1. INTRODUCTION

Technological innovation on the internet has brought the globalization trend to businesses and spawned an industry of "e-commerce" that has forever changed the way companies provide goods and services. Company web sites are accessible to virtually any internet user in the world. It is the unique global character of the internet to develop, however, that has prevented a uniform approach to jurisdiction over cases involving consumer transactions via the web. "Jurisdiction is the power and authority of a court to hear and determine a judicial proceeding."1 The lack of a uniform legal framework for jurisdiction regarding internet transactions between different countries means companies face the possibility of being subject to any foreign legal judgments in which their web sites can be accessed. The unpredictability of jurisdiction makes it difficult for companies with web sites to limit their legal liability and inhibits the growth of e-commerce.

This Comment will focus on the different approaches taken by the United States and European Union ("EU") towards determining jurisdiction and how this lack of uniformity limits the growth of the e-commerce industry because of the various strategies businesses must employ to limit their legal liability. Section 2 of this Comment gives an overview of the internet and how its infrastructure simultaneously encourages and hinders the development of e-commerce. Section 3 analyzes the U.S. and EU approaches for determining jurisdiction in internet cases.

---

* J.D. candidate, 2004, University of Pennsylvania Law School; I would like to thank my family for their love and support, and the Board members of the Journal of International Economic Law at the University of Pennsylvania for their hard work on this Comment. To the Comish and Batman - you made it bearable. I would also like to thank Schnader Harrison for this article's inspiration.

Beginning with the U.S.'s traditional framework of subject matter jurisdiction and personal jurisdiction that centers on a party's domicile, this Section goes on to explain the difficulties of establishing the domicile of an internet user who is party to a lawsuit. The two primary tests U.S. courts have used in deciding jurisdictional issues are the sliding scale commonly known as the "Zippo continuum," named after a case where the court held that a court's jurisdiction is dictated by a sliding scale between highly interactive contact and passive contact between the defendant company's web site and the plaintiff, and a broader, effects-based approach that analyzes where the actual effects of a web site occurred to determine jurisdiction. Next, this Section analyzes the EU's multi-prong regulatory approach. In March 2002, the European Council ("EC") revised the Brussels Convention in the form of the Brussels Regulation ("Brussels I") which attempted to create a uniform approach to internet jurisdiction within the EU. The legislation that focused on business-to-consumers ("B2C") transactions adopted a country-of-destination approach that is heavily protective of consumers by giving the consumer the choice of litigating in their local jurisdiction. In addition to Brussels I, the EC is also contemplating a proposed revision to the Rome Convention, which dictates the substantive law the Court should apply in a case, known as Rome II. Section 4 discusses the weaknesses of both the U.S. and EU approaches and the problem with developing a hybrid approach as the draft Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters is attempting to do.

---


7 See Hague Conference on Private International Law, Future Hague
Finally, Section 5 explains the various strategies businesses can employ to avoid jurisdictional disputes and examines the question of whether there is any legitimate protection from, or sufficient limitation to, legal liability.

2. OVERVIEW OF THE INTERNET AND ELECTRONIC COMMERCE

2.1. Development of the Internet

In 1969, the U.S. Department of Defense's Advanced Research Project Agency ("ARPA") created an experimental project called ARPANET, the internet's predecessor. ARPANET's purpose was "to be a decentralized, self-maintaining series of redundant links between computers and computer networks, capable of rapidly transmitting communications without direct human involvement or control, and with the automatic ability to reroute communications if one or more individual links were damaged or otherwise unavailable."\(^8\) The design was deliberately decentralized as a defense mechanism during the Cold War era. In 1984, the National Science Foundation ("NSF") established NSFNET for the purpose of encouraging the use of the internet throughout the higher education system and also agreed to provide the backbone for U.S. internet service by supplying supercomputers which made higher volume traffic possible.\(^9\) Dr. Tim Berners-Lee created the universal language of Hypertext Markup Language ("HTML") in the late 1980s that linked documents to computers connected to the internet and created the world wide web ("WWW").\(^10\) When asked about the difference between the internet and the web, Dr. Berners-Lee answered:

The internet ('Net) is a network of networks. Basically it is...

---


\(^10\) Id.
made from computers and cables. What [the founders of the internet] did was to figure out how this could be used to send around little "packets" of information. . . . That's what the Internet does. It delivers packets— anywhere in the world, normally well under a second . . . . The Web is an abstract (imaginary) space of information. On the Net, you find computers— on the Web, you find documents, sounds, videos . . . information. On the Net, the connections are cables between computers; on the Web, connections are hypertext links.  

