

Boston College International and Comparative Law Review

Volume 31 | Issue 2

Article 8

5-1-2008

The Continuing Conundrum of International Internet Jurisdiction

Kevin A. Meehan

Follow this and additional works at: <http://lawdigitalcommons.bc.edu/iclr>



Part of the [International Law Commons](#), and the [Internet Law Commons](#)

Recommended Citation

Kevin A. Meehan, *The Continuing Conundrum of International Internet Jurisdiction*, 31 B.C. Int'l & Comp. L. Rev. 345 (2008), <http://lawdigitalcommons.bc.edu/iclr/vol31/iss2/8>

This Notes is brought to you for free and open access by the Law Journals at Digital Commons @ Boston College Law School. It has been accepted for inclusion in Boston College International and Comparative Law Review by an authorized administrator of Digital Commons @ Boston College Law School. For more information, please contact nick.szydowski@bc.edu.

THE CONTINUING CONUNDRUM OF INTERNATIONAL INTERNET JURISDICTION

KEVIN A. MEEHAN*

Abstract: International law has long been concerned with resolving issues of international jurisdiction; however, the unique circumstances involved in Internet cases have thrown a wrench in the traditional machinery of international jurisdiction law. Domestic courts continue to struggle with the issue, and the international community has dragged its feet on developing a uniform standard for determining international Internet jurisdiction. Further complicating matters, states often have divergent substantive Internet regulations and policies. This Note discusses and analyzes the leading cases and theories on international Internet jurisdiction and concludes that none of the current proposed solutions alone provide a satisfactory solution. Nevertheless, an international resolution on internet jurisdiction that borrows elements from each of these proposals could be successfully established.

INTRODUCTION

Over the last decade, the Internet has exploded, making our world smaller.¹ The touch of a few keystrokes enables people to communicate, engage in commerce, and interact with others around the world.² This ability to cross international borders without leaving one's living room has created a jurisdictional void that has yet to be filled.³ When an international Internet conflict arises, several difficult questions must be answered: Where can the plaintiff sue? Which country's laws apply?⁴ Although these questions are not unique to Internet cases, the circumstances typically involved in such cases have made answers and consen-

* Kevin A. Meehan is an Articles Editor for the *Boston College International & Comparative Law Review*.

¹ See Tim Gerlach, Note, *Using Internet Content Filters to Create E-Borders to Aid International Choice of Law and Jurisdiction*, 26 WHITTIER L. REV. 899, 899 (2005).

² See *id.*

³ See *id.*

⁴ See *id.* at 900.

sus opinion far more difficult than in traditional international jurisdiction cases.⁵

Courts and commentators have long recognized these problems, yet little progress has been made toward finding a solution to the Internet jurisdiction dilemma.⁶ The failure of the legal community to develop jurisdictional standards has created significant concerns in the Internet community.⁷ Many Internet content providers are faced with the uncertainty of being sued in unanticipated jurisdictions for violating unknown laws with untold consequences.⁸ Their fear is grounded in a reality demonstrated by a Brazilian court order entered against Google subsidiary YouTube, which resulted in at least one Brazilian telecom company blocking the site from its Internet users.⁹ Although the judge vacated his order shortly after the ban went into effect, this libel case demonstrates the enormous impact Internet jurisdiction can have on e-commerce.¹⁰

Although the Internet is still relatively young, the legal principles of international jurisdiction are not. This Note begins with a brief explanation of traditional (non-Internet related) international jurisdiction law. Next, this Note summarizes the leading case involving international Internet jurisdiction and the leading theories for resolving its open issues. Finally, this Note suggests that, although alone they are each insufficient, aspects from each of these theories should be combined for a practical and comprehensive approach to international Internet jurisdiction.

I. BACKGROUND

A. *Introduction to International Jurisdiction*

The right of a sovereign state to create and enforce laws concerning activities within its borders is a fundamental principle of interna-

⁵ See Denis Rice, *2001: A Cyberspace Odyssey Through U.S. and E.U. Internet Jurisdiction over E-Commerce*, 661 PLI/PAT 421, 445 (2001).

⁶ See Gerlach, *supra* note 1, at 902–03.

⁷ See Holger Hestermeyer, *Personal Jurisdiction for Internet Torts*, 26 NW. J. INT'L L. & BUS. 267, 267–68 (2006).

⁸ See *id.* at 268.

⁹ See Associated Press, *YouTube's Legal Woes; Clip of Model Having Sex Ordered Blocked*, WASH. POST, Jan. 8, 2007, at C3.

¹⁰ See Jack Chang, *Order to Ban YouTube Ignites Brazil Firestorm*, SEATTLE TIMES, Jan. 14, 2007, at A18.

tional law,¹¹ yet there is often ambiguity as to whether such sovereign powers may extend beyond a state's borders.¹² As a result, the *corpus juris* concerning international jurisdiction is among the most voluminous in all of international law and acknowledges several bases of jurisdiction.¹³

The strongest basis for a state's jurisdiction is territoriality.¹⁴ Under this principle, a sovereign state necessarily has jurisdiction over all persons, objects, and activities within its borders.¹⁵

Although inherently weaker, several bases of extraterritorial jurisdiction are also acknowledged by the international community, such as nationality, passive personality, effects, protection, and universality principles.¹⁶ The nationality principle permits states to assert jurisdiction over their own nationals, wherever they are located.¹⁷ This principle is grounded in the relationship existing between states and their nationals in which citizens are subject to their state's laws because they enjoy the benefits of citizenship and have notice of the laws of their home state.¹⁸

Similarly, jurisdiction has been based on the nationality of the victim; however, such "passive personality" jurisdiction is not favored.¹⁹ Another common basis of extraterritorial jurisdiction is effects jurisdiction.²⁰ Under this principle, a state may assert jurisdiction over conduct that has an effect, but does not actually occur, within its border.²¹ In addition, jurisdiction has been upheld under the protection principle where extraterritorial conduct directly threatened crucial state interests, such as national security.²² Lastly, under the universality principle,

¹¹ See *The Lotus Case (Fr. v. Turk.)*, 1927 P.C.I.J. (ser. A) No. 10, at 18–19; see also *Am. Banana Co. v. United Fruit Co.*, 213 U.S. 347, 358 (1909) ("The very meaning of sovereignty is that the decree of the sovereign makes law.").

¹² See MARK W. JANIS & JOHN NOYES, *INTERNATIONAL LAW* 767 (3d ed. 2006) (noting that jurisdictional issues constitute a large amount of international law).

¹³ See *id.*

¹⁴ See MARK W. JANIS, *AN INTRODUCTION TO INTERNATIONAL LAW* 318 (4th ed. 2003).

¹⁵ See *Am. Banana Co.*, 213 U.S. at 357–58 (explaining that power to make laws defines sovereignty and "[a]ll legislation is *prima facie* territorial").

¹⁶ See JANIS, *supra* note 14, at 320, 322, 325.

¹⁷ See *Blackmer v. United States*, 284 U.S. 421, 437 (1932).

¹⁸ See *id.* at 438.

¹⁹ See *RESTATEMENT (THIRD) OF FOREIGN RELATIONS* § 402 cmt. g (1987).

²⁰ See *id.* cmt. d.

²¹ See *United States v. Aluminum Co. of Am.*, 148 F.2d 416, 443 (2d Cir. 1945).

