IS THERE A THERE THERE? TOWARD GREATER CERTAINTY FOR INTERNET JURISDICTION

By Michael A. Geist[†]

ABSTRACT

The unique challenge presented by the Internet is that compliance with local laws is rarely sufficient to assure a business that it has limited its exposure to legal risk. Since websites are accessible worldwide, the prospect that a website owner might be haled into a courtroom in a far-off jurisdiction is much more than a mere academic exercise, it is a very real possibility.

The article identifies why the challenge of adequately accounting for the legal risk arising from Internet jurisdiction has been aggravated in recent years by the adoption of the *Zippo* legal framework, commonly referred to as the passive versus active test. The test provides parties with only limited guidance and often results in detrimental judicial decisions from a policy perspective.

Given the inadequacies of the *Zippo* passive versus active test, it is now fitting to identify 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.

The solution submitted in the article is to move toward a targeting-based analysis. Unlike the *Zippo* approach, a targeting analysis would

---

† Assistant Professor, University of Ottawa Faculty of Law, and Director of E-Commerce Law, Goodmans LLP. The author would like to thank the Uniform Law Conference of Canada and Industry Canada for their financial support in sponsoring this paper; Teresa David and William Karam for their research assistance; Vaso Maric, Rene Geist, Harvey Goldschmid, Ted Killheffer, Denis Rice, as well as the participants at the Consumer Measures Committee/Uniform Law Conference of Canada April 2001 Workshop on Consumer Protection and Jurisdiction in Electronic Commerce, the TPRC 2001 Conference, and the Georgetown University Advanced E-commerce Institute, for their comments on earlier versions of this paper; the editors of the BERKELEY TECHNOLOGY LAW JOURNAL for their excellent work in bringing this paper to publication; and to Allison Geffen for her continued love and support. Any errors or omissions remain the sole responsibility of the author.

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 an effects analysis, the source of considerable uncertainty since Internet-based activity can ordinarily be said to create some effects in most jurisdictions.

TABLE OF CONTENTS

I. INTRODUCTION

> 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.[1]
>
> - Judge Nancy Gertner, Digital Equipment Corp. v. Altavista Technology, Inc., 1997

1. Digital Equip. Corp. v. Altavista Tech., Inc., 960 F. Supp. 456, 462 (D. Mass. 1997).

> We order the company YAHOO! Inc. to take all measures to dissuade and make impossible any access via Yahoo.com to the auction service for Nazi objects and to any other site or service that may be construed as constituting an apology for Nazism or contesting the reality of Nazi crimes . . . [2]
>
> - Judge Jean-Jacques Gomez, UEJF et LICRA v. Yahoo! Inc. et Yahoo France, May 2000

As business gravitated to the Internet in the late 1990s, concern over the legal risks of operating online quickly moved to the fore, as legal issues inherent in selling products, providing customer service, or simply maintaining an information-oriented website began to emerge.[3] Certain legal risks, such as selling defective products or inaccurate information disclosure, were already well-known to business, as these risks are encountered and addressed daily in the offline world.[4]

The unique challenge presented by the Internet is that compliance with local laws is rarely sufficient to assure a business that it has limited its exposure to legal risk. Since websites are instantly accessible worldwide, the prospect that a website owner might be haled into a courtroom in a far-off jurisdiction is much more than a mere academic exercise; it is a very real possibility.[5] Businesses seeking to embrace the promise of a global market at the click of a mouse must factor into their analysis the prospect of additional compliance costs and possible litigation.

The risks are not limited to businesses, however. Consumers anxious to purchase online must also balance the promise of unlimited choice, greater access to information, and a more competitive global marketplace with the fact that they may not benefit from the security normally afforded by local consumer protection laws. Although such laws exist online, just as they do offline, their effectiveness is severely undermined if consumers

---

2. Yahoo!, Inc. v. LICRA, C-00-21275 JF, 2001 U.S. Dist. LEXIS 18378, at *6, 7 (N.D. Cal. Nov. 7, 2001) (citing the French court's decision in UEJF et LICRA v. Yahoo! Inc. et Yahoo France).

3. *See*, *e.g.*, Louis Trager, *Unhappy Holidays at Toys "R" Us,* ZDNET INTERACTIVE WK., January 12, 2000, *at* http://www.zdnet.com/filters/printerfriendly/0,6061,2421416-35,00.html.

4. *See, e.g.*, Cornell Law School Legal Information Institute, Products Liability Law: An Overview, *at* http://www.law.cornell.edu/topics/products_liability.html (last visited Nov. 26, 2001).

5. *See, e.g.*, UEJF et LICRA v. Yahoo! Inc. et Yahoo France, T.G.I. Paris, May 22, 2000, N° RG: 00/05308 [hereinafter *Yahoo!France*]; *see also* Braintech, Inc. v. Kostiuk, [1999] 171 D.L.R. (4th) 46, 63-64 (B.C.C.A.) (translated by Richard Salis).

do not have recourse within their local court system or if enforcing a judgment requires further proceedings in another jurisdiction.[6]

Moreover, concerns over the legal risks created by the Internet extend beyond commercial activities. Public interest information-based websites on controversial topics may face the prospect of prosecution in far-away jurisdictions despite their legality within the home jurisdiction.[7] Meanwhile, anonymous posters to Internet chat sites face the possibility that the target of their comments will launch legal action aimed at uncovering their anonymous guise.[8]

In recent years, adoption of the *Zippo* legal framework has exacerbated the challenge of adequately accounting for the legal risk arising from Internet jurisdiction.[9] In the *Zippo* framework, commonly referred to as the passive versus active test, courts gauge the relative interactivity of a website to determine whether assertion of jurisdiction is appropriate. At one end of the spectrum lies "passive" websites—minimally interactive information-based websites.[10] At the other end of the spectrum lies "active" websites, which feature greater interactivity and end-user contacts.[11] The *Zippo* test suggests that courts should refrain from asserting jurisdiction over passive sites, while jurisdiction over active sites is appropriate. The test has proven to be largely unhelpful as it provides parties with only limited guidance and often results in detrimental judicial decisions from a

---

6. The U.S. Federal Trade Commission has noted:

> Shifting to a pure country-of-origin approach to address challenges inherent in the current system risks undermining consumer protection, and ultimately consumer confidence in e-commerce. The same would be true under a "prescribed-by-seller" approach to the extent it would allow contractual choice-of-law and choice-of-forum provisions dictated by the seller to override the core protections afforded to consumers in their home country or their right to sue in a local court.

United States Federal Trade Commission, Bureau of Consumer Protection, Consumer Protection in the Global Electronic Marketplace: Looking Ahead (Staff Report), *available at* http://www.ftc.gov/bcp/icpw/lookingahead/electronicmkpl.pdf (Sept. 2001).

7. *See Yahoo!France*, *supra* note 5*; see also Yahoo! Ordered To Bar French from Nazi Sites*, REUTERS, Nov. 20, 2000, *available at* http://www.zdnet.co.uk/news/2000/-46/ns-19192.html.

8. In Canada, see *Irwin Toy Ltd. v. Doe* [2000] O.J. No. 3318 (Ont.). In the United States see *J. Erik Hvide v. "John Does 1-8,"* No. 99-22831-CA01 (Fla. Cir. Ct. Jun. 14, 2001). *See also* John Doe, also known as Aquacool_2000 v. Yahoo! Inc., No. 00-20677 (Cal. Super. Ct. filed May 11, 2000); *see generally* C. S. Kaplan, *Judge Says Online Critic Has No Right To Hide*, N.Y. TIMES CYBER L. J., June 9, 2000 (on file with author).

9. Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1122-23 (W.D. Pa. 1997).

10. *Id.* at 1124.

11. *Id.* at 1127.

policy perspective. As courts start to break free from the passive versus active test, they have begun to shift toward an equally problematic effects-based approach that potentially grants jurisdiction to every court in the world.[12]

Yahoo.com France[13] and *iCraveTV*[14] are two recent cases involving Internet jurisdiction that illustrate the difficulties with the current test. In these two cases, international jurisdictional issues combine with complicated fact patterns to demonstrate the limitations of the *Zippo* test.

A. The *Yahoo.com France* case

Few cyberlaw 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.[15] Yahoo! reacted with alarm, maintaining that the French court could not properly assert jurisdiction over the matter.[16] Yahoo! noted that the company maintains dozens of country-specific websites, including a Yahoo.fr site customized for France, that were free of Nazi-related content.[17] These country-specific sites target the local population in their local language, and endeavor to comply with all local laws and regulations.[18]

The company argued that its flagship site, Yahoo.com, primarily targeted a United States audience. Since United States free speech laws pro-

---

12. *See infra* Part III.B.

13. *Yahoo!France*, *supra* note 5.

14. Twentieth Century Fox Film Corp. v. iCraveTV, No. 00-121, 2000 U.S. Dist. LEXIS 1013 (W.D. Pa. Jan. 28, 2000).

15. *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 ("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."); *see also* Kristi Essick, *Yahoo Told To Block Nazi Goods from French,* THE STANDARD, Nov. 20, 2000 (on file with author) ("A French judge upholds his previous decision, ordering the company to install a filtering system for its auction site. The case raises questions about the jurisdiction of national courts over international Net companies.").

16. Hu & Hansen, *supra* note 15.

17. *See* Brian Love, *Can Neo-Nazis Yahoo! in France?,* REUTERS, Aug. 10, 2000, *at* http://www.zdnet.com/zdnn/stories/news/0,4586,2614196,00.html ("French law prohibits the sale or exhibit of objects with racist overtones and none are directly available or visible on the Yahoo.fr site.").

18. *See* Yahoo! Terms of Service, *at* http://docs.yahoo.com/info/terms (last visited Nov. 26, 2001).

tect the sale of Nazi memorabilia, the auctions were entirely lawful.[19] Moreover, the Yahoo.com site featured a terms of use agreement, which stipulated that the site was governed by United States law.[20] 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.[21]

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.[22] 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.[23]

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.[24] Soon after, Yahoo! removed the controversial content from its site,[25] but the company proceeded to contest the validity of the French court's order in a California court.[26] In November 2001, the court ruled in favor of Yahoo!, holding that the French judgment was unenforceable in the United States.[27]

---

19. *See* Brendon Fowler et al., *Can You Yahoo!? The Internet's Digital Fences,* 2001 DUKE L. & TECH. REV. 12, ¶ 1, *at* http://www.law.duke.edu/journals/dltr/articles/2001dltr0012.html.

20. *See* Yahoo! Terms of Service, *supra* note 18.

21. *See id*.

22. *See Yahoo!France*, *supra* note 5.

23. *Id.; see also* UEJF et LICRA v. Yahoo! Inc. et Yahoo France, T.G.I. Paris, Nov. 20, 2000, N° RG: 00/05308 [hereinafter *Yahoo!France Interim Order*].

24. *See id*.

25. Lisa Guernsey, *Yahoo to Try Harder to Rid Postings of Hateful Material*, N.Y. TIMES, Jan. 3, 2001, *available at* http://www.nytimes.com/2001/01/03/technology/03YAHO.html ("Yesterday, Yahoo officials said the monitoring policy was not a response to the French ruling. Rather, they said, the company was responding to users who had requested a more active policy and to groups like the Wiesenthal Center and the Anti-Defamation League, which have been in talks with Yahoo throughout the year.").

26. Yahoo!, Inc. v. LICRA, C-00-21275 JF, 2001 U.S. Dist. LEXIS 18378 (N.D. Cal. Nov. 7, 2001).

27. *Id.* at *10.

B. The *iCraveTV* case

In late 1999, iCraveTV, a small Canadian Internet startup company, attracted the legal wrath of broadcasters, sports leagues, and movie studios in both Canada and the United States when it began providing Internet users with the opportunity to watch television in real-time on their personal computers.[28] The lawsuits proved effective. On February 28, 2000, approximately one month after a federal court issued an injunction banning its webcasting,[29] iCraveTV announced that it had reached a settlement with the broadcasters, sports leagues, and movie studios on both sides of the border. It agreed to permanently stop its unauthorized webcasting activities.[30]

One of the most interesting aspects of the case was the ease with which a United States court asserted jurisdiction over a Canadian company webcasting in Canada, referring to indicia such as the United States registrant address attached to the iCraveTV domain name. iCraveTV had sought to limit its distribution to Canadians and thus avoid United States jurisdiction.[31] Since iCraveTV recognized that its activities were legal in Canada, but potentially illegal elsewhere, it conditioned access on passing through three stages of verification. The company's clickwrap agreements were designed to ensure that only persons located in Canada could lawfully access the service.[32] The first step required the potential user to enter

---

28. "A tiny Canadian Internet startup is being hit with the wrath of Hollywood and the big broadcasting networks in the U.S. The company is called iCraveTV. It's been in business less than two months, and it's just been hit with a huge lawsuit, backed by most of the American entertainment industry." Michael Colton, *U.S. Broadcasters Take iCraveTV to Court* (CBC radio broadcast, Jan. 21, 2000).

29. Twentieth Century Fox Film Corp. v. iCraveTV, No. 00-121, 2000 U.S. Dist. LEXIS 1013, at *2 (W.D. Pa. Jan. 28, 2000).

