seek to ac-quire its benefits.

Starmedia Network v. Star Media, Inc.,[1038], the court asserted jurisdiction over an alleged out-of state trademark infringer, noting that:

> "the defendant knew of plaintiff's domain name before it registered 'starmediausa.com' as its domain name. Therefore, the defendant knew or should have known of plaintiff's place of business, and should have anticipated being haled into New York's courts to answer for the harm to a New York plaintiff caused by using a similar mark."[1039]

But the application of the knowledge principle is more complex when the sale involves digital goods for which there is no offline delivery; the seller is still customarily furnished with potentially relevant information.

Under the three-factor targeting test, it is important to note that no single factor is determinative. Analysis will depend on a combined assessment of all three factors in order to determine whether the party knowingly targeted the particular jurisdiction and could reasonably foresee being haled into court there. In an e-commerce context, the targeting test ultimately establishes a trade-off that should benefit both companies and consumers. Companies benefit from the assurance that operating an e-commerce site will not necessarily result in jurisdictional claims from any jurisdiction worldwide. They can more confidently limit their legal risk exposure by targeting only those countries where they can comply with domestic law.

6.9 Conclusion

Enjoyment of human rights in cyberspace will become ineffective, if they cannot be suitably enforced in the real world. Enforcement of the right actually determines the importance accorded to such rights by the State. In this regard enforcement mechanism for human rights assumes greater significance. Even though there are difficulties in determining jurisdiction and other related problems the assurance that

---

[1038] 2001 WL 417118 (S.D.N.Y. ,2001), available at http://209.85.175.104/search?q=cache:6irthx4qlc4J:www.nysd.uscourts.gov/courtweb/pdf/D02NYSC/01-04910.PDF+starmedia+network+v+star+media+inc&hl=en&ct=clnk&cd=1&gl=in , visited on 2 Feb 2004

[1039] ibid

netizens claims and rights will be enforced in cyberspace, would promote the interest of the network community. Promotion and protection of human rights of the cyberspace entities would usher a new era in the information age.

Resolving jurisdictional problems assumes greater significance for the enforcement of human rights in cyberspace. For most human rights violations, plaintiff must have an opportunity to institute the proceedings against defendant in his place. The 'destination theory' is more favored for finding the jurisdiction in human right violations.The establishment of European Human Rights Court which enforces human rights violations in EU member countries provides us the basis for establishing a international human rights court for the enforcement of human rights violations in cyberspace.

Multiple bases for the assertion of personal and prescriptive jurisdiction obviously lead to multiple fora with internationally and constitutionally proper jurisdiction over actors and their conduct. Jurisdictional principles can inform business decision making; knowledge that certain uses of technology may result in a distant court asserting jurisdiction and judging conduct under its own law, rendering a judgment a business' home forum would enforce, may determine what uses of technology a business undertakes. But jurisdictional principles can only acknowledge the reality that multiple laws, enforceable by multiple courts, may apply to the same conduct; it can not resolve whatever economic dislocations are caused by that reality[1040].

However, no regime of regulation or of dispute resolution has ever pretended to be the sole source to which parties turn to ease business intercourse. In every culture and in every time, private arrangements as well as governmental activity have attempted to reduce the occasions of conflict necessitating the exercise of judicial decision-making. The economic world of Cyberspace at the beginning of the 21st century is no different. Trade depends on confidence: confidence on the part of the buyer that goods or services will conform to legitimate expectations, and confidence

[1040] Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet. Report of the American Bar Association ("ABA") Jurisdiction in Cyberspace Project empanelled in 1998 under the title, "Transnational Issues in Cyberspace: A Project on the Law Relating to Jurisdiction." , available at www.abanet.org , visited on 14 Mar 2003

on the part of the seller that payment will be prompt and complete. Such confidence, in the interests of all parties, is fostered by industry self-regulation that reflects an honest attempt to identify and resolve potential conflicts before they arise. The forms of such regulation are many and are being actively explored as e-commerce becomes an increasingly important segment of the global economy. They include voluntary codes of conduct, the provision of private arbitration for the resolution of disputes, escrow accounts, agreements between buyers, sellers and credit card companies etc.

Beyond private ordering[1041] the harmonization of substantive laws across state and national lines can obviate at least one of the jurisdictional issues, that of prescriptive jurisdiction. To the extent the law of all fora related in any way to the dispute is the same, it matters little which is applied. In many instances, of course, such harmonization will be exceedingly difficult; different states, with different understandings of the needs and rights of those they protect, will argue for very different results with respect to such things as consumer protection, gambling, libel etc. On the other hand, there is likely to be agreement that fraud in an offering of securities is to be prevented. The greater the common understanding, even if laws are not identical, the greater is the likelihood that differences will matter little to the parties; compliance with both will flow more easily from compliance with one.[1042]

[1041] Private ordering is designed, of course, to avoid the need for litigation, but as cases considering the validity of contractual choice of forum and law clauses demonstrate, the judiciary can only remain uninvolved if both parties choose it to remain so.

[1042] States that share such common understandings may also be more willing to defer to contractual choices of a sharing state's law. *See* David R. Johnson, Susan P. Crawford, and Samir Jain, Deferring to Contractual Choices of Law and Forum to Protect Consumers (and vendors) in Ecommerce, available at http://www.kentlaw.edu/cyberlaw/docs/drafts/crawford.html, visited 23 Mar 2003