²² See *United States v. Pizzarusso*, 388 F.2d 8, 10 (2d Cir. 1968).

certain activities are by their very nature *jus cogens*,²³ and any nation may have jurisdiction over them.²⁴

In many cases, a number of states may have concurrent jurisdiction under any of the various forms of extraterritorial jurisdiction, resulting in a conflict of laws.²⁵ Forum selection clauses in international business contracts have become an increasingly important and accepted method of resolving international conflict of laws issues in the world of global commerce.²⁶ Outside of this arena, however, there are two doctrines commonly used by courts to resolve international conflicts of laws: international comity, and *forum non conveniens*.²⁷ International comity is the recognition that a nation grants to the legislative, executive, or judicial acts of another nation within its own territory.²⁸ Under this doctrine, a court may recognize and enforce a judgment of a foreign court,²⁹ apply the laws of another state,³⁰ or decline to assert its otherwise valid jurisdiction and dismiss the complaint in favor of a foreign forum.³¹ Under the *forum non conveniens* doctrine, a court can dismiss a case if it finds that it would not be a sufficiently convenient forum for adjudication.³²

B. International Internet Jurisdiction

1. The Internet Problem

Although the above legal framework worked relatively well in traditional contexts, the advent of the Internet introduced novel challenges

²³ *Jus cogens* is “a mandatory or peremptory norm of general international law accepted and recognized by the international community as a norm from which no derogation is permitted. A peremptory norm can be modified only by a later norm that has the same character.” BLACK’S LAW DICTIONARY 876 (8th ed. 2004); see also Milena Sterio, *The Evolution of International Law*, 31 B.C. INT’L & COMP. L. REV. 213, 222–23 (2008) (discussing universal jurisdiction).

²⁴ See *Filartiga v. Pena-Irala*, 630 F.2d 876, 890 (2d Cir. 1980) (holding jurisdiction could be asserted over torturer because extraterritorial conduct violated universal norms).

²⁵ See JANIS, *supra* note 14, at 326.

²⁶ See *M/S Bremen v. Zapata*, 407 U.S. 1, 15 (1972).

²⁷ See JANIS, *supra* note 14, at 326–27, 332.

²⁸ See *Hilton v. Guyot*, 159 U.S. 113, 163–64 (1895).

²⁹ See JANIS, *supra* note 14, at 327.

³⁰ See *Lauritzen v. Larsen*, 345 U.S. 571, 592 (1953) (holding Danish law applied in maritime tort case brought by Danish sailor).

³¹ See *M/S Bremen*, 407 U.S. at 8–9 (sending litigation to London per forum selection clause).

³² See *Piper Aircraft Co. v. Reyno*, 454 U.S. 235, 248–49 (1981).

for determining international jurisdiction.³³ In the traditional analog world, it is relatively easy for courts to determine the geographical locations of the persons, objects, and activities relevant to a particular case.³⁴ The geography of the digital world of the Internet, however, is not as easily charted.³⁵ Content providers may physically reside, conduct their business, and locate their servers in a particular location, yet their content is readily accessible from anywhere in the world.³⁶ Furthermore, attempts to identify the location of a particular user over the Internet have proven extremely difficult, and many Internet users compound this problem by intentionally hiding their location.³⁷ Traditional principles of international jurisdiction, particularly territoriality, are poorly suited for this sort of environment of geographic anonymity.³⁸ Courts have struggled to develop a satisfactory solution,³⁹ yet no progress has been made toward a uniform global standard of Internet jurisdiction.⁴⁰

2. Jurisdiction in *Yahoo! v. La Ligue le Racisme et L'Antisemitisme*

Perhaps the most highly publicized example of jurisdictional difficulties involving the Internet is *Yahoo! Inc. v. La Ligue le Racisme et L'Antisemitisme* (LICRA), a case that started in 2000.⁴¹ Two French citizens, LICRA, and L'Union Des Etudiants Juifs De France (UEJF), filed suit in France against Yahoo!, alleging that the website violated a French law prohibiting the display of Nazi paraphernalia by permitting users of its Internet auction service to display and sell such artifacts.⁴²

The two Paris based anti-racism groups demanded that Yahoo!'s French subsidiary (Yahoo.fr) remove all hyperlinks to the parent website (Yahoo.com) containing the offending content, and warn French

³³ See Catherine Heaven, Note, *A Proposal for Removing Road Blocks from the Information Superhighway by Using Integrated International Approach to Internet Jurisdiction*, 10 MINN. J. GLOBAL TRADE 373, 397 (2001).

³⁴ See Rice, *supra* note 5, at 429.

³⁵ See *id.*

³⁶ See Rinat Hadas, *International Internet Jurisdiction: Whose Law is Right?*, 15 FLA. J. INT'L L. 299, 307 (2002); Michelle Love, Note, *International Jurisdiction over the Internet*, 17 TEMP. INT'L & COMP. L.J. 261, 262 (2003).

³⁷ See Rice, *supra* note 5, at 458–59 (explaining geo-location technologies).

³⁸ See *id.* at 429.

³⁹ See *id.*

⁴⁰ See Gerlach, *supra* note 1, at 902–03.

⁴¹ See Hestermeyer, *supra* note 7, at 268.

⁴² See *Yahoo! Inc. v. La Ligue le Racisme et L'Antisemitisme (Yahoo! I)*, 145 F. Supp. 2d 1168, 1171–72 (N.D. Cal. 2001).

surfers of the offending content accessible on Yahoo.com.⁴³ In defense, Yahoo! argued that the French court lacked jurisdiction over the matter because its servers were located in the United States, its principle business was located there, and it had no intention of violating the French law prohibiting the display of Nazi paraphernalia by linking Yahoo.com to Yahoo.fr.⁴⁴

In a preliminary order, dated May 22, 2000 (the May Order), the Tribunal De Grande Instance De Paris rejected Yahoo!'s arguments.⁴⁵ The court held that it could properly assert jurisdiction because "the damage was suffered in France."⁴⁶ The May Order required Yahoo!: (1) to "dissuade and render impossible all visitation on Yahoo.com to participate in the auction service of Nazi objects, as well as to render impossible any other site or service which makes apologies of Nazism"; (2) to warn all surfers on Yahoo.fr that the display or sale of Nazi objects as well as the "banalization" of Nazism is strictly forbidden in France and exposure to such illegal material is possible by using the hyperlink to Yahoo.com or by conducting certain searches; (3) to submit to the court at a later hearing their proposed measures for implementing the previous two orders; and (4) to pay each plaintiff 10,000 francs.⁴⁷

During the subsequent hearing, Yahoo! again challenged the French Tribunal's jurisdiction to consider the matter.⁴⁸ Yahoo! also argued that compliance with the May Order would violate its First Amendment rights to freedom of expression, and, therefore, it could not be enforced in the United States.⁴⁹ Yahoo! further claimed that compliance with the order would be technologically impossible.⁵⁰ Finally, it argued that, even if it could comply with the May Order, implementing it "would entail unduly high costs for the company . . . and would to a degree compromise the existence of the Internet, being a

⁴³ See Richard Salis, *A Look at How U.S. Based Yahoo! Was Condemned by French Law* (Nov. 2000), <http://www.juriscom.net/txt/jurisfr/cti/yauctions.htm>.

⁴⁴ See *id.*

⁴⁵ See Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Paris, May 22, 2000, Interim Order No. 00/05308, *available at* <http://www.juriscom.net/txt/jurisfr/cti/yauctions20000522.htm> (Fr.).

⁴⁶ *Id.*

⁴⁷ *Id.* At the time the judgment was awarded, 10,000 francs would exchange for \$13,460. See Daily French Franc Rate Against the Dollar, <http://www.jeico.co.kr/cnc57frc.html> (lasted visited May 14, 2007).