30. Bloomberg News, *Broadcasters Pull the Plug on iCraveTV*, CNET NEWS.COM, Feb. 28, 2000, *at* http://news.cnet.com/category/0-1004-200-1559907.html. For the settlement agreement, see Canadian Association of Broadcasters, Settlement Agreement, *at* http://www.cab-acr.ca/english/joint/submissions/settlement.htm (last visited Nov. 26, 2001). Interestingly, the settlement provides that if a court in Canada makes a final determination that Internet webcasting without permission is not a violation of Canadian copyright law, iCraveTV can move to vary the terms of the settlement. Moreover, in addition to stopping the webcasting, iCraveTV agreed to stop its application for an Internet royalty before the copyright board. *Id.*

31. *See* Susanne Craig, *Court Shuts Down iCraveTV—for now*, GLOBE AND MAIL, Jan. 29, 2000, *available at* http://friendscb.org/articles/Globe&Mail/globe000129.htm ("iCraveTV argued in court that its service is intended only for Canadians and it has taken steps as recently as yesterday to prohibit non-Canadians from accessing the site.").

32. *See* Steven Bonisteel, *Peepers.com Lawsuit Eyes Net Jurisdiction*, INFOWAR.COM, May 24, 2000, *at* http://www.infowar.com/law/00/law_052-400b_j.shtml;

his local area code. If the area code was not a Canadian area code, the user was denied access to the service. This approach was viewed, with some justification, as an ineffective safeguard, since iCraveTV's own Toronto area code was posted on the site.[33]

The second step required the user to confirm that he was located in Canada.[34] The user was confronted with two icons—an "In Canada" icon and a "Not in Canada" icon.[35] If the user clicked on the "In Canada" icon, he was then presented with the third step, another clickwrap agreement.[36] This agreement contained a complete terms of use agreement including another confirmation that the user was located in Canada.[37] To complete the agreement, the user was required to scroll to the bottom of the agreement and click on the "I Agree" icon.[38]

The specific details of this case highlight the challenges of distinguishing between active and passive websites as required by the *Zippo* test. United States-based users were required to pass through three stages to access the site, including fraudulently entering into two clickwrap agreements. It is, therefore, arguable that under the *Zippo* test described below, while the iCraveTV site was "active" in Canada, it was actually "passive" for United States purposes, and therefore should have fallen outside of United States jurisdiction. If it was passive for United States users, the court should have lacked jurisdiction to hear the case under the *Zippo* test.

In light of the various standards being applied by courts in establishing jurisdictional rights in the online environment, this paper examines the effectiveness of the current approaches and recommends possible reforms. I argue that the passive versus active test established in *Zippo* has, with time, become increasingly outdated and irrelevant. It has been surpassed in practice by an effects-based analysis that poses even greater danger to legal certainty and the prospect for "over-regulation" of Internet-based activities. I argue instead for the adoption of a three-factor targeting test that includes analysis of contract, technology, and knowledge as the standard for assessing Internet jurisdiction claims.

Part II of this paper contains an analysis of the complications created by Internet jurisdiction, highlighting four policy considerations that must

---

see also Michael A. Geist, *iCraveTV and The New Rules of Internet Broadcasting,* 23 U. ARK. LITTLE ROCK L. REV. 223, 225 (2000).

33. *See* Geist, *supra* note 32, at 226.
34. *Id.*
35. *Id.*
36. *Id.*
37. *Id.*
38. *Id.*

be balanced in order to develop a test that garners approval from a diverse group of stakeholders and remains relevant as technologies change. These four policy considerations are: foreseeability, bias towards effects-based analysis, jurisdictional quid pro quo, and technological neutrality.

Mindful of these complications, Part III contains a review of recent Internet jurisdiction jurisprudence in both the United States and Canada, beginning with the development of and subsequent approval of the *Zippo* passive versus active test. It identifies the subtle changes that have been occurring since late 1999, as courts begin to find the *Zippo* test too constraining and shift their analysis toward an effects-based paradigm.

Having argued that the *Zippo* test should be replaced, Part IV presents an alternative, proposing a targeting-based test for Internet jurisdiction which is supported by the growing acceptance of targeting in both case law and international policy levels. It then advocates the adoption of a three-factor approach to targeting that includes assessments of any contractual provisions related to jurisdiction, the technological measures employed to identify the targeted jurisdiction, and the actual or implied knowledge of the website operator with respect to targeted jurisdictions.

Part V concludes by applying the targeting test to the *Yahoo! France* and *iCraveTV* cases. Although the analysis would not change the outcome in these cases, it demonstrates how the parties would benefit from the greater legal certainty that accompanies a targeting-based analysis.

II. JURISDICTION ON THE INTERNET

Internet jurisdiction suffers from heightened uncertainty on several levels. First, challenges in defining the issue have often left policy makers and courts at odds over which aspect of the jurisdictional issue should be analyzed. Second, the challenges of applying reasonableness and foreseeability principles to the online environment are complicated by changing technology and an environment where cross-border disputes are the norm.

Professor Yochai Benkler of NYU Law School argues that communications systems are divided among three interconnected layers.[39] There is a physical layer that includes the wires and connections needed to link phones, computers, routers, and other communications technology. Above the physical layer is a logical layer that determines who is able to access

---

39. The Information Law Institute at New York University School of Law, *Free Information Ecology in the Digital Environment*, at 29, *at* http://www.law.nyu.edu/ili/conferences/freeinfo2000/webcast/transcripts/105124DemDiscourse.pdf (last visited Nov. 26, 2001).

what on the network. Finally, above the logical layer is a content layer where the content being communicated resides.

Internet jurisdiction can also be conceptualized in three layers. There is an application layer that determines whether courts are entitled to apply their laws to a particular dispute. Above the application layer is a substantive layer, where courts apply their substantive laws to the dispute.[40] Above the substantive layer is the enforcement layer, where court orders must be enforced in an online environment that often resists the imposition of foreign judgments because of large distances and minimal monetary disputes.[41]

Internet jurisdiction discussions often fail to adequately distinguish between these three layers. For example, criticism leveled at the French court's decision in the *Yahoo!France* case has focused on the court's willingness to assert jurisdiction over a site based in the United States, the inappropriateness of French free speech law, and the challenge of forcing Yahoo! to comply with the order.[42] Although each of these criticisms is

---

40. The substantive layer tends to be the most contentious since it frequently pits divergent perspectives on fundamental legal freedoms, such as freedom of speech, against one another. *See*, *e.g.,* Stephan Wilske & Teresa Schiller, *International Jurisdiction in Cyberspace*: *Which States May Regulate the Internet?*, 50 FED. COMM. L.J. 117, 122-23 (1997) ("When CompuServe, Inc. blocked access by its subscribers in the United States and around the world to two hundred discussion groups after a federal prosecutor in Germany had indicated that they might violate German pornography laws, users realized that 'cyberspace doesn't belong to a single country,' but to a whole range of countries with diverse legal concepts.").

41. Despite this article's focus on the application layer—better known as adjudicatory jurisdiction—some commentators have opined that the enforcement layer actually presents the greatest challenge in the online environment. *See*, *e.g*., Henry H. Perritt, Jr., *Will the Judgment-Proof Own Cyberspace?,* 32 INT'L LAW. 1121, 1123 (1998) ("The real problem is turning a judgment supported by jurisdiction into meaningful economic relief. The problem is not the adaptability of *International Shoe*—obtaining jurisdiction in a theoretical sense. The problem is obtaining meaningful relief.").

42. The case was characterized in the following manner by the Center for Democracy and Technology:

> In a setback for free expression on the Internet, a French court has ruled that U.S.-based Yahoo, Inc. is to be held liable under French law for allowing French citizens to access auction sites for World War II Nazi memorabilia . . . . The ruling appears to impose blocking requirements that many view as impractical to implement on a wide scale and highly imperfect at identifying Internet users by country. It also sets a dangerous precedent for countries seeking to impose restrictions on speech outside their borders.

Center For Democracy and Technology, *French Court Holds Yahoo Accountable For U.S. Auction Content*, *at* http://www.cdt.org/publications/pp_6.20.shtml (last visited Nov. 26, 2001).

treated as a single critique of the case, each, in fact, involves a separate jurisdictional layer and merits a different response.

This paper focuses on Internet jurisdiction's application layer. Arguments about the substantive layer are much more difficult to defend—different countries have different norms and values, and it is unrealistic to expect the Internet to spur harmonization of all substantive issues. Similarly, arguments over the enforcement layer tend to involve business risk analysis—rather than legal risk analysis—because the ability to enforce a local decision will often depend upon whether the affected party has local assets subject to seizure or is sufficiently large enough that it cannot afford to ignore an outstanding court order, no matter where it is located.[43]

Sorting through conflicting laws and competing claims often presents lawmakers and courts with several difficult policy choices—choices that tend to blur the distinction between the three layers. For example, although it is intuitively appealing that local laws should protect consumers online in the same manner as they protect them offline, the application of these offline principles to the Internet is particularly complex. This complexity raises concern over the application of local law, the desire to protect local citizenry from harmful cyber-effects, the furtherance of policy goals that seek to encourage e-commerce and Internet use, as well as the difficulty in defining policies that can be applied in a technology-neutral fashion. Should local courts assert jurisdiction over every online consumer purchase (application layer)? Should policy explicitly seek to encourage e-commerce by creating protection legislation specific to e-commerce (substantive layer)? Will a consumer actually benefit from a local judgment if the award must still be enforced elsewhere (enforcement layer)?

At the heart of the matter lies a deceptively simple question—when is it appropriate to assert jurisdiction over Internet-based activities? Since the question of jurisdiction is not new (most countries have a rich body of law addressing conflict of laws, choice of forum, and enforcement of judgments),[44] most courts and policy makers quite properly revert to first principles in developing appropriate guidelines.[45]

In many jurisdictions, the litmus test for determining whether assertion of jurisdiction is appropriate involves analyzing whether jurisdiction is reasonable under the circumstances, with courts in the United States and

---

43. *See Yahoo!France*, *supra* note 5.

44. *See generally* EUGENE F. SCOLES & PETER HAY, CONFLICT OF LAWS (1998).

45. *See generally* Ogilvy Renault Internet Group, *Jurisdiction and the Internet*: *Are Traditional Rules Enough?*, *at* http://www.law.ualberta.ca/alri/ulc/current/ejurisd.htm (Jul. 1998).

Canada regularly relying on a reasonableness standard as their guide. In the United States, the reasonableness standard is couched in terms of "minimum contacts,"[46] while in Canada the language of choice is "real and substantial connection."[47] Although these terms necessitate somewhat different analyses, the core principle remains the same—the appropriateness of asserting jurisdiction depends upon whether the parties themselves would think it reasonable to do so.

Unfortunately, aside from reassuring parties that jurisdiction will not be asserted indiscriminately, substituting the word "reasonable" for "appropriate" does little to provide additional legal certainty. Accordingly, it has fallen on the courts to provide guidance on how the term "reasonable" should be interpreted. Case law analysis suggests that within the context of jurisdiction law, a foreseeability metric lies at the heart of the reasonableness standard. This metric dictates that a party should only be haled into a foreign court where it was foreseeable that such an eventuality might occur.[48]

Although a foreseeability test may not always provide absolute legal certainty, it does provide an intuitive sense of when a court will assert jurisdiction over a dispute. For example, if a contract dispute arises between two parties in different countries, it would generally be considered foreseeable that, absent a forum selection clause—a clause in which the parties settle on the governing jurisdiction in advance of the dispute—courts in either country might be willing to assert jurisdiction. In other instances, such as a defamation tort action, a court would likely conduct an effects-based analysis on foreseeability, concluding that the alleged defamer would have foreseen that the defamatory statements would have an impact within the defamed party's jurisdiction and thus she might face the prospect of litigation there.

While the foreseeability/reasonableness standard may have functioned effectively in the offline world, there are several reasons why the Internet complicates the issue. First, with worldwide Internet availability, foreseeability is much more difficult to gauge. Scholars have commented that the "borderless Internet" significantly impedes the application of physical laws, leading some to advocate for a separate cyberspace jurisdiction.[49] Since jurisdictional tests are rooted in the principle of providing greater clarity, the Internet clouds matters by providing an "all or nothing" envi-

---

46. International Shoe Co. v. Washington, 326 U.S. 310, 316 (1945).

47. Morguard Invs. Ltd. v. De Savoye [1990] 3 S.C.R. 1077.

48. World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 296 (1980).

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

ronment in which either every jurisdiction is foreseeable or none is foreseeable.

Second, courts and policy makers are likely to be biased toward asserting jurisdiction where harm has been experienced locally.[50] This can best be understood by assessing a simple business-to-consumer e-commerce transaction. Suppose that a consumer located in Ottawa downloads an electronic book from Amazon.com, a leading e-commerce business located in Seattle, Washington.[51] The terms of sale stipulate that all disputes are to be settled in Washington. Suppose further that the consumer is dissatisfied with the transaction because the downloaded e-book causes his computer system to crash and lose valuable data. If the parties are unable to negotiate a settlement, the consumer may wish to sue for the price of the book and resulting damages in Ontario. Amazon is likely to contest the action on jurisdictional grounds, arguing that the forum selection clause controls any disputes and that legal actions should be brought in a court in Washington.

Should the Ontario court dismiss the action by upholding the enforceability of the forum selection clause? Will doing so effectively eliminate the consumer's access to Ontario consumer protection legislation? Courts throughout North America appear divided on the issue. In a 1999 Ontario case, a court dismissed a class action lawsuit brought against Microsoft on the grounds that a clickwrap agreement between the parties provided for Washington to have exclusive jurisdiction over any disputes.[52] A recent California case ruled in the opposite manner, holding that a dispute between AOL and one of its customers could be heard in a California court

---

50. According to one report on European activity:

> The law, dubbed the Brussels I regulation, will come into effect next March. It states that where there is a dispute between a consumer in one EU country and an online retailer in another, the consumer will be able to sue in a court in his own country. The justice ministers and the European Commission, who drafted the regulation, argue that this focus on the consumer is essential to help get electronic commerce off the ground in Europe. 'A lack of consumer confidence is the main thing holding up the development of e-commerce here,' said Leonello Gabrici, spokesman on judicial matters for the Commission. He said that by handing jurisdiction of such cross-border disputes to the courts in the consumers' country, the regulation will be encouraging consumers to purchase online.