In 1993, Marc Andreesen developed the first web browser called Mosaic X that allowed for searches on the internet. The combination of HTML, which made graphically-attractive web sites, and an internet browser, which made it easier to access those web sites, made the world wide web more user-friendly to the public.

2.2. Technical Basics of the Internet

There are two types of computers connected to the internet— clients and servers. A client, such as a browser, is a software program in the computer that reads files from a web server. The browser contacts a server and requests information while the server provides that requested information to clients. Based upon Transmission Control Protocol/Internet Protocol ("TCP/IP"), data is broken up into packets, each of which is accompanied by the router information (to help point the way to the destination), header information (IP addresses of origin and destination computers), TCP/IP information (method of breaking down, placing header information, determining size of packets, sending packets, ensuring arrival, resending bad packets, verifying data) and the actual data. The TCP divides the data into packets while the IP gives each packet the address of the final destination. Each

11 Id.
12 Id.
packet is sent along a chain of routers that connect the various networks of the internet together. The routers determine the most efficient path for the packet, which means that if one route is particularly slow or damaged, the packet is simply rerouted and when the receiving computer has all the packets in its proverbial hand, it can reassemble the file and display the document to the recipient user.¹⁵ A Uniform Resource Locator ("URL") is an address for a specific web site and each portion of the URL contains information.¹⁶ For example, in the URL http://www.dukebasketballreport.com/summaries/index.cgi?268, "http://" indicates the protocol (http is a HTML document), "www.dukebasketballreport.com/" indicates the server or domain name, "summaries/" indicates the path name to the directory requested (like a folder), and "index.cgi?268" is the filename requested (actual data wanted).¹⁷ To access the internet, a computer must be connected to a gateway which then connects it to a network of networks which is the internet.¹⁸


¹⁷ The Duke Basketball Report web site is dedicated to the Duke Men's Basketball team and maintained by rabid Duke fans.

2.3. Electronic Commerce (E-Commerce) Growth

The internet has become more accessible and user-friendly, with an estimated 700 to 945 million internet users projected in 2004. Not only have more people been accessing the internet, but more people have been utilizing it to set up their own web sites, as well. According to the Organization for Economic Cooperation and Development ("OECD"), in July 2000, the United States hosted 46.5 web sites per 1000 inhabitants while the EU hosted 12.7 web sites per 1000 inhabitants. It is not surprising, then, that e-commerce involving sale of goods and services on the internet has exploded, as well. There are primarily two types of transactions in e-commerce—B2C relationships and business-to-business ("B2B") relationships. B2C transactions involve the purchase of products by individuals outside their trade or profession while B2B transactions involve performance against payment or performance against performance. In 1999, the ratio between B2C and B2B transactions reached 40%/60% in the United States and 31%/69% in the EU. This trend does not seem to be diminishing for "[e]ven after the dot-com shakeout in the year 2000, Forrester [Research, Inc.] predicted that North American e-commerce alone 'would reach $3.2 trillion in 2004.'"
2.4. How the Internet’s Design Impacts E-Commerce Businesses

2.4.1. Advantages for Businesses

The internet’s global expanse enables businesses to reach millions of potential customers through their web sites. There is a low cost of entry into the marketplace as a business need only to invest in a computer and an internet connection to have a worldwide presence. Record-keeping can become more accurate because web transactions can be recorded with computer software that never requires manual entry. Time spent on customer service becomes more efficient as well, for the web permits a company to communicate with its customers more quickly through e-mail or even instant messaging programs that operate in real-time (instantaneous time).23

2.4.2. Disadvantages for Businesses

As beneficial as the internet can be to a business, it also exposes the business to some unorthodox risks not seen in traditional commercial transactions. An e-commerce transaction is more difficult to trace, identify, and distinguish. This lack of transparency allows for anonymity, should the consumer desire it.24 Such anonymity could make it potentially difficult to resolve any disputes that arise from the transaction itself. A customer could leave the company unpaid, and it could be difficult to track him down. Due to the anonymity of the consumer party, any resolution would be far-fetched, if not impossible.

Furthermore, there are also security risks that may be more technologically advanced than a business is equipped to handle.25 For example, denial of service ("DOS") attacks launched by

23 Lenda, supra note 14, at 27.

24 Id. at 28 ("There are at least five different aspects of the anonymity of Internet transactions: who (which person or persons) are involved in the transaction; what constitutes the object of the transaction (including elements of privacy); where does the transaction take place; when does an activity have legal consequences; and how are transactions performed.").