⁴⁸ See Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Paris, Nov. 20, 2000, *available at* <http://www.cdt.org/speech/international/20001120yahoofrance.pdf> (Fr.).

⁴⁹ See *id.*

⁵⁰ See *id.*

space of liberty and scarcely receptive to attempts to control and restrict access.”⁵¹

In November, the court again rejected Yahoo!’s jurisdiction arguments on the same grounds as in the May Order.⁵² Relying heavily on a report of Internet experts, it also rejected Yahoo!’s technological impossibility argument, and devoted much of its opinion to explaining how compliance with the May Order could be achieved.⁵³ In rejecting the First Amendment argument, the court stated that “it would most certainly cost the company very little to extend its ban to symbols of Nazism, and such an initiative would also have the merit of satisfying an ethical and moral imperative shared by all democratic societies.”⁵⁴ The court then ordered Yahoo! to comply with the May Order within three months of receiving notice of the November Order.⁵⁵

In response to the November Order, Yahoo! initiated suit in California against LICRA and UEJF, seeking a declaratory judgment that the French orders were constitutionally unenforceable in the United States as contrary to the First Amendment.⁵⁶ In an initial opinion, the district court denied the defendants’ motion to dismiss for lack of jurisdiction.⁵⁷ The district court first determined that the case was ripe for adjudication,⁵⁸ and then turned to the *International Shoe* personal jurisdiction analysis.⁵⁹

The court held that the defendants purposefully availed themselves of the forum state because they sent a “cease and desist” letter to Yahoo!’s California headquarters, requested the French court to require Yahoo! to take specific actions in California that would violate Yahoo!’s First Amendment rights, and engaged U.S. Marshals to serve process on Yahoo!.⁶⁰ The court then determined that it would not be unreasonable to maintain Yahoo!’s suit, noting that the United States

⁵¹ *Id.*

⁵² *See id.*

⁵³ Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Paris, Nov. 20, 2000, available at <http://www.cdt.org/speech/international/20001120yahoofrance.pdf> (Fr.).

⁵⁴ *Id.*

⁵⁵ *See id.*

⁵⁶ *See Yahoo! I*, 145 F. Supp. 2d 1168, 1171–72 (N.D. Cal. 2001).

⁵⁷ *Id.* at 1171.

⁵⁸ *See id.* at 1172 n.2.

⁵⁹ *See id.* at 1172–73. The Due Process Clause permits courts to assert jurisdiction over a non-resident defendant only if that defendant has “minimum contacts” with the forum state such that adjudication there “does not offend traditional notions of fair play and substantial justice.” *Int’l Shoe v. Washington*, 326 U.S. 310, 316 (1945).

⁶⁰ *See Yahoo! I*, 145 F.3d at 1174.

was a superior forum to France for determining the limited question of whether it “should recognize and enforce the French Order that required Yahoo! to censor its U.S.-based service to conform to French penal law.”⁶¹

In a subsequent opinion, the district court granted Yahoo!’s motion for summary judgment and declared the French Orders unenforceable.⁶² Addressing the issue of international comity, the court reasoned that, although U.S. courts will generally recognize and enforce a foreign judgment, it could not do so in this case because enforcement of the French orders would violate Yahoo!’s constitutional rights “by chilling protected speech that occurs simultaneously within our borders.”⁶³

LICRA and UEJF appealed and a divided panel of the Ninth Circuit reversed.⁶⁴ The majority held the district court lacked jurisdiction over LICRA and UEJF because they had not engaged in wrongful conduct targeted at the forum state.⁶⁵ The majority further noted that Yahoo! cannot expect to have both the commercial benefits of having its content viewed worldwide as well as the benefit of using the First Amendment as a shield against foreign litigants seeking to enforce judgments based on foreign speech laws.⁶⁶ In an en banc rehearing, an 8-3 majority of the court upheld the district court’s exercise of jurisdiction over LICRA and UEJF; however, the district court’s judgment was ultimately reversed on the ripeness issue.⁶⁷

II. DISCUSSION

A. *Theories of Internet Regulation*

As the last century drew to a close, the Internet was becoming a global phenomenon,⁶⁸ yet the swelling scale of online commerce and

⁶¹ *Id.* at 1178, 1179–80.

⁶² See *Yahoo! Inc. v. La Ligue le Racisme et L’Antisemitisme (Yahoo! II)*, 169 F. Supp. 2d 1181, 1194 (N.D. Cal. 2001).

⁶³ *Id.* at 1192.

⁶⁴ See *Yahoo! Inc. v. La Ligue le Racisme et L’Antisemitisme (Yahoo! III)*, 379 F.3d 1120, 1126 (9th Cir. 2004).

⁶⁵ See *id.*

⁶⁶ See *id.*

⁶⁷ *Yahoo! Inc. v. La Ligue le Racisme et L’Antisemitisme (Yahoo! IV)*, 433 F.3d 1199, 1201 (9th Cir. 2006).

⁶⁸ See Margaret Khayat Bratt & Norbert F. Kugele, *Who’s in Charge?* MICH. B.J., July, 2001, at 43.

content caused increased concerns over regulating Cyberspace.⁶⁹ Attempts at regulating the Internet, however, have proven problematic because of the decentralized nature of the Web and fears of inhibiting a rapidly growing engine of global commerce and communication.⁷⁰ Nevertheless, at least four prominent theoretical models of Internet regulation have emerged: (1) the self-regulation model; (2) the neo-mercantilist model; (3) the culturalist model; and (4) the globalism model.⁷¹

The self-regulation model insists that the Internet community is capable of regulating itself and promulgation of domestic or international laws would be both unnecessary and undesirable.⁷² Self-regulation is likely rooted in the ideals of the “Free Software Movement” starting in the 1980s within the Internet/Hi-tech industry, which was characterized by the free exchange of proprietary information for the purpose of advancing the art through public collaboration.⁷³ The Internet has become the primary conduit for such free communication, and attempts at regulating it have traditionally faced sharp criticism from the online community.⁷⁴ One Internet commentator illustrated the views of many in the online community stating:

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

. . . Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different.⁷⁵

⁶⁹ See Spencer Kass, *Regulation and the Internet*, 26 S.U. L. REV. 93, 93 (1998).

⁷⁰ See *id.*

⁷¹ See Love, *supra* note 36, at 271.

⁷² See Lyombe Eko, *Many Spiders, One Worldwide Web: Towards a Typology of Internet Regulation*, 6 COMM. L. & POL'Y 445, 451 (2001).

⁷³ See Karl Fogel, *What Is Free Software*, Sept. 29, 2005, <http://www.onlamp.com/pub/a/onlamp/2005/09/29/what-is-free-software.html>.

⁷⁴ See *generally* Elec. Frontier Found. (EFF), About EFF, <http://www.eff.org/about/> (last visited May 14, 2007) (advocating various online freedoms from privacy to use of copyrighted materials).

⁷⁵ John Perry Barlow, *A Declaration of the Independence of Cyberspace*, EFF, 1996, <http://homes.eff.org/~barlow/Declaration-Final.html>.