Paul Meller, *European Justices Pass Stiff E-Commerce Law*, IDG.NET, Nov. 30, 2000, *at* http://www.idg.net/idgns/2000/11/30/EuropeanJusticesPassStiffECommerceLaw.shtml

51. *See* amazon.com, *at* http://www.amazon.com/exec/obidos/subst/misc/companyinfo.html/002-2423967-3027211 (last visited Nov. 26, 2001).

52. Rudder v. Microsoft Corp., [1999] 2 C.P.R. (4th) 474 (Ont.).

despite the existence of a forum selection clause that provided that all disputes be brought in a Virginia court.[53]

The scenario becomes even more complicated when the case involves free speech rather than commercial concerns. For example, the recent French Nazi memorabilia case involving Yahoo! illustrates how a local court may assert jurisdiction—even in the absence of evidence that the harm was directed at that jurisdiction—reasoning that the perceived local harm is too great to ignore.[54] While such an approach raises few concerns when it involves activity such as securities fraud, where global rules are relatively uniform,[55] the application of an effects-based standard on issues such as free speech is likely to prove highly contentious since restrictions on free speech vary between even democratic countries.

Although courts and policy makers may have a bias towards protecting local citizenry from commercial or content-based harm, the issue is further complicated by the fact that all countries face the same concern. Accordingly, while a country may wish to protect its own consumers by asserting jurisdiction over out-of-country entities, it would prefer that other countries not exert the same authority over its citizens and companies.[56]

Moreover, the laws applied locally will vary because different countries will promote different policy priorities. Some countries may view consumer protection as more important than promotion of e-commerce growth and thus adopt a policy of aggressively asserting jurisdiction to protect local consumers. Others may favor the promotion of privacy protection and will thus seek to assert jurisdiction over a privacy framework. As Lawrence Lessig argues in his seminal book, *Code and Other Laws of Cyberspace*, these competing policy priorities encourage countries to engage in a quid pro quo approach to jurisdictional cooperation.[57] In discussing Minnesota's desire to enforce state anti-gambling laws, Lessig notes:

> Why would any other jurisdiction want to carry out Minnesota's regulation?

---

53. Mendoza v. AOL (Cal. Super. Ct.) (unreported, on file with author).

54. *See Yahoo!France*, *supra* note 5.

55. International Organization of Securities Commissions (IOSCO), Technical Committee, Securities Activity on the Internet, Sept. 1998, *at* http://www.iosco.org/download/pdf/1998-internet_security.pdf [hereinafter IOSCO].

56. Dean Henry Perritt notes "[e]xtending the bases of jurisdiction is a two-edged sword. United States citizens may be able to assert U.S. law in U.S. courts with respect to harmful conduct occurring offshore, but they also may be subject to prosecution or litigation in foreign tribunals." Perritt, *supra* note 41, at 1131.

57. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 55 (1999).

> The answer is that they would not if this were the only regulation at stake. Minnesota wants to protect its citizens from gambling, but New York may want to protect its citizens against the misuse of private data. The European Union may share New York's objective; Utah may share Minnesota's.
>
> Each state has its own stake in controlling certain behaviors, and these behaviors are different. But the key is this: the same architecture that enables Minnesota to achieve its regulatory end can also help other states achieve their regulatory ends. And this can initiate a kind of quid pro quo between jurisdictions.[58]

As if the policy choices were not already sufficiently complicated, an additional consideration must be factored into the analysis. As policy makers continue to grapple with the challenges of the Internet, it has become increasingly accepted that establishing effective and enduring guidelines or standards for the Internet requires the adoption of a "technology neutral" approach.[59] Technology neutral approaches have been a hallmark of many Internet law policy initiatives, including the development of e-commerce legislation[60] and the adoption of electronic evidence statutes.[61] "Technology neutral" in this context refers to statutory tests or guidelines that do not depend upon a specific development or state of technology, but rather are based on core principles that can be adapted to changing technologies.[62] Since technological change is constant, standards created with specific technologies in mind are likely to become outdated as the technology changes. In the context of Internet jurisdiction, using indicia that reflect the current state of the Internet and Internet technologies is a risky proposition since those indicia risk irrelevancy when the technology changes.

---

58. *Id*.

59. As the Australian Attorney General's office has noted within the context of UNCITRAL e-commerce negotiations, "[a] technology neutral approach is preferable as it has become clear that technology specific legislative schemes can inhibit market choice. Furthermore, legislative regimes that prefer one technology over another create impediments to electronic commerce and restrict innovation." Australian Attorney General's Department, Information Economy Section*, UNCITRAL Developments*, *at* http://law.gov.au/publications/ecommerce (last visited Nov. 26, 2001).

60. Uniform Law Conference of Canada (ULCC), Uniform Electronic Commerce Act (Model Law), *available at* http://www.law.ualberta.ca/alri/ulc/current/euecafin.htm (last visited Nov. 26, 2001).

61. *Id.*

62. *See* Telecommunications Standards Advisory Council of Canada (TSACC), Business Transaction Model: Data Component, *at* http://www.tsacc.ic.gc.ca/openforum/docs/TSACC-010-313.pdf (last visited Nov. 26, 2001).

In seeking to balance these four factors—foreseeability, bias towards effects-based analysis, jurisdictional quid pro quo, and technological neutrality—the development of a single standard for Internet jurisdiction analysis presents a difficult, though not insurmountable, challenge. Unfortunately, the current passive versus active test moves the law squarely in the wrong direction by failing to provide parties with sufficient guidance on any of these four factors.

III. THE RISE AND FALL OF THE *ZIPPO* TEST

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. This section traces the case law development of Internet jurisdiction in the United States and Canada.

A. The Emergence of the *Zippo* Passive versus Active Test

In *International Shoe Co. v. Washington*, the Supreme Court outlined the contemporary basis for jurisdiction.[63] Under *International Shoe*, a court can 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.'"[64] The minimum contacts standard serves two purposes: protecting defendants from burdensome litigation and ensuring that states do not reach too far beyond their jurisdictional limits.[65]

"Minimum contacts" have been defined as "conduct and connection with the forum . . . such that [the defendant] should reasonably anticipate being haled into court there."[66] 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 avail[ed] itself of the privilege of conducting activities within the forum State, thus invoking the benefits and protections of its laws."[67] The plaintiff has the burden of showing that the defendant took action "purposefully

---

63. 326 U.S. 310, 316 (1945).
64. *Id.* (quoting Milliken v. Meyer, 311 U.S. 457, 463 (1940)).
65. World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 291 (1980).
66. *Id*. at 297.
67. Hanson v. Denckla, 357 U.S. 235, 253 (1958).

directed" at the forum and that the cause of action arises from this action.[68] 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."[69]

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.[70]

One of the first North American applications of these principles to the Internet traces back to 1996 and *Inset Systems, Inc. v. Instruction Set, Inc.*, a Connecticut district court case.[71] 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."[72] 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."[73] 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 con-

---

68. *See* 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).

69. Burger King v. Rudzewicz, 471 U.S. 462, 475 (1985).

70. See *id*. at 476-77.

71. Inset Sys., Inc. v. Instruction Set, Inc., 937 F. Supp. 161 (D. Conn. 1996).

72. 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, *at* http://www.bereskinparr.com/art-pdf/TM&InternetOverview.pdf.

73. *Inset*, 937 F. Supp. at 163.

duct meet the minimum contacts standard outlined by the United States Supreme Court in *World-Wide Volkswagen*?[74]

The *Inset* court concluded that it could properly assert jurisdiction, basing its decision on Instruction Set's use of the Internet.[75] 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.[76]

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 the fundamental principle of jurisdiction.[77] 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.[78] If the court was correct, every court, everywhere, could assert jurisdiction where a website was directed toward its forum. This approach would stifle future Internet growth, as would-be Internet participants would be forced to weigh the advantages of the Internet with the potential of being subject to legal jurisdiction throughout the world. Third, the court did not assess Instruction Set's actual activity on the Internet.[79] The mere *use* of the Internet was sufficient for this court to establish jurisdiction.[80] 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 state.[81]

A more complete analysis of the underlying facts would have included an assessment of precisely what the parties were doing on the Internet. Was Instruction Set selling products directly to people in Connecticut through its website? Was it providing a service directly through its website? Was it actively soliciting the participation of potential users by encouraging correspondence? What was the approximate number of Connecticut users who actually accessed the website? Asking these and similar questions would have provided the court with a much stronger basis for holding that Instruction Set had purposefully directed its activity toward Connecticut.

---

74. World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 291-92 (1980).
75. *Inset*, 937 F. Supp. at 160.
76. *Id.* at 165.
77. *Id.*
78. *Id.*
79. *Id.*
80. *Id.*
81. *Id.* at 162-63.

With the *Inset* precedent established, however, many similar cases soon followed. In *Maritz, Inc. v. Cybergold, Inc.*, for example, a Missouri federal district court confronted the question of personal jurisdiction on the Internet in the context of a trademark infringement action.[82] Citing the *Inset* decision with approval, the Court struggled for an effective metaphor, noting that:

> the nature and quality of contacts provided by the maintenance of a website on the Internet are clearly of a different nature and quality than other means of contact with a forum such as the mass mailing of solicitations into a forum . . . . or that of advertising an 800 number in a national publication.[83]

Unable to arrive at an effective analogy, the court concluded that Inset made a conscious decision to transmit advertising information to all Internet users and that such knowledge was sufficient for the assertion of personal jurisdiction.[84]

In Canada, the experience with of Internet jurisdiction closely paralleled that of the United States. In keeping with the *Inset* line of cases, the Newfoundland Supreme Court asserted jurisdiction based partly on the provision of information via the Internet in *Alteen v. Informix Corp*.[85] *Alteen* involved allegations that Informix Corporation, a United States-based maker of database software, issued false and misleading statements that led to an inflated stock price. When shareholders residing in Newfoundland launched a lawsuit, Informix responded by arguing that the local court could not properly assert jurisdiction since the company did not trade shares on a Canadian public exchange, issue public statements to the Canadian press, or maintain direct contact with the plaintiffs.[86]

The court rejected the argument and sided with the plaintiffs who maintained that the availability of public statements on the Internet often led to Canadian media coverage.[87] Since the shares were purchased in Newfoundland and corporate information was available within the province, the court ruled that it was entitled to assert jurisdiction over the tort action.[88] Although the action involved tort rather than trademark infringement, *Alteen* bears a striking similarity to the early United States Internet

---

82. 947 F. Supp. 1328 (E.D. Mo. 1996).
83. *Id.* at 1333.
84. *Id.*
85. [1998] N.J. No. 122 (Newf.).
86. *Id.* at ¶ 8.
87. *Id.* at ¶ 13.
88. *Id.* at ¶¶14, 15.

cases, where the mere availability of information on the Internet was viewed as sufficient grounds to assert jurisdiction. Had that analysis been adopted, all Canadian courts would theoretically be entitled to assert jurisdiction over parties posting information on the Internet.

While several additional United States cases followed the *Inset* approach,[89] a New York district court case stands out as an important exception.[90] The Blue Note was a small Columbia, Missouri club operated by Richard King. King promoted his club by establishing a website that included information about the club, a calendar of events, and ticketing information.[91] 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.[92] King was familiar with the New York Blue Note as he included a disclaimer on his website that stated: "The Blue Note's Cyberspot should not be confused with one of the world's finest jazz club[s], [the] Blue Note, located in the heart of New York's Greenwich Village. If you should find yourself in the Big Apple give them a visit."[93]

Within months of the establishment of King's Blue Note website, Bensusan brought a trademark infringement and dilution action in New York federal court.[94] Once again, the court faced the question of personal jurisdiction in a trademark action arising out of activity on the Internet. Unlike the *Inset* 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—several affirmative steps by a New York resident would be necessary to bring any potentially infringing product into the state.[95] 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.[96] The

---

89. *See*, *e.g.*, Heroes, Inc. v. Heroes Found., 958 F. Supp. 1, 5 (D.D.C. 1996) (citing *Inset* with approval in finding that a website sustained contact with the District of Columbia); Panavision Int'l, L.P. v. Toeppen, 938 F. Supp. 616 (C.D. Cal. 1996) (finding that use of a trademark infringing domain name in Illinois was an act expressly directed at California).

90. Bensusan Rest. Corp. v. King, 937 F. Supp. 295 (S.D.N.Y. 1996), *aff'd* 126 F.3d. 25 (2d Cir. 1997).

91. *Id.* at 297.

92. *Id.* at 298.

93. *Id.* at 297-98.

94. *Id.* at 297.

95. *Id.* at 299.

96. *Id.*

purchaser would have to travel to Missouri to obtain the tickets.[97] Given the level of passivity, the court ruled that the website did not infringe Bensusan's trademark in New York.[98] The court argued "[t]he 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."[99]

The *Bensusan* decision, which the Court of Appeals for the Second Circuit affirmed in September 1997,[100] 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 cases.[101] 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.[102]

In early 1997, a new approach emerged, led by a Pennsylvania district court decision, *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*[103] 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. Zippo Manufacturing was a Pennsylvania based manufacturer of the well-known "Zippo" brand of tobacco lighters.[104] Zippo Dot Com was a California

---

97. *Id.*
98. *Id.*
99. *Id.*
100. Bensusan Rest. Corp. v. King, 126 F.3d 25, 29 (2d Cir. 1997).
101. *See, e.g.,* Hearst Corp. v. Goldberger, No. 96 Civ. 3620 PKL AJP, 1997 WL 97097, at *15 (S.D.N.Y. Feb. 26, 1997). The *Goldberger* court relied heavily upon the *Bensusan* analysis in refusing to assert personal jurisdiction in a trademark infringement matter involving the domain name "Esqwire.com." *Id.* The *Goldberger* court carefully reviewed Internet case law to that point, noted its disagreement with decisions such as *Inset*, *Maritz*, and *Panavision*, and cautioned that:

> [w]here, 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.