As the Internet began to grow in the late 1990s, the self-regulation model appeared to receive acceptance from certain governments, particularly the United States.⁷⁶ In fact, the Clinton-Gore administration called for governments to “refrain from imposing new and unnecessary regulations, bureaucratic procedures, or taxes and tariffs on commercial activities that take place via the Internet.”⁷⁷ The self-regulation model, however, is not universally accepted,⁷⁸ and “[m]ost countries regulate the Internet within the framework of their political, legal, moral and cultural values.”⁷⁹

Neo-mercantilism, the second theoretical model of Internet regulation, “combines several libertarian principles—the marketplace of ideas, laissez-faire economics, free trade and the free flow of information, goods and services—and applies them to the Internet, thereby making them global concepts.”⁸⁰ The underlying premise of the model is that the Internet is essentially a vehicle of commerce.⁸¹ The role of government, therefore, is to ensure the free flow of commerce along the information superhighway and to remove any impediments.⁸² This model is considered to be the American approach to Internet regulation.⁸³

In contrast, the culturalist model views cultural protection as the primary objective of Internet regulation.⁸⁴ Governments adhering to this model tend to “enact Internet laws and policies rooted in the specific intellectual, aesthetic and moral values of their national or regional civilizations or cultures, with little consideration of their extra-territorial or global impact.”⁸⁵ Culturalist governments often perceive Internet content not as neutral, but serving the interest of its country of origin, which in most cases is the United States.⁸⁶ The cultural homogeneity of the Internet is thus believed to be a potential cause of global cultural impoverishment.⁸⁷

⁷⁶ See Eko, *supra* note 72, at 450.

⁷⁷ See WILLIAM J. CLINTON & ALBERT GORE, JR., TECHNOLOGY ADMINISTRATION, DEPARTMENT OF COMMERCE, A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE (1997), available at <http://www.technology.gov/digeconomy/framewrk.htm>.

⁷⁸ See Love, *supra* note 36, at 271.

⁷⁹ Eko, *supra* note 72, at 461.

⁸⁰ *Id.* at 463–64.

⁸¹ See *id.* at 464.

⁸² See *id.*

⁸³ See *id.*

⁸⁴ Eko, *supra* note 72, at 465.

⁸⁵ *Id.* at 466.

⁸⁶ See *id.* at 467.

⁸⁷ See *id.*

The French orders in the Yahoo! case illustrate a culturalist perspective.⁸⁸ That court was primarily concerned with protecting French surfers from viewing websites that “violated French law by ‘offending the collective memory of the country.’”⁸⁹ The court seemed to dismiss the compliance costs imposed on Yahoo! and failed to address the implications of the extraterritorial effects of its orders.⁹⁰

Lastly, the globalism model requires multinational political, economic, technological, and cultural cooperation in regulating the Internet.⁹¹ This model relies on treaties and international conventions to achieve that goal.⁹² Although international regulation of intellectual property and child pornography on the Internet has made some progress,⁹³ there are no international agreements resolving Internet jurisdiction.⁹⁴

B. *Proposed Solutions to the Internet Jurisdiction Problem*

1. A *Res Communes* Solution

One solution to the Internet jurisdiction problem is to declare cyberspace a new global space or Common Heritage of Mankind (CHM).⁹⁵ This solution reflects many of the underlying policies of the self-regulation model; however, the international community, instead of the Internet community, would resolve the jurisdictional issues by regulating the Internet through treaties and norms rather than applying traditional jurisdiction doctrines.⁹⁶

CHM is grounded in the *res communes* doctrine that “all nations should benefit from the resources that are recovered from areas in which all nations have an interest.”⁹⁷ The High Seas, Antarctica, and Outer Space are all regulated by treaties and international conventions as CHM.⁹⁸ A CHM cannot be appropriated; rather, all states share the

⁸⁸ See *id.* at 471.

⁸⁹ Eko, *supra* note 72, at 471.

⁹⁰ See Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Paris, Nov. 20, 2000, available at http://www.cdt.org/speech/international/20001120_yahoofrance.pdf (Fr.).

⁹¹ See Eko, *supra* note 72, at 463.

⁹² See *id.*

⁹³ See *id.*

⁹⁴ See Gerlach, *supra* note 1, at 901–02.

⁹⁵ See Love, *supra* note 36, at 273; Heaven, *supra* note 33, at 400.

⁹⁶ See Love, *supra* note 36, at 273.

⁹⁷ Heaven, *supra* note 33, at 390.

⁹⁸ See *id.* at 391.

burden of managing a CHM's resources and the benefits of its exploitation.⁹⁹ Those resources must also be preserved for future generations, and a CHM can only be utilized for peaceful purposes.¹⁰⁰

Advocates of a *res communes* solution to the Internet jurisdiction problem envision a comprehensive international regulatory scheme.¹⁰¹ An international convention would lead to a treaty setting forth "universal standards" and declaring the Internet CHM.¹⁰² The treaty would also create an international body that would promulgate civil and criminal Internet regulations and jurisdictional rules.¹⁰³ Advocates argue that regulations drafted pursuant to the treaty must be adopted by all nations without reservations or modifications, and individual nations would be required to insert these regulations into their domestic legal codes.¹⁰⁴

The clear advantage of international Internet regulation is uniformity.¹⁰⁵ Courts would no longer have the discretion of deciding whether their laws or the laws of another nation apply in a given case.¹⁰⁶ Moreover, the enforcement of foreign judgments would not violate domestic laws because the laws regulating the Internet would be the same in all countries.¹⁰⁷ Users and providers of Internet services and content would be afforded the certainty of knowing that their conduct is regulated by a single set of globally applicable laws.¹⁰⁸ In addition, proponents argue that a user or provider who violates a universal Internet regulation would simply be prosecuted in their home jurisdiction because, at least in theory, the outcome would be the same in all jurisdictions and the defendant's home jurisdiction would be the most convenient forum.¹⁰⁹

⁹⁹ *See id.*

¹⁰⁰ *See id.*

¹⁰¹ *See id.* at 400.

¹⁰² *See Heaven, supra* note 33, at 390.

¹⁰³ *See id.* at 400.

¹⁰⁴ *See id.*; Love, *supra* note 36, at 273–74.

¹⁰⁵ *See Love, supra* note 36, at 274.

¹⁰⁶ *See id.*

¹⁰⁷ *See id.*

¹⁰⁸ *See id.*

¹⁰⁹ *See Heaven, supra* note 33, at 401. Although Heaven argues uniform laws would make jurisdictional issues easier in the context of criminal violations, she acknowledges that the question of civil jurisdiction is not as readily resolved. *See id.* Even in the criminal context, however, there would likely be significant debate over whether sovereign rights of the defendant's nation to protect its citizens should trump the sovereign right of the victim's nation to protect its citizens and to prosecute crimes occurring or having substantial effects within its borders. It is unclear whether declaring the Internet *res communes* would remove from consideration these deeply engrained principles of sovereignty.

A universal regulatory scheme may have great appeal, but even supporters of a *res communes* solution to Internet regulation admit that it will be a “daunting task . . . coaxing sovereign nations into giving up territorial rights” over the commercial and intellectual resources of the Internet.¹¹⁰ Proponents, however, contend that the challenges of establishing an Internet CHM are both necessary and doable.¹¹¹

2. A Global Standard for Determining Jurisdiction

Another proposal involves establishing a global standard for determining jurisdiction in Internet cases.¹¹² Similar to the *res communes* solution, the global standardization approach to Internet jurisdiction requires an international convention or treaty.¹¹³ It would, however stop short of declaring the Internet CHM and formulating substantive Internet regulations.¹¹⁴ Specifically, proponents of global standardization desire the international adoption of a single test for determining Internet jurisdiction.¹¹⁵ Several tests have been proposed to resolve the Internet jurisdiction problem including: (1) the accessibility test;¹¹⁶ (2) the Zippo test;¹¹⁷ (3) the effects test;¹¹⁸ and (4) the targeting test.¹¹⁹

The Zippo test determines whether jurisdiction may be properly asserted based on “the nature and quality of the commercial activity” conducted over the Internet.¹²⁰ This test involves evaluating the relevant Internet activity and placing it into one of three categories falling along a sliding scale.¹²¹ “At one end of the spectrum are situations where a defendant clearly does business over the Internet.”¹²² Jurisdiction in these cases would be proper.¹²³ “At the opposite end are situa-

¹¹⁰ *Id.* at 402.