Id. at *13.
102. Michael Geist, *The Reality of Bytes*: *Regulating Economic Activity in the Age of the Internet*, 73 WASH. L. REV. 521, 538 (1998).
103. 952 F. Supp. 1119, 1126 (W.D. Pa. 1997).
104. *Id.* at 1121.

based Internet news service that used the domain name "Zippo.com" to provide access to Internet newsgroups.[105] Zippo Dot Com offered three levels of subscriber service—free, original, and super.[106] 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.[107] 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.[108] 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.[109] Once again, the issue before the court was one of personal jurisdiction arising out of a claim of trademark infringement and dilution.[110]

Rather than using Internet analogies as the basis for its analysis, the court focused on the prior, somewhat limited Internet case law.[111] 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*.[112]

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 where a defendant has simply posted information

---

105. *Id.*
106. *Id.*
107. *Id.*
108. *Id.*
109. *Id.*
110. *Id.*
111. One case omitted from the discussion but relied upon by the *Zippo* 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 distribute 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 available to users of its proprietary network (not Internet users at large).
112. *Zippo,* 952 F. Supp. at 1127.

> 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 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.[113]

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.

B. Post-*Zippo* Case Law

In the years following *Zippo*, the passive versus active approach has been cited with approval in numerous cases.[114] For example, in *Cybersell, Inc. v. Cybersell, Inc.*, the Ninth Circuit considered whether it could exercise jurisdiction over a website containing an allegedly infringing service mark.[115] Both Cybersell Arizona, the owner of the "Cybersell" federal service mark, and Cybersell Florida provided Internet marketing and consult-

---

113. *Id.* at 1124 (internal citations omitted).

114. *See, e.g.,* Am. Eyewear, Inc. v. Peeper's Sunglasses and Accessories, Inc., 106 F. Supp. 2d 895 (N.D. Tex. 2000); Am. Online, Inc. v. Huang, 106 F. Supp. 2d 848 (E.D. Va. 2000); Citigroup v. City Holding Co., 97 F. Supp. 2d 549 (S.D.N.Y. 2000); Standard Knitting, Ltd. v. Outside Design, Inc., No. 00-2288, 2000 WL 804434 (E.D. Pa. Jun. 23, 2000); Decker v. Circus Circus Hotel, 49 F. Supp. 2d 748 (D. N.J. 1999); Hasbro, Inc. v. Clue Computing, Inc., 66 F. Supp. 2d 117 (D. Mass. 1999); Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998); Mallinkrodt Med., Inc. v. Sonus Pharm., Inc., 989 F. Supp. 265 (D.D.C. 1998); Resuscitation Techs., Inc. v. Cont. Health Care Corp., No. IP 96-1457-C-M/S, 1997 WL 148567 (S.D. Ind. Mar. 24, 1997); Smith v. Hobby Lobby Stores, Inc., 968 F. Supp. 1356 (W.D. Ark. 1997); TELCO Communications v. An Apple A Day, 977 F. Supp. 404 (E.D. Va. 1997); Conseco, Inc. v. Hickerson, 698 N.E.2d 816 (Ind. App. 1998); State by Humphrey v. Granite Gate Resorts, Inc., (Minn. App. 1997).

115. 130 F.3d. 414 (9th Cir. 1997).

ing services.[116] Cybersell Florida's presence in Arizona was limited to a website advertising its services and inviting interested parties to contact it for additional information.[117] The court, in determining the appropriateness of exercising jurisdiction, noted:

> [N]o court has ever held that an Internet advertisement alone is sufficient to subject the advertiser to jurisdiction in the plaintiff's home state. Rather, in each, there has been 'something more' to indicate that the defendant purposefully (albeit electronically) directed his activity in a substantial way to the forum state.[118]

The court followed the *Zippo* approach by attempting to ascertain the nature and quality of Cybersell Florida's web-based activity.[119] The court considered the passive nature of the site, the fact that no Arizonian other than Cybersell Arizona visited the site, and the lack of evidence that any Arizonians had entered into a contractual relationship with Cybersell.[120] On these facts, the court concluded that it could not properly assert jurisdiction in this matter.[121]

Similarly, in *Mink v. AAAA Development L.L.C.*,[122] the plaintiff, a computer program developer, filed suit in Texas district court against a Vermont corporation, which allegedly conspired to copy the plaintiff's computer program.[123] The district court refused to assert personal jurisdiction in the case and dismissed the suit.[124] On appeal to the Fifth Circuit, the plaintiff argued that Texas was the proper forum because the defendant corporation's website was accessible from that state.[125] The court dismissed the appeal on the grounds that, while the website provided users with a printable mail-in order form, an e-mail address, a toll-free telephone number and a mailing address, the fact that no orders were taken through the site meant that it was nothing more than a passive advertisement.[126] In *GTE New Media Services Inc. v. Ameritech Corp.*,[127] the court

---

116. Interestingly, the principals behind Cybersell Arizona were Laurence Canter and Martha Siegel, attorneys who are infamous among web users as the first Internet "spammers" or junk e-mailers. *Id.* at 415.
117. *Id.* at 419.
118. *Id.* at 418.
119. *Id.*
120. *Id.*
121. *Id.* at 420.
122. 190 F.3d 333 (5th Cir. 1999).
123. *Id.* at 335.
124. *Id.*
125. *Id.*
126. *Id.* at 336-37.

was asked to assert jurisdiction over a company that was providing national Yellow Pages directory services over the Internet. Applying the passive versus active test, the court noted that the defendants maintained an interactive website that was available in the District of Columbia.[128] This fact, coupled with the fact that the defendants derived advertising revenues from the directory sites when District of Columbia residents accessed and utilized its Internet Yellow Pages, led the court to exercise personal jurisdiction.[129]

Finally, in *Desktop Technologies, Inc. v. Colorworks Reproduction & Design, Inc.*,[130] the plaintiff, a Pennsylvania corporation, filed suit in Pennsylvania district court against a Canadian company that carried on business exclusively in western Canada.[131] The complaint alleged trademark infringement and breach of state unfair competition law based on the defendant's use of a trademark as its domain name on the Internet.[132] The defendant brought a motion to dismiss the action for lack of personal jurisdiction.[133] Citing the fact that its Internet presence and e-mail links were its only contacts with Pennsylvania, it noted that the company had never entered into any contracts in Pennsylvania nor sold anything in the state.[134] Applying *Zippo* to these facts, the court ruled that the level of interactivity available on the defendant corporation's website did not justify exercising specific personal jurisdiction over the defendant since it was not doing business over the Internet with Pennsylvania residents.[135]

Canadian courts signaled their approval of the *Zippo* approach in *Braintech Inc. v. Kostiuk*.[136] This 1999 British Columbia Court of Appeal case, the first Canadian appellate level decision to address the Internet jurisdiction issue, involved a series of allegedly defamatory messages posted on a stock chat site by a British Columbia resident.[137] Braintech, a British Columbia based company, sued the poster in a Texas court; the court

---

127. 44 F. Supp. 2d 315 (D.D.C. 1999).
128. *Id*. at 315-16.
129. *Id*. at 315.
130. No. Civ. A. 98-5029, 1999 WL 98572 (E.D. Pa. Feb. 25, 1999).
131. *Id*. at *1.
132. *Id*.
133. *Id*. at *2.
134. *Id*. at *1.
135. *Id*. at *5.
136. [1999] 171 D.L.R. (4th) 46, 61 (B.C.C.A.). For a critical analysis of the *Braintech* decision, see Vaughn Black & Mike Deturbide, Braintech Inc. v. Kostick: *Adjudicatory Jurisdiction for Internet Torts*, 33 CANADIAN BUS. L.J. 427 (2000).
137. *Braintech*, 171 D.L.R. (4th) at 48.

awarded the company roughly $300,000 in damages.[138] When the company returned to British Columbia to enforce the judgment, the British Columbia courts examined the appropriateness of the Texas court's assertion of jurisdiction over the dispute.[139] Adopting the passive versus active test and citing directly to the *Zippo* case, the British Columbia Court of Appeal ruled that the Texas court had improperly asserted its jurisdiction.[140] It argued that the postings were passive in nature and thus provided insufficient grounds to grant the Texas court authority over the case. The Canadian Supreme Court denied Braintech's leave to appeal in early March 2000.[141]

The widespread approval for the *Zippo* test should come as little surprise. The uncertainty created by the Internet jurisdiction issue led to a strong desire for a workable solution that provided a fair balance between the fear of a lawless Internet and one burdened by over-regulation. The *Zippo* test seemed the best available alternative. This is particularly true in light of the *Inset* line of cases, which illustrated that the alternative might well be the application of jurisdiction by any court, anywhere. The court in *Neato v. Stomp L.L.C.*, a 1999 federal court case in California, aptly summarized the competing policy positions of consumers and businesses: protecting consumers and encouraging the development of Internet commerce, respectively.[142] The court chose to side squarely with consumers, noting that businesses can choose to sell their goods only to consumers in a particular geographic location:

---

138. *Id.*

139. *Id.* at 63.

140. *Id.*

141. Press Release, Supreme Court of Canada, Judgments in Leave Applications: Braintech Inc. v. John Kostiuk, Mar. 9, 2000, *at* http://www.lexum.umontreal.ca/csc scc/en/com/2000/html/00-03-09.3a.html.

142. Stomp, Inc. v. Neato LLC, 61 F. Supp. 2d 1074 (C.D. Cal. 1999). The court also recognized that:

> [S]uch a broad exercise of personal jurisdiction over defendants who engage in commerce over the Internet might have devastating effects on local merchants and small businesses that seek to expand through the Internet. These small businesses make up the backbone of the American economy and should not have to bear the burden of defending suits in distant fora when they intend only to sell to local consumers their wares from the convenience of their own homes. This concern must be balanced against the ability of a distant consumer to press its cause against a defendant who uses the Internet to do business within the forum while remaining outside the boundaries of the jurisdiction.

Id. at 1080-81.

> When a merchant seeks the benefit of engaging in unlimited interstate commerce over the Internet, it runs the risk of being subject to the process of the courts of those states.[143]

The *Zippo* passive versus active test is grounded in traditional jurisdictional principles. The analysis conducted as part of the test draws heavily from a foreseeability perspective, suggesting that it is not foreseeable for the owner of a passive website to face the prospect of being sued in multiple jurisdictions worldwide. Conversely, as the court in *Neato* recognized, the active e-commerce website owner must surely foresee the possibility of disputes arising in other jurisdictions, and recognize that those courts are entitled to protect local residents by applying local law and asserting jurisdiction.

Most importantly, however, in an emphatic repudiation of the "Internet as a separate jurisdiction[al]" approach, the *Zippo* case made it explicit that local law still applies to the Internet. Although it is at times difficult to discern precisely whose law applies, there is little doubt that at least one jurisdiction, if not more, can credibly claim jurisdiction over any given Internet dispute. With this principle in hand, the *Zippo* court sent a clear signal to the Internet community: courts were willing to establish a balanced approach to Internet jurisdiction.

C. The Shift Away from *Zippo*

Despite the widespread acceptance of the *Zippo* doctrine (and indeed the export of the test to foreign countries, including Canada), limitations of 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 were using other criteria to determine when assertion of jurisdiction was appropriate.[144]

Numerous judgments reflect that courts in the United States moved toward a broader, effects-based approach when deciding whether or not to assert jurisdiction in the Internet context. Under this new approach, rather than examining the specific characteristics of a website and its potential

---

143. *Id.*

144. In addition to the cases discussed *infra*, see also Panavision Int'l., L.P. v. Toeppen, 141 F.3d 1316, 1320 (9th Cir. 1998); Compuserve v. Patterson, 89 F.3d 1257 (6th Cir. 1996); Neogen Corp. v. Neo Gen Screening, Inc., 109 F. Supp. 2d 724, 729 (W.D. Mich. 2000); Search Force v. Data Force Intern., 112 F. Supp. 2d 771, 777 (S.D. Ind. 2000); Uncle Sam's Safari Outfitters, Inc. v. Uncle Sam's Navy Outfitters—Manhattan, Inc., 96 F. Supp. 2d 919, 923 (E.D. Mo. 2000); Bochan v. La Fontaine, 68 F. Supp. 2d 692, 701-02 (E.D. Va. 1999); Rothschild Berry Farm v. Serendipity Group LLC, 84 F. Supp. 2d 904, 908 (S.D. Ohio 1999).