¹¹¹ *See id.*

¹¹² *See* Gerlach, *supra* note 1, at 905.

¹¹³ *See* Hestermeyer, *supra* note 7, at 287 (advocating targeting test provision for Hague Convention).

¹¹⁴ *See id.*

¹¹⁵ *See id.*

¹¹⁶ *See id.* at 276. The accessibility test broadly holds jurisdiction properly asserted if defendant’s site was accessible in the forum state. *See id.*

¹¹⁷ *See id.* at 277 (discussing *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997)).

¹¹⁸ *See* Rice, *supra* note 5, at 477 (discussing *Panavision Int’l, L.P. v. Toepfen*, 144 F.3d 1316 (9th Cir. 1998)).

¹¹⁹ *See* Hestermeyer, *supra* note 7, at 279.

¹²⁰ *Zippo Mfg.*, 952 F. Supp. at 1124.

¹²¹ *See id.*

¹²² *Id.*

¹²³ *See id.*

tions where a defendant has simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions.”¹²⁴ Asserting jurisdiction over these “passive Web sites” would be improper.¹²⁵ “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 the level of interactivity and commercial nature of the exchange of information that occurs on the Web site.”¹²⁶ While many U.S. courts have applied the Zippo test,¹²⁷ it appears to be fading in popularity.¹²⁸

Rather than focusing on the interactivity of the defendant’s website, some courts determine Internet jurisdiction based on whether the conduct “has an effect in the forum state.”¹²⁹ A simplified example of this test is demonstrated in the Tribunal De Grande Instance De Paris’ holding in the Yahoo! case: “Whereas the damage was suffered in France, our jurisdiction is therefore competent.”¹³⁰ In the United States, the effects test is grounded in the Supreme Court’s ruling in *Calder v. Jones* that jurisdiction is proper where the defendant’s intentional conduct was calculated to cause injury in the forum state.¹³¹ Courts may invoke the effects test to assert jurisdiction in cases where the facts would be insufficient under the Zippo test.¹³² Applying an effects test, by itself, however, has been criticized as potentially exposing websites to liability anywhere in the world.¹³³

The targeting test offers a narrower and more flexible standard.¹³⁴ Under this test, courts determine whether the defendant website targeted the jurisdiction by considering the steps taken by the defendant to enter or avoid the particular forum state.¹³⁵ The question of whether the defendant targeted the jurisdiction is itself a vague standard.¹³⁶

¹²⁴ *Id.*

¹²⁵ *Zippo Mfg.*, 952 F. Supp. at 1124.

¹²⁶ *Id.*

¹²⁷ See, e.g., *Cybersell, Inc. v. Cybersell, Inc.*, 130 F.3d 414, 419 (9th Cir. 1997); *Am. Eyewear, Inc. v. Peeper’s Sunglasses & Accessories, Inc.*, 106 F. Supp. 2d 895, 900–01 (N.D. Tex. 2000).

¹²⁸ See Hestermeyer, *supra* note 7, at 278.

¹²⁹ *Panavision Int’l, L.P. v. Toeppen*, 144 F.3d 1316, 1321 (9th Cir. 1998).

¹³⁰ Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Paris, May 22, 2000, Interim Order No. 00/05308, available at <http://www.juriscom.net/txt/jurisfr/cti/yauctions20000522.htm> (Fr.).

¹³¹ See 465 U.S. 783, 790 (1984).

¹³² See Rice, *supra* note 5, at 477–78.

¹³³ See Hestermeyer, *supra* note 7, at 286.

¹³⁴ See *id.*

¹³⁵ See *id.* at 279.

¹³⁶ See *id.*

Commentators, however, suggest that courts, in applying the targeting test, should consider the totality of the circumstances or develop a non-exhaustive list of factors.¹³⁷ The suggested factors include the languages used, the currencies accepted, disclaimers, the use of geo-location technologies, the top-level domain used,¹³⁸ pictorial suggestions, advertising, and market participation.¹³⁹ The targeting test has been applied in the United States¹⁴⁰ and elsewhere.¹⁴¹

3. Content Filtering & E-Borders

Many commentators view the Internet jurisdiction problem as one of weakened national borders.¹⁴² Some have argued that the Internet has created a borderless society because the Internet lacks a physical location.¹⁴³ This argument, however, is largely inaccurate.¹⁴⁴ "Internet communication begins 'from a fixed location and ends at a fixed location.'"¹⁴⁵ Proponents of content filtering argue that filtering technologies can be placed within this infrastructure to create e-borders.¹⁴⁶

The Internet jurisdiction problem, from the content filtering perspective, results from the large volume of unmonitored Internet traffic crossing international borders.¹⁴⁷ Governments would regain control of their borders by placing blocking and tracking technologies at interna-

¹³⁷ See *id.*; Rice, *supra* note 5, at 512.

¹³⁸ The top level domain refers to the last part of a domain name, thus the top level domain of www.website.com would be [.com](http://www.website.com). Some top level domains, such as country codes, tie the website to a geographic location. ICANN, *Top Level Domain Names*, <http://www.icann.org/tlds> (last visited May 19, 2008).

¹³⁹ See Hestermeyer, *supra* note 7 at 286–87; Rice, *supra* note 5, at 512–15.

¹⁴⁰ See *Toys "R" Us, Inc. v. Step Two, S.A.*, 318 F.3d 446, 454 (3d Cir. 2003) (holding that purposeful availment element of personal jurisdiction in Internet cases requires evidence showing defendant directly targeted its site to forum state).

¹⁴¹ See Hestermeyer, *supra* note 7, at 286 (noting German courts routinely apply targeting test in certain cases).

¹⁴² Cherie Dawson, Note, *Creating Borders on the Internet: Free Speech, the United States, and International Jurisdiction*, 44 VA. J. INT'L L. 637, 638 (2004); Gerlach, *supra* note 1, at 912.

¹⁴³ See, e.g., Dawson, *supra* note 142, at 638; Heaven, *supra* note 33, at 374.

¹⁴⁴ Although it might be easy to view the Internet as lacking a physical location, the effective operation of the Internet requires a tremendous amount of hardware. An article discussing Google's construction of a new computing center described it as "sprawling like an information age factory" and noted that it would be "hard to keep [it] a secret when it is a computing center as big as two football fields, with twin cooling plants protruding four stories into the sky." John Markoff & Saul Hansell, *Hiding in Plain Sight, Google Seeks More Power*, N.Y. TIMES, June 14, 2006, at A1.

¹⁴⁵ Timothy Lester, *Globalized Automatic Choice of Forum: Where Do Internet Consumers Sue?*, 9 NEW ENG. J. INT'L & COMP. L. 431, 447 (2003).

¹⁴⁶ See Gerlach, *supra* note 1, at 912.