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*.[145]

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 c) cause harm to the plaintiff in the forum state, which the defendant knows is likely to be suffered.[146] In *Calder*, a California entertainer sued a Florida publisher for libel in a California district court.[147] In ruling that personal jurisdiction was properly asserted, the Court focused on the effects of the defendant's actions.[148] 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 the defendant had intentionally targeted a California resident and thus it was proper to sue the publisher in that state.[149]

The application of the *Calder* test can be seen in the Internet context in *Blakey v. Continental Airlines, Inc.*,[150] 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.[151] 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.[152]

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.[153] The court applied the effects doctrine and held that while the actions causing the effects in New Jersey

---

145. 465 U.S. 783 (1984).
146. *Id.* at 789.
147. *Id.* at 784.
148. *Id.* at 789.
149. *Id.* at 789-90.
150. 751 A.2d 538 (N.J. 2000).
151. *Id.* at 543-48.
152. *Id.*
153. *Id.* at 543.

were performed outside the state, this did not prevent the court from asserting jurisdiction over a cause of action arising out of those effects.[154]

The broader effects-based analysis has moved beyond the defamatory tort action at issue in *Calder* and *Blakey* to a range of disputes including intellectual property and commercial activities. On the intellectual property front, *Nissan Motor Co. Ltd. v. Nissan Computer Corp.,*[155] typifies the approach. The plaintiff, an automobile manufacturer, filed a complaint in a California district court against a Massachusetts-based computer seller. Prompting the complaint 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.[156] In October 1999, the parties met to discuss the possibility of transferring the "nissan.com" domain name.[157] These negotiations proved unsuccessful.[158] 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.[159]

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.[160] Moreover, since the plaintiff was based in California, the majority of the harm was suffered in the forum state.[161] The court rejected the defendant's argument that it was not subject to personal jurisdiction because it merely operated a passive website.[162] Although the defendant did not sell anything over the Internet, it derived advertising revenue through the intentional exploitation of consumer confusion.[163] 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.[164]

Similarly, in *Euromarket Designs Inc. v. Crate & Barrel Ltd.*,[165] the issue before the court was whether an Illinois-based company could sue an

---

154. *Id.* at 556.
155. 89 F. Supp. 2d 1154 (C.D. Cal. 2000).
156. *Id.* at 1157.
157. *Id*.
158. *Id.* at 1158.
159. *Id.*
160. *Id.* at 1160.
161. *Id.*
162. *Id.*
163. *Id.*
164. *Id.* at 1159.
165. 96 F. Supp. 2d 824 (N.D. Ill. 2000).

Irish retailer for trademark infringement with an interactive website that allowed Illinois residents to order goods for shipment to a foreign address in a local court. The court noted that the pivotal considerations in resolving this issue were whether the defendant purposefully and deliberately availed itself of the forum and whether the defendant's conduct and connection with the forum was such that he should reasonably anticipate being haled into court there.[166] The court stated that the defendant deliberately established minimum contacts with Illinois and purposefully availed itself of the privilege of conducting activities in Illinois.[167]

The court concluded that the defendant's actions established jurisdiction under the effects doctrine because: a) if plaintiff's trademark was infringed, the injury would be felt primarily in Illinois; b) the defendant intentionally and purposefully directed its actions toward Illinois and the plaintiff, an Illinois corporation, allegedly causing harm to the plaintiff in Illinois; and c) the defendant knew that harm would likely be suffered in Illinois.[168]

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.,*[169] 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.[170] The site featured several interactive pages that allowed customers to take and score performance tests, download product demonstrations, and order products online.[171]

The court characterized the site as interactive but refused to assert jurisdiction over the matter.[172] Relying on evidence that no Texans had actually purchased from the website, 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 its web-

166. *Id.* at 834-35.
167. *Id.*
168. *Id.* at 836.
169. No. Civ. A. 399-CV-2339-L, 2000 WL 1030619 (N.D. Tex. Jul. 25, 2000).
170. *Id.* at *2.
171. *Id.* at *1.
172. *Id.* at *4.

site."[173] Instead, the plaintiff had to show that the defendant had "purposefully availed itself of the benefits of the forum state and its laws."[174]

A copyright dispute over craft patterns yielded a similar result in *Winfield Collection, Ltd. v. McCauley*.[175] 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 the plaintiff had supplied to the defendant.[176] The defendant moved to dismiss the suit for lack of personal jurisdiction.[177] 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 website that could send and receive messages.[178]

The court refused to assert jurisdiction, dismissing both arguments.[179] With respect to the plaintiff's first argument, the court focused on the fact that the sales were in fact conducted on eBay, an online auction site.[180] Because the items were sold to the highest bidder, the defendant had no advance knowledge about where the products would be sold.[181] As such, she did not purposefully avail herself of the privilege of doing business in Michigan.[182]

In response to the plaintiff's second argument, the court held that it was not prepared to broadly hold "that the mere act of maintaining a website that includes interactive features *ipso facto* establishes personal jurisdiction over the sponsor of that website anywhere in the United States."[183] In its judgment, the court noted that the plaintiff had provided it with the unpublished opinion in a case called *Amway v. Proctor & Gamble*.[184] In that case, the court held that "something more" than mere interactivity should be required to assert personal jurisdiction and found that "something more" to be the effects doctrine.[185] The court held that the plaintiff

---

173. *Id.* at *4.
174. *Id*.
175. 105 F. Supp. 2d 746, 751 (E.D. Mich. 2000).
176. *Id.* at 747.
177. *Id.*
178. *Id.* at 748.
179. *Id.* at 751.
180. *Id.* at 749.
181. *Id.*
182. *Id.*
183. *Id*. at 751.
184. *Id.*
185. *Id.*

could not rely on that doctrine since it failed to identify a continuing relationship with Michigan or with any resident of Michigan.[186]

One of the strongest criticisms of the *Zippo* doctrine can be found in *Millennium Enterprises, Inc. v. Millennium Music L.P.*,[187] 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.[188] The plaintiffs, an Oregon-based corporation, sued the defendants in Oregon district court for trademark infringement.[189] The defendant filed a motion to dismiss for lack of personal jurisdiction.[190] After canvassing numerous Internet jurisdiction cases decided in the Ninth Circuit, as well as *Zippo*, the court stated:

> [T]he 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 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*.[191]

Applying this reasoning to the facts before it, the court allowed the defendants' motion to dismiss the case on the grounds that the defendants had consummated no transaction and had not made deliberate and repeated contacts with Oregon through their website such that they could reasonably anticipate being haled into Oregon court.[192] In its concluding remarks, the court said:

> For all of these reasons, this court will not abandon the basic principle that defendants must have taken some action to direct their activities in the forum so as to "purposely avail" themselves of the privilege of doing business within Oregon. The timeless and fundamental bedrock of personal jurisdiction assures us all that a defendant will not be "haled" into a court of a foreign ju-

---

186. *Id.* at 747.
187. 33 F. Supp. 2d 907 (D. Or. 1999).
188. *Id.* at 909.
189. *Id.*
190. *Id.* at 919-20.
191. *Id*. at 921 (internal citations omitted).
192. *Id.*

> risdiction based on nothing more than the foreseeability or potentiality of commercial activity with the forum state.[193]

Applying that principle to the Internet, the court concluded that:

> [D]efendants cannot reasonably anticipate that they will be brought before this court, simply because they advertise their products through a global medium which provides the capability of engaging in commercial transactions.[194]

Although the case law illustrates that there is no single reason for the courts to shift away from the *Zippo* test, a number of themes do emerge. First, the test simply does not work particularly well in every instance. For example, with courts characterizing chat room postings as passive in nature,[195] many might be inclined to dismiss cases involving allegedly defamatory or harassing speech on jurisdictional grounds. Such speech may often be targeted toward a particular individual or entity located in a jurisdiction different from the poster or the chat site itself. Characterizing this act as passive does not result in a desirable outcome since the poster knows or ought to know that the effect of his posting will be felt most acutely in the home jurisdiction of the target. If the target is unable to sue locally due to a strict adherence to the passive versus active test, the law might be seen as encouraging online defamatory speech by creating a jurisdictional hurdle to launching a legal claim.

The *Zippo* test also falls short when active sites are at issue, as the court in *People Solutions* recognized.[196] That court's request for evidence of actual sales within the jurisdiction illustrates that the mere potential to sell within a jurisdiction does not necessarily make a website active.[197] While the owner of an active website 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.

The problems with the *Zippo* test are 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.

---

193. *Id.* at 923.

194. *Id.*

195. *See* Braintech, Inc. v. Kostiuk [1999] 171 D.L.R. (4th) 46, 61 (B.C.C.A.); *see also* Barrett v. Catacombs Press, 44 F. Supp. 2d 717, 728 (E.D. Pa. 1999).

196. People Solutions, Inc. v. People Solutions, Inc., No. Civ. A. 399-CV-2339-L, 2000 WL 1030619, at *4 (N.D. Tex. Jul. 25, 2000).

197. *Id.*

Most countries have embraced the potential of e-commerce and adopted policies designed to encourage the use of the Internet for commercial purposes.[198] The *Zippo* test, however, inhibits e-commerce by effectively discouraging the adoption of interactive websites. Prospective website owners who are concerned about their exposure to legal liability will rationally shy away from developing active websites because such sites increase the likelihood of facing lawsuits in far-off jurisdictions. Instead, the test encourages passive websites that feature limited legal exposure and therefore present limited risk. Since public policy aims 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 reasons 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.[199]

---

198. The Canadian government's e-commerce policy is stated as follows:

> On September 22, 1998, the Prime Minister announced Canada's Electronic Commerce Strategy, outlining initiatives designed to establish Canada as a world leader in the adoption and use of electronic commerce. Working in close collaboration with the private sector, the federal government has concentrated on creating the most favorable environment possible in areas which are critical to the rapid development of e-commerce.

Industry Canada, Electronic Commerce in Canada: Canadian Strategy, *at* http://www.ecom.ic.gc.ca/english/60.html (last modified Feb. 14, 2001).

The U.S. government shares a similar e-commerce policy :

> Commerce on the Internet could total tens of billions of dollars by the turn of the century. For this potential to be realized fully, governments must adopt a non-regulatory, market-oriented approach to electronic commerce, one that facilitates the emergence of a transparent and predictable legal environment to support global business and commerce. Official decision makers must respect the unique nature of the medium and recognize that widespread competition and increased consumer choice should be the defining features of the new digital marketplace.

A Framework for Global Electronic Commerce, Jul. 1, 1997, *at* http://www.ecommerce.gov/framewrk.htm.

199. John Gedid noted the following at an international conference on Internet jurisdiction:

> The *Zippo* opinion is comprehensive, thorough and persuasive . . . . The court's review of precedents is sweeping and thorough, and its logic is compelling. The *Zippo* court fully understood and explained difficult

In the final analysis, however, the *Zippo* test simply does not deliver the desired effect. 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 unbeknownst to the individual user.[200] Given the value of personal data,[201] its collection is properly characterized as active, regardless of whether it occurs transparently or surreptitiously.[202] Similarly, sites such as online chatrooms may appear to be active, yet courts have consistently characterized such sites as passive.[203]

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

---

> precedents, so that they could be understood in terms of the *International Shoe* criteria. While there are some who would question the approach on the theories that it does not go far enough or that it goes too far, nevertheless, it is an attempt at stating a more comprehensive and coherent approach to Internet jurisdiction cases. The result was that the *Zippo* opinion is probably the most persuasive and influential opinion that has been published on the subject of cyberspace jurisdiction.

John L. Gedid, *Minimum Contacts Analysis in Cyberspace—-Sale Of Goods And Services*, Jul. 1997, *at* http://ilpf.org/events/jurisdiction/presentations/gedid_addl.htm.

See generally, Charles H. Fleischer, *Will The Internet Abrogate Territorial Limits on Personal Jurisdiction*?, 33 TORT & INS. L.J. 107 (1997); Michael J. Sikora III, *Beam Me into Your Jurisdiction*: *Establishing Personal Jurisdiction Via Electronic Contacts in Light of the Sixth Circuit's Decision in* Compuserve, Inc. v. Patterson, 27 CAP. U. L. REV. 163, 184-85 (1998).

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

201. *Id*.

202. Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1126 (W.D. Pa. 1997).

203. *See, e.g.*, Barrett v. Catacombs Press, 64 F. Supp. 2d 440 (E.D. Pa. 1999).

technology. In fact, it can be credibly argued that owners of websites must constantly re-evaluate their positions on the passive versus active spectrum as web technology changes.

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 now easily in excess of $100,000,[204] 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.

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 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. In the next section, this paper will offer an alternative test.

IV. TOWARD A TRIO OF TARGETS

Given the inadequacies of the *Zippo* passive versus active test, a new standard is needed to determine jurisdiction over Internet contacts. This section sketches the components of a targeting test by focusing on three factors: contracts, technology, and actual or implied knowledge.

A. Advantages of a Targeting Approach

The *Zippo* experience suggests that 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.

The solution submitted here is to move toward a targeting-based analysis. 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

---

204. David Legard, *Average Cost to Build E-commerce Site*: *$1 Million*, THE STANDARD, May 31, 1999 (on file with author).

reliance on effects-based analyses, the source of considerable uncertainty because Internet-based activity can ordinarily be said to cause effects in most jurisdictions.

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*.,[205] 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 wrongful conduct targeted at a plaintiff whom the defendant knows to be a resident of the forum state*.[206]

Targeting has also been raised in the context of online gambling cases, where United States courts have aggressively characterized offshore gambling sites as "targeting" local residents. In *People v. World Interactive Gaming*,[207] the court determined that illegal gambling websites targeting New York residents were within its jurisdiction. Allowing targeted websites to escape New York jurisdiction would "severely undermine this state's deep-rooted policy against unauthorized gambling, [and] also would immunize from liability anyone who engages in any activity over the Internet which is otherwise illegal in this state."[208] The court concluded that "[a] computer server cannot be permitted to function as a shield against liability, particularly in this case where respondents actively targeted New York as the location where they conducted many of their allegedly illegal activities."[209]

The strongest indication of a move toward a targeting test for Internet jurisdiction came in April 2001 in *American Information Corp. v. American Infometrics, Inc.*, a Maryland district court case.[210] The court left little

---

205. 223 F.3d 1082 (9th Cir. 2000).
206. *Id.* at 1087 (internal citations omitted) (emphasis added).
207. 714 N.Y.S.2d 844 (Sup. Ct. 1999).
208. *Id.* at ¶ 22.
209. *Id.* at ¶ 22.
210. 139 F. Supp. 2d 696 (D. Md. 2001).

doubt that targeting was a central consideration in its jurisdictional analysis, stating that:

> In the case at bar, non-customers cannot interact with the website except to submit their contract information to inquire about available services or jobs, according to Goreff, and no one from Maryland has ever inquired, or been a customer of American Infometrics. On a company's website, neither the "mere existence of an e-mail link, without more," nor "receiving . . . an indication of interest," without more, subjects the company to jurisdiction. The ability of viewers to ask about the company's services, particularly in the absence of any showing that anyone in Maryland has ever done so, does not subject the company to jurisdiction here.[211]

Fourth Circuit cases on minimum contacts supported the view that the American Informetrics' website did not create jurisdiction in Maryland. A company's sales activities focusing "generally on customers located throughout the United States and Canada without focusing on and targeting" the forum state did not yield personal jurisdiction.[212] A web presence that permits no more than basic inquiries from Maryland customers that has never yielded an actual inquiry from a Maryland customer, and that does not target Maryland in any way, similarly, should not yield personal jurisdiction.[213]

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 Guidelines 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."[214]

Similarly, a recent draft of the Hague Conference on Private International Law's Draft Convention on Jurisdiction and Foreign Judgments in-

---

211. *Id*. at 700.