¹⁴⁷ See Dawson, *supra* note 142, at 638.

tional access points or at the Internet Service Provider's (ISP) servers to act as centurions.¹⁴⁸ Many governments have already implemented such technologies to monitor and regulate Internet activities of their citizens.¹⁴⁹ In an ironic twist on the Yahoo! case, Yahoo!, Google, and Microsoft have been criticized for filtering their search results in China for terms such as "democracy" and "human rights."¹⁵⁰

There are four basic forms of content filtering: Host Name Blocking; IP Address Blocking;¹⁵¹ Keyword Blocking; and Content-Based Image Blocking.¹⁵² The first two, Host Name Blocking and IP Address Blocking, are the simplest filtering methods because they only check the web address and not the entire site.¹⁵³ Host Name Blocking restricts access to web addresses containing banned terms.¹⁵⁴ IP Address Blocking restricts access to sites based on a list of banned IP addresses compiled by the filter manager, or it can restrict user access to a pre-approved list of websites, called Whitelist Filters.¹⁵⁵ Keyword Blocking is similar to Host Name Blocking; however, its scope is much greater because Keyword Blocking searches the entire site for banned terms.¹⁵⁶ Content-Based Image Filtering scans images displayed on websites.¹⁵⁷

Proponents of content filtering view it as a more realistic solution to the Internet jurisdiction problem than attempting to get the world to agree on a single set of universal regulations and jurisdictional standards.¹⁵⁸ Moreover, Internet filtering allows states to erect e-borders and regulate the Internet activity of its citizens without having an impact on foreign users or content providers.¹⁵⁹ Critics, however, argue that the filtering approach unduly restricts the free flow of information

¹⁴⁸ See Gerlach, *supra* note 1, at 912.

¹⁴⁹ See Rice, *supra* note 5, at 455.

¹⁵⁰ See Tom Zeller Jr., *Internet Firms Facing Questions About Censoring Online Searches in China*, N.Y. TIMES, Feb. 15, 2006 (quoting a Yahoo! Spokeswoman: "Just like any other global company, Yahoo! must ensure that its local country sites operate within the laws, regulations and customs of the country in which they are based"); OpenNet Initiative, Google Search & Cache Filtering Behind China's Great Firewall, (Aug. 30, 2004) <http://www.opennetinitiative.net/bulletins/006>.

¹⁵¹ See Gerlach, *supra* note 1, at 916. IP address blocking is also known as packet filtering. See *id.*

¹⁵² See *id.*

¹⁵³ See *id.*

¹⁵⁴ See *id.*

¹⁵⁵ See *id.*

¹⁵⁶ See Gerlach, *supra* note 1, at 916–17.

¹⁵⁷ See *id.* at 917.

¹⁵⁸ See *id.* at 912–13.

¹⁵⁹ See *id.*

for which the Internet was created.¹⁶⁰ In addition, many have echoed Yahoo!'s argument that filtering technology is easily circumvented or in itself largely ineffective.¹⁶¹ Nevertheless, at least twenty countries currently impose significant filtering restrictions on Internet access.¹⁶²

4. Choice of Law Provisions

Another solution to the Internet jurisdiction problem is to allow content providers and users to agree to resolve disputes in a particular forum via choice of law provisions in terms of service contracts.¹⁶³ For example, the content provider could require users to consent to a terms of service agreement containing a forum selection clause as a condition for entering the site.¹⁶⁴ These provisions would be valid if: (1) "the chosen law and forum are clearly disclosed to the consumer"; (2) "the chosen forum is reasonably accessible and neutral"; and (3) "the chosen law provides reasonable, baseline consumer protections."¹⁶⁵ The choice of law approach could also result in the development of new forms of alternative dispute resolution (ADR) specifically tailored for the unique contours of the Internet.¹⁶⁶

The choice of law solution draws heavily from the self-regulation and neo-mercantilist models in that it relies primarily on private ordering rather than governmental or international regulation.¹⁶⁷ The only external regulation appears to be the establishment of an international consensus regarding the validity of such agreements; however, given the European Union's reluctance to allow forum selection clauses, such a consensus does not seem likely.¹⁶⁸

¹⁶⁰ See OpenNet Initiative, About Us, <http://opennet.net> (follow "About Filtering" link) [hereinafter OpenNet Initiative] (last visited May 14, 2008).

¹⁶¹ See Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Paris, Nov. 20, 2000, available at <http://www.cdt.org/speech/international/20001120yahoofrance.pdf> (Fr.); see also Gerlach, *supra* note 1 at 926–27 (acknowledging current limitations in filtering technology, but noting that such technologies continue to improve).

¹⁶² See Rice, *supra* note 5, at 457.

¹⁶³ See Lester, *supra* note 145, at 441–42.

¹⁶⁴ See Yahoo!, Terms of Service Agreement <http://info.Yahoo.com/legal/us/Yahoo!/utos/utos-173.html> (last visited May 19, 2007).

¹⁶⁵ John Goldsmith, *Jurisdiction: Building Confidence in a Borderless Medium*, Internet Law & Policy Forum, http://www.ilpf.org/events/jurisdiction/transcript/goldsmith_summary.htm (last visited May 14, 2007).

¹⁶⁶ See *id.*

¹⁶⁷ See *id.*

¹⁶⁸ See Rice, *supra* note 5, at 492–94 (discussing Brussels Convention and Hague Convention proposals that would hold choice of forum contracts null and void).

III. ANALYSIS

A. *The Global Internet Commons: Unfounded and Impractical*

The solution of declaring the Internet CHM is certainly appealing. It would attempt to create a utopian global common in which persons from around the world could exchange information, ideas, goods, and services. Unfortunately, the *res communes* solution suffers from a host of failures, both practical and theoretical. First, the theoretical support for declaring the Internet CHM, such as the Moon Treaty and the Outer Space Treaty, is very weak.¹⁶⁹ Second, drafting a single set of Internet regulations is likely too ambitious, and might even prove more problematic than helpful.¹⁷⁰ Third, the solution would take an incredible amount of time to implement and modify because it would necessarily require the participation and ratification of every nation on earth.¹⁷¹ Lastly, it would require states to relinquish their sovereign authority over Internet activities that are entirely domestic and have no international effects or implications.

The Outer Space Treaty and Moon Treaty are extremely weak authority to support declaring the Internet CHM.¹⁷² International participation in CHM treaties falls well short of the global ratification required for an Internet CHM to be successful.¹⁷³ In addition, these treaties tend to promulgate aspirational goals concerning the use of resources that are extremely difficult or expensive to exploit, whereas proponents of an Internet CHM envision a comprehensive regulatory scheme.¹⁷⁴ Furthermore, the aspiration of peaceful and environmentally friendly space exploration has hardly been successful.¹⁷⁵ In sum,

¹⁶⁹ *Contra* Heaven, *supra* note 33, at 398.

¹⁷⁰ See Jamie Spataro, *Personal Jurisdiction over the Internet: How International Is Today's Shoe?*, 2 U. PITTSBURG J. TECH. L. & POL'Y art. 3, (2002), available at <http://tlp.law.pitt.edu/articles/VolIII-1Spataro.pdf>.

¹⁷¹ See *id.*

¹⁷² *Contra* Heaven, *supra* note 33, at 398.

¹⁷³ See U.N. Office of Outer Space Affairs, Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, <http://www.unoosa.org/oosa/en/SpaceLaw/outerspt.html> (last visited May 14, 2008); U.N. Office of Outer Space Affairs, Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, <http://www.unoosa.org/oosa/SpaceLaw/moon.html> (last visited May 14, 2008).

¹⁷⁴ See Heaven, *supra* note 33, at 402.

¹⁷⁵ See William Broad, *Orbiting Junk, Once a Nuisance, Is Now a Threat*, N.Y. TIMES, Feb. 6, 2007, at F1 (discussing space pollution); William Broad & David Sanger, *Flexing Muscle, China Destroys Satellite in Test*, N.Y. TIMES, Jan. 19, 2007, at A1 (discussing anti-satellite weapons).

existing CHM treaties have not demonstrated the feasibility of creating a universal set of concrete, binding Internet regulations.¹⁷⁶

Additionally, the international regulatory regime envisioned by CHM proponents attempts too much. As previous CHM treaties have shown, it is an extremely daunting task to get all nations to ratify such a treaty.¹⁷⁷ Even proponents admit that certain legal issues (e.g., issues over which countries are in sharp disagreement) would have to remain unaddressed by the initial treaty in order to gain universal support.¹⁷⁸ Many hotly debated jurisdictional issues, however, are those that are in the most critical need of resolution, such as freedom of expression¹⁷⁹ and validity of forum selection clauses.¹⁸⁰ Further complicating matters, the CHM solution would also attempt to promulgate substantive regulations.¹⁸¹ CHM proponents fail to see that nearly all Internet activities have real world analogs, such as libel,¹⁸² breach of contract,¹⁸³ intellectual property infringement,¹⁸⁴ identity theft, fraud,¹⁸⁵ pedophilia, drugs,¹⁸⁶ and product liability.¹⁸⁷ International Internet regulators would thus need to create an international rule for nearly every criminal and civil action available anywhere in the world.¹⁸⁸

Even if the CHM regulators were successful in getting every nation to adopt universal Internet rules, two significant concerns would likely arise. First, there would be conflicts between these universal Internet regulations and the domestic laws regulating the same activities. For example, if domestic libel laws differed from Internet libel regulation,

¹⁷⁶ *Contra Heaven*, *supra* note 33, at 398.

¹⁷⁷ *See id.* at 402.

¹⁷⁸ *See id.* at 400.

¹⁷⁹ *Compare Dawson*, *supra* note 142, at 662 (favoring expression), *with Gerlach*, *supra* note 1, at 912–13 (arguing sovereignty permits states to limit individual rights on Internet).

¹⁸⁰ *See Rice*, *supra* note 5, at 492–93.

¹⁸¹ *See Heaven*, *supra* note 33, at 400.

¹⁸² *See Clendenning*, *supra* note 10.

¹⁸³ *See Lester*, *supra* note 143, at 433–34 (discussing e-commerce contracts).

¹⁸⁴ *See MGM Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 918–19 (2005) (holding file-sharing website could be liable for copyright infringement by third-party users).

¹⁸⁵ *See United States v. Jackson*, 346 F.3d 22, 23 (2d Cir. 2003) (discussing defendant's commission of identity theft and fraud over Internet).

¹⁸⁶ *See Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Paris*, Nov. 20, 2000, *available at* <http://www.cdt.org/speech/international/20001120yahoofrance.pdf> (Fr.) (noting that Yahoo! filters content pertaining to pedophilia and drugs).

¹⁸⁷ If a jurisdiction recognizes product liability actions against traditional retailers, *see Vandermark v. Ford Motor Co.*, 61 Cal.2d 256, 262 (Cal. 1964), then, presumably, online retailers could also face liability.

¹⁸⁸ *See supra* notes 183–87 and accompanying text.

then a newspaper publisher and an Internet blogger might receive different treatments in the same court. Second, because states themselves have struggled with Internet issues, there is no reason to believe the international community would fare much better.¹⁸⁹ The Internet is a relatively new and constantly evolving medium, further decreasing the odds that an international convention could formulate a satisfactory set of standards.¹⁹⁰

Timing is another factor that works against a CHM solution.¹⁹¹ By the time the convention is able to draft regulations on which all nations can agree, Internet use may have evolved to the point where the regulations are obsolete before they are even ratified.¹⁹² If, for whatever reason, the CHM regulations turn out to be faulty, the international community would be essentially locked into those poor standards.¹⁹³ In short, a CHM solution is too stodgy for the rapid pace of Internet activity.¹⁹⁴

Lastly, the CHM solution would require courts to follow international standards in cases that in no way concern the international community. For example, there seems to be little reason for international standards of jurisdiction to apply in a case where an American plaintiff sues an American defendant for libel over the Internet. Sovereign nations have the right to create their own laws and enforce them within their borders and amongst their citizens.¹⁹⁵

B. *Targeting an International Standard for Internet Jurisdiction*

As discussed above, courts have applied several Internet jurisdiction tests; however, many commentators view the targeting test as the best.¹⁹⁶ An international convention solution might, therefore, adopt the targeting test as a global standard for determining international Internet jurisdiction or, at least, use it as a starting point for developing a new standard.¹⁹⁷ In addition, an international convention solution

¹⁸⁹ See Spataro, *supra* note 168, part II(1).

¹⁹⁰ See *id.*

¹⁹¹ See *id.*

¹⁹² See *id.*

¹⁹³ See *id.*

¹⁹⁴ See Spataro, *supra* note 168, part II(1).

¹⁹⁵ See Gerlach, *supra* note 1, at 912.

¹⁹⁶ See, e.g., Michael Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 16 BERKELEY TECH. L.J. 1345, 1380 (2001); Hestermeyer, *supra* note 7, at 286; Lester, *supra* note 145, at 465.

¹⁹⁷ See Hestermeyer, *supra* note 7, at 286.

might incorporate the targeting test with other provisions, such as filtering.¹⁹⁸

Of course, the adoption of a single standard for determining jurisdiction in Internet cases suffers from many of the same failings as the *res communes* solution; however, an international convention that is limited to jurisdictional issues is far less ambitious and time consuming than declaring the Internet CHM.¹⁹⁹ Adopting a targeting standard, or something similar, alleviates concerns about being locked²⁰⁰ into an inadequate universal standard because such a test would consider the totality of the circumstances under a list of non-exhaustive factors, thereby providing flexibility to adapt to changes in Internet uses.²⁰¹

C. Content Filtering: Inadequacies and Other Concerns

The question to ask is not whether governments and private entities are going to use filtering and monitoring technologies—that has already been answered in the affirmative.²⁰² Countries such as Saudi Arabia, Singapore, and China, have already implemented filtering and monitoring technologies in their Internet infrastructures.²⁰³ Other countries, such as Britain, Russia, and the United States, have taken steps to monitor Internet activities.²⁰⁴ These examples demonstrate the increasing desire of states to regulate Internet activities within their borders and suggest that filtering and monitoring technologies will continue to play a role in such regulation.²⁰⁵ The more difficult ques-

¹⁹⁸ See Lester, *supra* note 145, at 468.

¹⁹⁹ See Heaven, *supra* note 33, at 400–01 (acknowledging that incremental promulgation of regulations may be slow, but would avoid delays of regulating most controversial issues).

²⁰⁰ See Spataro, *supra* note 170, part II(1).

²⁰¹ See Hestermeyer, *supra* note 7, at 287.

²⁰² See Rice, *supra* note 5, at 455.

²⁰³ *Id.* Saudi Arabia links all thirty of the country's ISPs to a single Internet entrance-way to support its State-run telephony monopoly and ban content deemed subversive, contrary to the State, or damaging to its leaders' reputations. *See id.* at 455–56. Singapore requires its ISPs to install filters that remove content it considers to undermine public security, racial and religious harmony, or public morals. *Id.* at 457. Although China decentralized its Internet, it requires ISPs to filter out specific government banned sites. *See id.*

²⁰⁴ *Id.* Britain enacted a law extending phone tapping privileges to the Internet and private firms and individuals are required to help authorities decode data. Russian law requires telephone providers and ISPs to reroute data traffic to local law enforcement to permit monitoring of phone calls and emails. *See id.* at 458. The U.S. Department of Justice recently subpoenaed Google, Yahoo!, Microsoft, and AOL demanding the firms provide them with web search data of private users. See Arshad Mohammed, *Google Refuses Demand for Search Information*, WASH. POST, Jan. 20, 2006, at A01.