212. *Id.*

213. *Id*.

214. 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 (last visited Nov. 26, 2001).

cludes provisions related to targeting.[215] 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."[216]

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 addressed through the implementation by issuers and financial service providers of precautionary measures that are reasonably designed to ensure that offshore Internet offers are not targeted to persons in the United States or to U.S. persons.[217]

The same targeting approach has been met with approval in Canada,[218] the United Kingdom,[219] and other parts of the world.[220] In Canada, the Canadian Securities Association has adopted a policy that requires online securities offerings to specifically exclude Canada in order to avoid the jurisdictional reach of Canadian securities regulators. According to the CSA, excluding Canada requires the use of a prominent disclaimer as well as reasonable precautions to ensure that securities are not sold to anyone in Canada.[221]

---

215. Hague Conference on Private International Law, *Preliminary Draft Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters*, Oct. 30, 1999, *at* http://www.hcch.net/e/conventions/draft36e.html.

216. *Id*. at art. 7(4)(a).

217. Press Release, U.S. Securities & Exchange Commission, Interpretation re: Use of Internet Websites to Offer Securities, Solicit Securities Transactions, or Advertise Investment Services Offshore, Release No. 33-17516, Mar. 23, 1998 (on file with author).

218. *See* British Columbia Securities Commission, *National Policy 47-210*: *Trading in Securities Using the Internet and Other Electronic Means*, *at* http://www.bcsc.bc.ca/Policy/Nin98-72.pdf (on file with author) [hereinafter *National Policy 46-210*].

219. Financial Services Authority, *Discussion Paper - The FSA's Approach To Regulation Of The Market Infrastructure*, Jan. 2000 (on file with author).

220. *See* IOSCO, *supra* note 55.

221. *See National Policy 46-210, supra* note 218.

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.[222] It was noted in the report:

> [E]ntities 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.[223]

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.[224]

B. The 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

---

222. *See* American Bar Association, *Achieving Legal and Business Order in Cyberspace*: *A Report on Global Jurisdiction Issues Created By the Internet* (on file with author). In the interests of full disclosure, it should be noted that the author was chair of the Sale of Services Working Group, one of nine working groups tasked with developing Internet jurisdiction recommendations.

223. *Id*.

224. Currently in beta, Google offers searchers the ability to configure their Google searching to translate automatically any results that appear in a foreign language. *See* Google, *at* http://www.google.com/machine_translation.html (last visited Nov. 26, 2001).

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.

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.[225] Consumer groups, meanwhile, have lobbied for a "rule of destination" approach that ensures that consumers can always sue in their home jurisdiction.[226] 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 *Neato* court did, that business must shoulder some of the risk arising from e-commerce transactions.[227]

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.

---

225. *See, e.g.*, Global Business Dialogue on Electronic Commerce, *at* http://www.gbde.org (last visited Nov. 26, 2001).

226. *See, e.g.*, Consumers International, *at* http://www.consumersinternational.org (last update Oct. 16, 2001).

227. Stomp Inc. v. Neato L.L.C., 61 F. Supp. 2d 1074, 1080-81 (C.D. Cal. 1999).

Although all three factors are important, no single factor should be determinative. 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 involve a contractual element, though evidence from the knowledge factor is likely to prove sufficient to identify the targeted jurisdiction.

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.

1. Contracts

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 both Canada and the United States have upheld the per se enforceability of an online contract,[228] commonly referred to as a clickwrap agreement. 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.*,[229] the court upheld a forum selection clause contained in an electronic ISP Terms of Service Agreement. The court feared that not

228. Graves v. Pikulski, 115 F. Supp. 2d 931 (S.D. Ill. 2000); Kilgallen v. Network Solutions, 99 F. Supp. 2d 125 (D. Mass. 2000); Rudder v. Microsoft Corp., [1999] 2 C.P.R. (4th) 474 (Ont.).

229. *Rudder,* 2 C.P.R. (4th) at 2.

upholding the clause would not only fail to advance the goal of "commercial 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."[230]

Courts in the United States have been similarly supportive of forum selection clauses found in clickwrap contracts. In *Kilgallen v. Network Solutions, Inc.,*[231] the court faced a dispute over the re-registration of a domain name. The plaintiff claimed that Network Solutions, the defendant, was in breach of contract when it transferred its domain name to a third party.[232] Network Solutions defended its actions by countering that the plaintiff had failed to make the annual payment necessary to maintain the domain.[233] Moreover, it sought to dismiss the action on the grounds that the registration agreement specified that all disputes were to be resolved in the Eastern District of Virginia.[234] The federal court in Massachusetts agreed, ruling that forum selection clauses are enforceable unless proven unreasonable under the circumstances.[235]

Notwithstanding the apparent support for enforcing forum selection clauses within clickwrap agreements, the presence of such a clause should only serve as the starting point for analysis. A court must first consider how assent to the contract was obtained. If the agreement is a standard clickwrap agreement in which users were required to positively indicate their agreement by clicking on an "I agree" or similar icon, the court will likely deem this to be valid assent. Many jurisdictional clauses are not found in a clickwrap agreement, however, but rather are contained in the terms of use agreement on the website. The terms typically provide that users of the website agree to all terms contained therein by virtue of their use of the website.

The validity of this form of contract, in which no positive assent is obtained and the website visitor is unlikely to have read the terms, stands on shakier ground. Three recent United States cases have considered this form of contract with the consensus moving toward nonenforcement. In *Ticketmaster v. Tickets.com*,[236] a dispute over links between rival event

---

230. *Id.* at ¶¶ 14-16.
231. *Kilgallen,* 99 F. Supp. at 129.
232. *Id.* at 126.
233. *Id.*
234. *Id.*
235. *Id.* at 129.
236. No. CV 99-7654 HLH, 2000 WL 525390 (C.D. Cal. Mar. 27, 2000).

ticket sites, the court considered the enforceability of the terms and conditions page found on the Ticketmaster site and concluded that the forum selection clause was not enforceable.[237] The terms and conditions set forth on the Ticketmaster home page provided that users going beyond the home page were prevented from making commercial use of the information and were prohibited from deep linking.[238] Ticketmaster defended on the grounds that courts enforce "shrink-wrap licenses" where "packing on the outside of the CD stated that opening the package constitutes adherence to the license agreement . . . contained therein."[239]

The court found that Ticketmaster's system of notification did not create a binding contract on the user.[240] Unlike the agreement on the Ticketmaster site, "the 'shrink-wrap license agreement' is open and obvious and in fact hard to miss."[241] Ticketmaster's terms and conditions did not require the user to "click on 'agree' to the terms and conditions before going on" as many websites do.[242] The court further noted that customers were required "to scroll down the home page to find and read" the terms and conditions.[243] Given this system, "[m]any customers . . . are likely to proceed to the event page of interest rather than reading the 'small print.' *It cannot be said that merely putting the terms and conditions in this fashion necessarily creates a contract with any one using the website*."[244] This case suggests that mere inclusion of a forum selection or other jurisdictional clause, within the terms and conditions, may not be enforceable because the term is not brought sufficiently to the attention of the user.

Several months after the Ticketmaster decision, another federal court adopted a different approach in *Register.com, Inc. v. Verio, Inc.*[245] This case involved a dispute over Verio's use of automated software to access and collect the domain name registrant's contact information contained in the Register.com WHOIS database. Verio collected the data to use for marketing purposes.[246] Register.com provided the following terms and conditions for those wishing to access its WHOIS database:

---

237. *Id.*
238. *Id.* at *3.
239. *Id.*
240. *Id.*
241. *Id.*
242. *Id.*
243. *Id.*
244. *Id.* (emphasis added)
245. 126 F. Supp. 2d 238 (S.D.N.Y. 2000).
246. *Id.* at 252.

> By submitting a WHOIS query, you agree that you will use this data only for lawful purposes and that, under no circumstances will you use this data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via direct mail, electronic mail, or by telephone; or (2) enable high volume, automated, electronic processes that apply to Register.com (or its systems). The compilation, repackaging, dissemination or other use of this data is expressly prohibited without the prior written consent of Register.com. Register.com reserves the right to modify these terms at any time. By submitting this query, you agree to abide by these terms.[247]

Unlike the *Ticketmaster* case, the court in Register.com ruled that these terms were binding on users, despite the absence of a clear manifestation of assent.[248] The court relied on the users' willingness to engage with the website, by using the WHOIS database, as evidence that the user could impliedly be considered to have agreed to the terms of the contract.

Most recently, in *Specht v. Netscape Communications Corp.*,[249] the same federal court in New York distinguished between clickwrap contracts, which it argued features positive assent in the form of clicking "I agree", and browsewrap contracts, in which the user is merely alerted to the existence of a contract through a disclaimer or other notice. The court ruled that the latter form of contract, employed in this case by Netscape Communications, was not binding against the user since Netscape had failed to obtain the user's positive assent. Netscape argued "the mere act of downloading indicates assent."[250] As the court noted, however, "downloading is hardly an unambiguous indication of assent" because "[t]he primary purpose of downloading is to obtain a product, not to assent to an agreement."[251] The court criticized Netscape for not drawing the user's attention to the clickwrap contract, for not requiring an affirmative manifestation of assent, and for only making a "mild request" that the user review the terms of the licensing agreement.[252]

---

247. *Id.* at 242-43.

248. *Id.*

249. 150 F. Supp. 2d 585 (S.D.N.Y. 2001).

250. *Id.* at 595.

251. *Id.*

252. Furthermore, unlike the user of Netscape Navigator or other click-wrap or shrink-wrap licensees, the individual obtaining SmartDownload is not made aware that he is entering into a contract. SmartDownload is available from Netscape's website free of charge. Before downloading the software, the user need not view any license agreement terms or even any reference to a license agreement, and need not do anything to manifest assent to such a license agreement other than actually taking possession of the product.

While the form of assent may call into question the validity of an online contract, the actual terms of the contract itself are of even greater consequence. Courts are required to consider the reasonableness of the terms of a contract as part of their analysis. Within the context of a jurisdictional inquiry, several different scenarios may lead the court to discount the importance of the contract as part of a targeting analysis. A court may simply rule that the forum selection clause is unenforceable in light of the overall nature of the contract.

This occurred in *Mendoza v. AOL*,[253] a recent California case involving a disputed ISP bill. After Mendoza sued AOL in California state court, AOL responded by seeking to have the case dismissed on the grounds that the AOL service contract contains a forum selection clause that requires all disputes arising from the contract to be brought in Virginia.[254] The court surprised AOL by refusing to enforce the company's terms of service agreement on the grounds that "it would be unfair and unreasonable because the clause in question was not negotiated at arm's length, was contained in a standard form contract, and was not readily identifiable by plaintiff due to the small text and location of the clause at the conclusion of the agreement."[255] Though cases such as *Mendoza* are the exception rather than the rule, they do point to the fact that a forum selection clause will not always be enforced, particularly in consumer disputes where the provision may be viewed by a court as too onerous given the small amount at issue.[256]

From the user's vantage point, SmartDownload could be analogized to a free neighborhood newspaper, readily obtained from a sidewalk box or supermarket counter without any exchange with a seller or vendor. It is there for the taking. The only hint that a contract is being formed is one small box of text referring to the license agreement, the text that appears below the screen used for downloading and that a user need not even see before obtaining the product: "Please review and agree to the terms before downloading and using the software for the Netscape Smart Download software license agreement." Couched in the mild request, "[p]lease review," this agreement reads as a mere invitation, not as a condition. The language does not dictate that a user must agree to the license terms before downloading and using the software. While clearer language appears in the License Agreement itself, the language of the invitation does not require the reading of those terms or provide adequate notice either that a contract is being created or that the terms of the License Agreement will bind the user. *Id.* at 595-96.

253. Mendoza v. AOL (Cal. Super. Ct.) (unreported, on file with author).

254. *Id.*

255. *Id*.

256. For another example in which a Massachusetts state court refused to enforce the AOL forum selection clause in a class action suit over AOL system software see *Williams v. AOL*, No. 00-0962 (Mass. Super. Ct. Feb 2001) (on file with author).

Courts may also be unwilling to enforce such clauses where the court perceives the clause to be an attempt to contract out of the jurisdiction with the closest tie to the parties. Courts must be vigilant to ensure that forum selection clauses are not used to create a "race to the bottom" effect whereby parties select jurisdictions with lax regulations in an attempt to avoid more onerous regulations in the home jurisdictions of either the seller or purchaser.[257] Aggressive courts may also be unwilling to enforce a clause with no tie to the jurisdiction. In *Standard Knitting, Ltd. v. Outside Design, Inc.*,[258] for example, a trademark infringement case involving a Canadian plaintiff, the federal court in Pennsylvania transferred the case to Washington state after it found that venue would be more convenient for the parties there.