²⁰⁵ See Rice, *supra* note 5, at 455.

tions concerning these technologies are whether they are effective²⁰⁶ and whether they are appropriate.²⁰⁷

The efficacy of filtering technologies suffers from two significant problems. First, the technologies themselves currently lack the accuracy to create a completely effective e-border; however, proponents argue that advancements in technology will resolve these issues.²⁰⁸ Second, filtering and monitoring technologies are currently engaged in “a battle at the level of the architecture” with privacy technologies that circumvent filters and cloak their users’ identities and locations.²⁰⁹ Although governments using filtering and monitoring technologies have targeted privacy-protection sites, those sites have, so far, been able to develop new strategies to stay ahead of blocking technologies.²¹⁰

The technology war between governments and privacy-protection companies reflects the theoretical battle over whether Internet regulation is a good idea in general.²¹¹ Those in favor of filtering contend that the Internet is a lawless medium, and these technologies are necessary to protect national security, intellectual property rights, and cultural and religious values.²¹² Opponents argue that filtering technologies infringe on civil liberties and stifle global communication.²¹³ Critics point to restrictive regimes, such as China and Saudi Arabia, as evidence of filtering’s negative impact on human rights.²¹⁴ They fail, however, to explain why online speech deserves unique protections that would not be afforded to similar speech in newspapers, television, or radio.²¹⁵ Although the human rights and economic issues regarding filtering and monitoring technologies should concern the international community, keeping these issues separate from Internet jurisdiction would better facilitate the resolution of the latter.

²⁰⁶ See Gerlach, *supra* note 1, at 926–27.

²⁰⁷ See OpenNet Initiative, *supra* note 160.

²⁰⁸ See Gerlach, *supra* note 1, at 926–27; Rice, *supra* note 5, at 461.

²⁰⁹ Rice, *supra* note 5, at 459.

²¹⁰ See *id.* at 460–61.

²¹¹ Compare Gerlach, *supra* note 1, at 912–13 (arguing governments have right to impose speech inhibiting Internet regulations), with OpenNet Initiative, *supra* note 160 (arguing against uses of filtering for restricting speech).

²¹² See OpenNet Initiative, *supra* note 160.

²¹³ See *id.*

²¹⁴ See Rice, *supra* note 5, at 455–59.

²¹⁵ See Gerlach, *supra* note 1, at 912–13.

D. *Online Forum Shopping*

The validity of choice of forum contracts has long been a hotly debated issue.²¹⁶ The European Union has taken the stance that forum selection clauses are null and void in business-to-consumer contracts.²¹⁷ In the United States, however, courts acknowledge that “agreeing in advance on a forum acceptable to both parties is an indispensable element in international trade, commerce, and contracting.”²¹⁸ Because of this disagreement, it is unlikely that a solution to the Internet jurisdiction problem would include a provision permitting forum selection clauses in terms of service or online purchase agreements, at least in the context of a business-to-consumer contracts.²¹⁹ Forum selection clauses contained in high value business-to-business contracts, however, should be presumed valid because, at some point, the value of goods or services exchanged in the transaction indicates a level of sophistication sufficient to contract away such rights.²²⁰ Furthermore, the international Internet community should not be deterred from utilizing other common forms of ADR, such as credit card chargebacks.²²¹ In addition, the private sector should try and develop other informal, quick, and inexpensive forms of ADR to handle Internet disputes that would be more appealing to Internet users than traditional litigation.²²²

E. *A Proposal for an International Internet Convention*

Despite the variety of solutions currently available, questions concerning international Internet jurisdiction remain unresolved²²³ and continue to be a concern, particularly to content providers.²²⁴ The reason for the deadlock concerning Internet jurisdiction could reflect the fact that, as noted above, each of the most common solutions have significant drawbacks.²²⁵ Moreover, common ground is difficult to find because each of the common solutions are founded in starkly different

²¹⁶ See Lester, *supra* note 145, at 454.

²¹⁷ See Rice, *supra* note 5, at 492.

²¹⁸ *M/S Bremen v. Zapata*, 407 U.S. 1, 13–14 (1972).

²¹⁹ See Lester, *supra* note 143, at 454–55.

²²⁰ See *id.* at 455, 469.

²²¹ See *id.* at 469. When a consumer challenges a charge on their account, the card issuer can reverse the charge by issuing a chargeback to the merchant’s account. Chargebacks are fast, convenient, informal, and very common in both the United States and the European Union. See *id.* at 462–64.

²²² See *id.* at 463.

²²³ See Gerlach, *supra* note 1, at 902–03.

²²⁴ See Hestermeyer, *supra* note 7, at 267–68.

²²⁵ See Gerlach, *supra* note 1, at 905.

principles of Internet regulation.²²⁶ Nevertheless, the Internet's global scope makes it necessary for the international community to formulate universal standards for determining jurisdiction in Internet disputes.²²⁷

A convention on international Internet jurisdiction could achieve a global consensus on Internet jurisdiction with participation and ratification by every country.²²⁸ Although universal ratification will no doubt be very difficult, a convention limited to jurisdictional issues would be an easier sell than an attempt to completely carve out and regulate a new international space.²²⁹ Furthermore, over time a convention ratified by a majority of states could still become binding customary law.²³⁰ The convention should strongly consider adopting some version of the targeting test because it is flexible and has been successfully applied in several jurisdictions.²³¹ A targeting test considers steps taken by content providers to avoid the jurisdiction, thus reducing the likelihood that content providers will be forced to litigate in unforeseen jurisdictions.²³² In formulating its targeting test, the convention should identify a number of factors it considers of high probative value, such as the use of disclaimers, filtering technology, and the accepted forms of currency.²³³ The convention might consider whether forum selection clauses should be presumed valid in the context of high value transactions between sophisticated businesses.²³⁴ The convention should avoid highly contentious issues, such as business-consumer choice of forum agreements, substantive Internet regulations, and the appropriateness of nation-level content filtering and Internet monitoring.²³⁵

CONCLUSION

The lack of clear standards for determining jurisdiction in Internet cases is an international problem requiring an international solution. Although achieving full participation and ratification by every nation will likely be an extremely difficult task, no other viable solutions are available. A convention on international Internet jurisdiction is nec-

²²⁶ See Eko, *supra* note 72, at 482.

²²⁷ See Heaven, *supra* note 33, at 400.

²²⁸ See *id.* at 402.

²²⁹ See *id.*

²³⁰ See *The Paquete Habana*, 175 U.S. 677, 708 (1900) (holding capture of civilian fishing vessel contrary to customary law independent of any treaty).

²³¹ See Hestermeyer, *supra* note 7, at 286.

²³² See *id.* at 286–87.

²³³ See *id.*

²³⁴ See Lester, *supra* note 143, at 469.

²³⁵ See Heaven, *supra* note 33, at 400.

essary to clarify the expectations of the Internet community. Currently, content providers could be sued anywhere and everywhere for unintentionally violating domestic laws they never knew existed. Similarly, Internet users must surf the web without any certainty that redress is available for harms they might suffer in cyberspace. The international community should not allow this jurisdictional void to continue, and a universal standard for determining international Internet jurisdiction based on the targeting test should be adopted.