An alternative to dictating jurisdiction terms to the consumer and risking a court's refusal to enforce those terms is to provide the consumer with the opportunity to self-declare his or her jurisdiction. The advantage of this approach is that the business can refuse to deal with the consumer if the consumer self-declares a jurisdiction with increased legal risk for the business. For example, Expedia, a leading online travel site, asks users to indicate their home jurisdiction prior to using the service.[259] If the user indicates the United States as her home jurisdiction, she remains at the Expedia.com site. If the user lists Canada as her home jurisdiction, she is transferred to Expedia.ca, a Canada-specific site. If the user lists Mexico as her home jurisdiction, the site advises her that Expedia is unable to provide service at the present time due to regulatory constraints.

An additional advantage to this approach is that the business should be able to rely on the consumer's self-declaration. If the consumer intentionally proffers incorrect information—he resides in Mexico but declares that the United States is his home jurisdiction—Expedia should be able to rely on the consumer statement to ensure that they do not run afoul of Mexican regulatory law because they were clearly targeting their activity to the United States.[260]

---

257. For example, the *Wall Street Journal* reports that Bermuda has become a haven for dot-com operations seeking to avoid tax and other regulatory measures in North America. Michael Allen, *As Dot-Coms Go Bust in the U.S., Bermuda Hosts a Little Boomlet*, WALL ST. J., Jan. 8, 2001, at A4.

258. No. 00-2288, 2000 WL 804434, at *5 (E.D. Pa. Jun. 23, 2000).

259. *See* Expedia, *at* http://www.expedia.com (last visited Nov. 26, 2001).

260. The legal implications of a mistaken self-declaration are more problematic. The possibility of a mistaken self-declaration is a genuine possibility where the question posed requires a layperson to apply legal principles. For example, the answer to "where do you habitually reside?" might differ from the answer to the question "where do you live?" If the consumer is unfamiliar with the legal standards for habitual residence, he

Despite the potential advantages of self-declaration, courts have ruled that companies cannot rely on the self-declaration of a user where they know or suspect it to be false. For example, in *People v. World Interactive Gaming*,[261] an online gambling case, the court rejected attempts by the online casino to limit registration to gamblers residing in a state that permits gambling. In particular, the court noted that the site required users to enter their permanent addresses when they opened accounts.[262] Users who claimed residency in "a state that permitted land-based gambling, such as Nevada, [were] granted permission to gamble."[263] Users who indicated that their permanent addresses were in states, "such as New York, which does not permit land-based gambling, [were] denied permission to gamble." The court noted, however, that

> because the software does not verify the user's actual location, a user initially denied access could easily circumvent the denial by changing the State entered to that of Nevada, while remaining physically in New York State. The user could then log onto the GCC casino and play virtual slots, blackjack or roulette. This raises the question if this constitutes a good-faith effort not to engage in gambling in New York.[264]

This court's approach to self-declaration is reminiscent of the court's approach in the *iCraveTV* case, which, as discussed earlier, was dismissive of that company's attempts to use contract to limit its signal to Canadians.[265]

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 foregoing review of recent online contracting case law reveals, 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.

---

may mistakenly self-declare his jurisdiction. Under such circumstances, it is unclear whether the consumer should bear the legal burden of the mistaken self-declaration should a dispute arise.

261. 714 N.Y.S.2d 844 (Sup. Ct. 1999).

262. *Id.*

263. *Id.* at 847.

264. *Id.*

265. *See id; see also supra* Part I.B.

2. Technology

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. The rapid emergence of these new technologies challenges what has been treated as a truism in cyberlaw—that the Internet is borderless and thus impervious to attempts to impose on it real-space laws that mirror traditional geographic boundaries.[266]

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 possible online. In *American Libraries Ass'n v. Pataki*,[267] a Commerce Clause challenge to a New York state law targeting Internet content classified as obscene, the court characterized geography on the Internet in the following manner:

> 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.[268]

Although the ALA court's view of the Internet 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.[269] 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

---

266. *See generally* Johnson & Post, *supra* note 49.

267. Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160 (S.D.N.Y. 1997).

268. *Id.* at 170.

269. Bob Tedeschi, *E-commerce*: *Borders Returning to the Internet*, N.Y. TIMES, Apr. 2, 2001 (on file with author).

now be better positioned to apply their offline regulations to the online environment.[270]

Since both business and government share a vested interest in bringing geographic borders to the online environment (albeit for different reasons), it should come as little surprise that these technologies have so quickly arrived onto the marketplace. In fact, they have become available before the Internet community has engaged in a current discussion on the benefits, challenges, and consequences of creating borders or "zoning" the Internet with these new technologies.[271] This is most unfortunate since geographic bordering technologies raise important privacy considerations that have, as yet, attracted little debate.[272]

Although critics often point to the inaccuracy of these technologies, few users of the technology actually demand perfection.[273] Businesses want either to target their message to consumers in a specific jurisdiction

---

270. In addition to the discussion below, see Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 YALE L.J. 785, 810-12 (2001).

271. Although in fairness, there are some that saw these developments coming many years ago. For example, Professor Lawrence Lessig, in the same Stanford Law Review issue featuring Post's and Johnson's *Law and Borders* article, *supra* note 49, commented that:

> In its present design, cyberspace is open, and uncontrolled; regulation is achieved through social forces much like the social forms that regulate real space. It is now unzoned: Borders are not boundaries; they divide one system from another just as Pennsylvania is divided from Ohio. The essence of cyberspace today is the search engine—tools with which one crosses an infinite space, to locate, and go to, the stuff one wants. The space today is open, but only because it is made that way. Or because we made it that way. (For whatever is true about society, at least cyberspace is socially constructed.)
>
> It could be made to be different, and my sense is that it is. The present architecture of cyberspace is changing. If there is one animating idea behind the kinds of reforms pursued both in the social and economic spheres in cyberspace, it is the idea to increase the sophistication of the architecture in cyberspace, to facilitate boundaries rather than borders. It is the movement to bring to zoning to cyberspace.

Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1408-9 (1996) [hereinafter Lessig, *Zones*]; *see also*, LESSIG, *supra*, note 57, at 56-57.

272. Stefanie Olsen, *Geographic Tracking Raises Opportunities, Fears*, CNET NEWS.COM, Nov. 8, 2000, *at* http://news.cnet.com/news/0-1005-200-3424168.html.

273. As Lessig points out, "[a] regulation need not be absolutely effective to be sufficiently effective." Lessig, *Zones, supra* note 271, at 1405. The same applies to bordering technologies; whether used for targeted marketing or to ensure legal compliance, they need not be perfect.

or to engage in "jurisdictional avoidance."[274] Effective jurisdictional avoidance provides the means to exclude the majority of visitors who cannot be verified as residing in the desired jurisdiction. For example, iCraveTV did not use identifying technologies, choosing instead to rely on the user clickwrap agreements.[275] JumpTV, a new Canadian entry into the webcasting market, has indicated that it will use identifying technologies to ensure that only Canadians access its signal.[276] While this may exclude some Canadians who cannot be positively identified as coming from Canada, it will provide the company with a greater level of assurance in meeting its goal of limiting its online signal.

Government, on the other hand, may often want to engage in jurisdictional identification so that it can more easily identify when its laws are triggered. For example, Nevada recently enacted legislation that paves the way for the Nevada Gaming Commission to legalize online gambling.[277] Central to the new legislation is jurisdiction identification. Section 3(2) provides:

> The commission may not adopt regulations governing the licensing and operation of interactive gaming until the commission first determines that:
>
> (a) Interactive gaming can be operated in compliance with all applicable laws;
>
> (b) Interactive gaming systems are secure and reliable, and provide reasonable assurance that players will be of lawful age and communicating only from jurisdictions where it is lawful to make such communications.[278]

To reach the determination required by subsection (b), an analysis of available geographic identification technology will be necessary.

Geographic identification technologies can be grouped into at least three categories: a) user identification, which is typically based on IP address identification; b) self-identification, which often occurs through attribute certificates; and c) offline identification.

---

274. *See* Tedeschi, *supra* note 269.

275. Twentieth Century Fox Film Corp. v. iCraveTV, No. 00-121, 2000 U.S. Dist. LEXIS 1013 (W.D. Pa. Jan. 28, 2000).

276. Matthew Fraser, *Jump TV Takes On Vested Interests*, FIN. POST, Jan. 29, 2001, at C02.

277. *Nevada Governor Signs Internet Gambling Bill*, SAN JOSE MERCURY NEWS, June 15, 2001, *available at* http://www.siliconvalley.com/docs/news/tech/060919.htm.

278. H.R. 466, 71st Ass., Reg. Sess., (Nev. 2001), *available at* http://www.leg.state.nv.us/71st/bills/AB/-AB446_EN.html.

a) User Identification

User identification has been utilized on a relatively primitive scale for some time. For example, for many years, in order to comply with United States regulations prohibiting the export of strong-encryption web browsers, Microsoft used Internet Protocol (IP) lookups, which determine user locations by cross-checking their IP address against databases that list Internet service provider locations.[279] Although imperfect, the process was viewed as sufficiently effective to meet the standards imposed by the regulations. Recently, several companies have begun offering more sophisticated versions of similar technologies. Brief descriptions of some of the leading companies offering geo-identification technologies follow.

i) Infosplit

Infosplit claims to have the ability to accurately pinpoint the location of any IP address using a proprietary set of techniques and algorithms.[280] The technology provides instant and precise geographic identification and page routing in a process invisible to the web user. The company maintains 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.

The Infosplit technology returns a geographic location by sending the user's IP address to the various algorithms including Trace Route, the ARIN/RIPE/APNIC database, and a DNS reverse look-up. The ARIN/RIPE/APNIC component analyzes information obtained from the ARIN/RIPE/APNIC database. The DNS Reverse Lookup component analyzes publicly available domain name registration data. The Trace Route algorithm discovers and interprets the trail left by network packets associated with the viewer's web page request. By combining the results of all three algorithms, Infosplit can provide a more effective result than with an IP lookup alone.

ii) NetGeo

NetGeo provides geographic identification primarily through IP address analysis.[281] The company features a database and collection of Perl scripts used to map IP addresses and domain names to geographical loca-

---

279. Anick Jesdanun, *The Potential and Peril of National Internet Boundaries,* S.F. EXAMINER, Mar. 4, 2001, *available at* http://www.examiner.com/business/default.jsp?story=b.net.0107.

280. *See* Infosplit, *at* http://www.infosplit.com (last visited Nov. 26, 2001).

281. *See* NetGeo, *at* http://www.netgeo.com (last visited Nov. 26, 2001).

tions. To determine the latitude/longitude values for a domain name, NetGeo first searches for a record containing the target name in its own database. The NetGeo database caches the location information parsed from the results of previous *whois* lookups, which provide IP address information to minimize the load on *whois* servers. If a record for the target domain name is found in the database, NetGeo returns the requested information. If no matching record is found in the NetGeo database, NetGeo performs one or more *whois* lookups using the InterNIC and/or RIPE *whois* servers, until a *whois* record for the target domain name is found.

After obtaining a record from a *whois* server, the NetGeo Perl scripts parse the *whois* record and extract location information and the date of last update. The NetGeo parser attempts to extract the city, state, and country from the text of the *whois* record. For United States addresses, the parser also extracts the zip code, if possible. If the parser is unable to parse an address, it attempts to find an area code or international phone code in the contact section. The phone code is mapped to a country and then the parser attempts to parse the address again, using the hint provided by the phone code. The parser also guesses the country from email addresses with country-code TLDs found in the contact section.

iii) EdgeScape

Akamai, a network caching service, also provides a geographic identification service called EdgeScape.[282] EdgeScape maps user IP addresses to their geographic and network point of origin. This information is assembled into a database and made available to EdgeScape customers. Each time a user accesses the client's website, EdgeScape provides data detailing the country from which the user is accessing the site, the geographic region within that country (i.e., state or province), and the name of user's origin network. The company claims accuracy rates as high as 99 percent at the country level, though accuracy diminishes at the state and local levels.

iv) Digital Envoy

Founded in 1999, Atlanta-based Digital Envoy's core competency is geographic identification on the web.[283] The company's flagship product, NetAcuity, claims country targeting capability exceeding 99% accuracy with targeting regions, states, or cities as another possibility. The company's primary focus has been the corporate marketing sector, which re-

---

282. *See* Akamai, *at* http://www.akamai.com (last visited Nov. 26, 2001).

283. *See* Digital Envoy, *at* http://www.digitalenvoy.com/prod_netacu.htm (last visited Nov. 26, 2001).

lies on Digital Envoy to allow for geographically targeted advertising.[284] The company's technology is also used by CinemaNow Inc., a California-based online distributor of feature-length films. It uses the technology to limit distribution of the films to ensure it is compliant with distribution-license rules that vary by country.[285]

v) Quova

One of the best-funded companies offering geographic identification technologies is Quova,[286] a California-based startup that purchased European leader RealMapping in early 2001.[287] The company spent nine months scanning the Internet's 4.2 billion IP addresses, yielding a detailed physical map of the Internet.[288] The result was the company's flagship product GeoPoint, which boasts 98 percent accuracy at determining web surfers' countries and 85 percent accuracy at the city level.[289] Currently in development is new technology that will allow for greater identification of AOL users, whose geographic origins are typically more difficult to identify than most other ISPs.[290]

b) Self-identification

Unlike user identification technologies, which identify the user's geographic location without requesting permission to do so, self-identification uses technologies that enable users to provide geographic identification directly to the website. This is most frequently accomplished through the use of attribute certificates, which, as Michael Froomkin explains, provide information about the attributes of a particular user without revealing his actual identity:

> Although identifying certificates are likely to be the most popular type of certificate in the short run, in the medium term CAs are likely to begin certifying attributes other than identity. An authorizing certificate might state where the subject resides, the subject's age, that the subject is a member in good standing of an

---

284. Nicole Harris, *Digital Envoy Offers a Way To 'Geo-Target' Web Surfers*, WALL ST. J., Apr. 12, 2001, at B5.

285. Patricia Jacobus, *Cinema Now Appeases Studios by Locating Web Surfers,* CNET NEWS.COM, Feb. 26, 2001 (on file with author).

286. *See* Quova, *at* http://www.quova.com (last visited Nov. 26, 2001).

287. Stefanie Olsen, *Tracking Web Users into European Territory,* CNET NEWS.COM, Apr. 3, 2001 (on file with author).

288. *See* Olsen, *supra* note 272.

289. *See* Olsen, *supra* note 287.

290. *Id.*

> organization, that the subject is a registered user of a product, or that the subject possesses a license such as bar membership.[291]

Froomkin points out that attribute certificates have many potential applications, chief among them geographic identification.[292] Self-identification technology represents a middle ground between user identification, which puts the power of identification solely in the hands of the website, and self-declaration, in which the user declares where they reside but without any independent or technological verification of the accuracy of the declaration. The danger with self-identification technologies is that if they become popular, they may also quickly cease to be voluntary since businesses may begin to require that their users supply the data contained in an attribute certificate in order to obtain service.[293]

c) Offline Identification

Offline identification combines an online presence with certain offline knowledge to form a geographic profile of a user. The best example of offline identification is credit card data. Since credit cards remain the preferred payment mechanism for most online transactions, sellers are regularly asked to verify the validity of a user's credit card. The verification process for online purchases includes an offline component, as the address submitted by the user is cross-checked with the address on file to confirm a match prior to authorization of the charge.[294] This process provides websites with access to offline data such as the user's complete address—which is confirmed through a third party, the financial intermediary.

While this system may be effective for sites actively engaged in e-commerce and for those whose geographic risks are confined strictly to

---

291. A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce,* 75 OR. L. REV. 49, 62 (1996).

292. It is illegal to export high-grade cryptography from the United States without advance permission from the federal government, but there are no legal restrictions on the distribution of strong cryptography to resident aliens or United States citizens in the United States. The lack of a reliable means to identify the geographical location of a person from an Internet address creates a risk of prosecution for anyone making cryptographic software available over the Internet. For example, if Alice is making high-grade cryptography available for distribution over the Internet, she might protect herself from considerable risk by requiring that Bob produce a valid certificate from a reputable CA, stating that he is a United States citizen or green card holder residing in the United States, before allowing him to download the cryptographic software. *Id.*

293. *See* LESSIG, *supra* note 57, at 42.

294. *Credit Card Fraud Crippling Online Merchants*, E-COMMERCE TIMES, Mar. 20, 2000, *at* http://www.ecommercetimes.com/news/articles2000/000320-2.shtml ("At present, credit card companies only verify if a credit card number is correct and then match the number against the customer's billing address.").

those circumstances when they are selling into a particular jurisdiction, the use of credit-card data is of limited utility to those who do not actively sell online or those who are concerned about jurisdictional issues prior to the submission of a credit card number and address information. This would include sites such as JumpTV, which use an advertiser-supported model so that they do not require users to provide credit card data, yet are concerned with the availability of the site outside Canada.

Two other offline identifiers present similar possibilities of geographic identification, but simultaneously raise serious privacy concerns. At one time, Microsoft included a feature in its software that could be used to transmit personal information via the Internet without the user's knowledge.[295] The feature enabled Microsoft software such as Word or Excel to issue identification numbers unique to the software and the computer on which the software was installed. During the online registration process, the number, known as a Global Unique Identifier (GUID), was transferred to Microsoft along with the user's name, address, and other personal information. Microsoft could then identify users by matching their GUID with the information stored in the Microsoft-controlled database.[296] Following numerous complaints from the privacy rights community, the software giant altered the feature to better protect user privacy.

Intel found itself embroiled in a similar privacy controversy when it was revealed that the company was able to identify people online by using a Processor Serial Number (PSN). A PSN was a number burned onto an Intel processor chip at the time of manufacture and designed to provide authentication in Internet communication and commerce. The PSN identified a person on the Internet by the actual hardware of the computer they were using, limiting their ability to protect their anonymity online and providing for the prospect of quick identification.[297] Intel responded to privacy concerns by switching the default setting on the PSN such that users were required to proactively initiate the feature to track users.

Though clearly limited in scope, offline identifiers have the advantage of being the most inexpensive method of identifying geographic location because they rely on offline data collected independently of online activities. Precisely because they merge offline and online, these technologies raise profound privacy concerns, creating the prospect of personally iden-

---

295. M. Ricciuti, *Microsoft Admits Privacy Problem, Plans Fix,* CNET NEWS.COM, Mar. 7, 1999, *at* http://news.cnet.com/news/0-1006-200-339622.html.

296. *Id.*

297. Privacy Exchange, *Privacy and the Internet Tutorial*: *Protecting Web Privacy - Processor Serial Number* (on file with author).

tifiable information being transferred along with non-identifiable geographic data.

d) Targeting and Technology

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 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. Geographic 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, from doing so. A fair and balanced targeting jurisdiction test demands that they do just that.

It is important to note that parties are not typically required to use geographic identification technologies.[298] In many instances, they do not care who accesses their site and thus will be unwilling and may not have the incentive to incur the expense of installing such systems. In other instances, the party may be acutely aware of the need to identify users from a jurisdiction that bans access to certain content or certain activities. In such instances, the party may wish to limit access to those users it can positively identify from a legally safe jurisdiction.

The inclusion of technology into the targeting test does not, therefore, obligate parties to use the technology. Rather, it forces parties to acknowledge that such technologies are available and that prudence may dictate using them in some capacity. Moreover, the test does not prescribe any specific technology—it only requires that consideration be given to the technologies used and available at a particular moment in time. This technology neutral prong of the targeting test, which does not prescribe a particular type of technology but rather the outcome, also provides an effective counterbalance to the contract and knowledge factors. It removes the ability to be willfully blind to users who enter into a clickwrap contract stating that they are from one jurisdiction, while the technological evidence suggests something else entirely.

---

298. Except where as required by law. *See*, *e.g.*, Jesdanun, *supra* note 279.

3. Actual or Implied Knowledge

The third targeting 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,[299] the geographic identification technologies described above 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 implied knowledge factor is most apparent in the defamation tort cases that follow from the *Calder* decision. In those cases, courts have accepted that the defaming party is or should be aware that the injury inflicted by her speech would be felt in the jurisdiction of her target. Accordingly, in such cases a party would be unable to rely on a contract that specifies an alternate jurisdiction as the choice of forum.

The court's desire to dismiss any hint of willful blindness is evident in the *People v. World Interactive Gaming* case, referred to earlier.[300] In that case, the online casino argued that it had limited access to only those users that had entered an address of a jurisdiction where gambling was permitted. The court saw through this ruse, however, firmly stating that:

> [t]his Court rejects respondents' argument that it unknowingly accepted bets from New York residents. New York users can easily circumvent the casino software in order to play by the simple expedient of entering an out-of-state address. Respondents' violation of the Penal Law is that they persisted in con-

---

299. *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 acquire its benefits.

Id. at 605-06.

300. People v. World Interactive Gaming, 714 N.Y.S.2d 844 (Sup. Ct. 1999).

> tinuous illegal conduct directed toward the creation, establishment, and advancement of unauthorized gambling.[301]

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 *Starmedia Network v. Star Media, Inc.,*[302] an April 2001 federal case from New York, the court asserted jurisdiction over an alleged out-of state trademark infringer, noting that:

> [t]he 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.[303]

Although 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. As discussed above, most telling may be credit card data that the purchaser typically provides to the seller. In addition to the credit card number and expiration date, the purchaser is often also required to supply billing address information so that the validity of the card can be verified before authorization. Since the seller is supplied with a real-space billing address for digital transactions, there remains the opportunity to forego the sale if there is a jurisdictional concern. For example, the Washington Capitals hockey team recently rejected attempts by rival fans from Pittsburgh to purchase tickets on the team's website. The site was set to reject purchase attempts from customers entering a Pittsburgh-area code.[304] While some sellers may be loathe to use consumer payment information in this fashion, the approach reflects a more general trend toward recognizing

---

301. *Id*.

302. No. 00 Civ. 4647 (DLC), 2001 WL 417118 (S.D.N.Y. Apr. 23, 2001).

303. *Id.* at *4.

304. Thomas Heath, *Capitals Owner Puts Pittsburgh Fans on Ice*, THE WASH. POST, Apr. 14, 2001 (on file with author).

the important role that payment intermediaries such as credit card companies play in the consumer e-commerce process.[305]

V. CONCLUSION

With courts increasingly resisting the *Zippo* passive versus active approach to Internet jurisdiction, the time for the adoption of a new targeting-based test has arrived. Unlike the *Zippo* test, which suffers from a series of drawbacks including inconsistent and undesirable outcomes as well as the limitations of a technology-specific approach, a targeting-based analysis provides all interested parties—including courts, e-commerce companies, and consumers—with the tools needed to conduct more effective legal risk analysis.

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 are compliant with local law.

Consumers also benefit from this approach since they receive the reassurance that online companies that target them will be answerable to their local law. The test is sufficiently flexible to allow companies to deploy as many or as few precautions as needed. For example, if the company is involved in a highly regulated or controversial field, it will likely want to confine its activities to a limited number of jurisdictions, avoiding locations with which it is unfamiliar. Under the targeting test, the company could adopt a strategy of implementing technological measures to identify its geographic reach, while simultaneously incorporating the desired limi-

---

305. In March 2001, the *Electronic Commerce and Information, Consumer Protection Amendment and Manitoba Evidence Amendment Act* (S.M. 200, c. E55. 77) and the *Internet Agreements Regulations* (Man. Reg. 176/2000) took effect within the province of Manitoba. Designed to foster an online environment where consumer confidence will flourish, the new laws apply exclusively to the online retail sale of goods or services or the retail lease-to-own of goods between buyers and sellers. Under the new rules, binding e-commerce transactions require the seller to provide certain obligatory information to the buyer under threat of a purchaser contract cancellation remedy.

tations into its contract package. Conversely, companies with fewer legal concerns and a desire to sell worldwide can still accomplish this goal under the targeting test analysis. These companies would sell without the technological support, incurring both the benefits and responsibilities of a global e-commerce enterprise.

Notwithstanding the advantages of a targeting test, there are, nevertheless, some potential drawbacks. First, the test accelerates the creation of a bordered Internet. Although a bordered Internet carries certain advantages, it is also subject to abuse because countries can use bordering technologies to keep foreign influences out and suppress free speech locally.[306] Second, the targeting test might also result in less consumer choice since many sellers may stop selling to consumers in certain jurisdictions where risk analysis suggests that the benefits are not worth the potential legal risks.

The most effective illustration of the advantages of a targeting test comes from considering how the test would apply to the two cases outlined at the start of this paper. Although the outcomes would remain unchanged, the analysis would be different, providing courts and companies alike with a clearer sense of where the boundaries lie. In the *Yahoo! France* case, the company argued vociferously that it should not be subject to the jurisdiction of the French court because its flagship dot-com site had not targeted France. Applying the targeting test's three factors, however, suggests that the French court handled the case correctly. Yahoo! utilizes a terms and conditions page stipulating that the site is governed by United States law, but as the *Ticketmaster* case demonstrated, that form of contract may not be enforceable. Moreover, the company employed some technological measures to identify the geographic location of visitors accessing its website in order to provide French visitors with French language targeting advertising.[307] The company was clearly cognizant that some visitors were French residents. Though the outcome may be the same, the use of a targeting test would have provided the company with a more effective tool to gauge the likelihood of a foreign court asserting jurisdiction.

---

306. *Cf.* Joel R. Reidenberg, *The Yahoo Case and the International Democratization of the Internet* (Fordham Law & Econ. Working Paper No. 11, 2001) (arguing that online bordering facilitates democracy by allowing democratically elected governments to implement policy choices that affect their citizens both offline and online), *available at* http://papers.ssrn.com/paper.taf?ABSTRACT_ID=267148 (last visited Nov. 26, 2001).

307. *Yahoo!France Interim Order*, *supra* note 23, at 4 ("Whereas Yahoo is aware that it is addressing French parties because upon making a connection to its auctions site from a terminal located in France it responds by transmitting advertising banners written in the French language.").

Applying the targeting test to the *iCraveTV* case, the United States court might still have asserted jurisdiction over the company, but it would have done so for different reasons. Using a targeting analysis, the company would have pointed to its contracts in which users self-affirm that they were Canadian residents as well as its (rather porous) technological measures that were designed to keep its signal within Canada. A court would have likely reviewed the iCraveTV effort and, noting that the company was well aware that United States residents were accessing the site and that its technical measures were ineffective, asserted jurisdiction. The case also highlights how a successor to iCraveTV could effectively limit its jurisdictional liability by employing stronger technological measures to keep its signal from straying across the border.

Although the targeting test will not alter every jurisdictional outcome, it will provide all parties with greater legal certainty and a more effective means of conducting legal risk assessments. The move toward using contract and technology to erect virtual borders may not answer the question of whether there is a there there, but at least it will go a long way in determining where the there might be.