25 Hackers may be able to enter a company’s electronic archive and steal vital information, such as customer credit card numbers. Viruses or denial-of-service (DOS) attacks can render a company web site inaccessible. See, e.g., Financial Times, Virus Hits A.T.M.s and Computers Across Globe, N.Y. Times, Jan. 26, 2003 (demonstrating how a virus can affect e-commerce), at http://www.nytimes.com/2003/01/26/business/FT1042491212045.html.
hackers which prevent communication between the network and its clients and servers are commonplace. In February 2000, there were three straight days of DOS attacks on Yahoo!, Amazon.com, Buy.com, CNN.com and other popular web sites which slowed down web traffic considerably and cost businesses lost revenue.\(^{26}\) Normally, a client computer will send a request to a server for authentication. The server returns authentication approval and the client computer is allowed on to the network.\(^{27}\) In a DOS attack, the client sends numerous requests to the server which ties up the network's other lines.\(^{28}\) Because these requests usually have false addresses, when the server tries to return authentication approval, it cannot.\(^{29}\) In similar fashion to a fax machine, the server then waits a few minutes before trying to return the authentication approval again.\(^{30}\) After a few tries, it then quits, whereupon the client sends another batch of false authentication requests, thereby starting the process all over again.\(^{31}\) Aggregated activity from several client computers makes it difficult for the server to distinguish between legitimate and false traffic.\(^{32}\) As a result, a DOS attack clogs up internet traffic and slows down activity on the web sites that are being attacked. Protecting a company's web site from DOS attacks or other computer viruses can be costly and in some cases, prohibitive.

### 3. U.S. AND EU APPROACHES TO INTERNET JURISDICTION

Traditionally, jurisdiction in legal systems has been anchored in the geographic location of the parties in a lawsuit.

#### 3.1. U.S. Approach to Internet Jurisdiction

##### 3.1.1. Traditional Notions of Jurisdiction in the U.S. Courts


\(^{28}\) Id.

\(^{29}\) Id.

\(^{30}\) Id.

\(^{31}\) Id.
In the United States, subject matter jurisdiction ("SMJ") deals with the court’s authority to hear and decide cases in certain areas of the law. Personal jurisdiction is the court’s authority over a defendant and arises only when a defendant has sufficient ties to a state that makes him answerable to that state’s courts. When a connection is found between the defendant and the state, the defendant is served a summons, or notice, about the lawsuit pending against him. Most states have long-arm statutes that set the state’s guidelines for when its courts can assume jurisdiction over a non-resident defendant. To comply with due process concerns, personal jurisdiction cannot offend “traditional notions of fair play and substantial justice.” There are two kinds of personal jurisdiction—general and specific. General jurisdiction is asserted over a non-resident defendant only if the defendant’s contacts with the state are “continuous and systematic,” even if the contacts are unrelated to the dispute at hand. Specific jurisdiction arises when the lawsuit is related to the defendant’s contacts with the forum state. Ultimately, the question is whether the defendant’s “minimum contacts” with the forum state can cause him to reasonably anticipate being sued in the forum state’s Court. There are three tests courts have used to find whether the defendant’s minimum contacts with the forum state reached the level to cause specific jurisdiction to arise. A defendant may purposefully direct his activity towards a forum state, purposefully avail himself of the benefits of doing business in the forum state, or deliver his products into the stream of commerce of the forum state to satisfy the requisite level of contact for specific jurisdiction.

---

32 Id.
33 FRASCOGNA, JR. ET. AL, supra note 1, at 143-44.
34 See Int’l Shoe Co. v. Washington, 326 U.S. 310 (1945) (explaining how the long-arm statute gives courts authority to assume jurisdiction over non-residents).
35 Id. at 316 (citations omitted).
36 Id. at 317.
37 Id.
38 Id.
40 Burger King Corp. v. Rudzewicz, 471 U.S. 462 (1985).
3.1.2. Difficulties of Determining Jurisdiction in Internet Cases

The traditional notions of jurisdiction focus heavily on the location where the transaction in dispute took place to determine the proper jurisdiction to adjudicate the dispute. However, internet transactions are conducted over a network, and as a result, it does not conform to traditional geographic boundaries. There are several ways that the infrastructure of the internet has made it difficult to establish the geographic location of the internet user.

(1) The internet is insensitive to geographic location and is designed to ignore rather than document geographic location.\textsuperscript{42}

(2) Addresses on the internet are digital and not geographic addresses.\textsuperscript{43}

(3) The internet cannot feasibly be closed to users from another state as it is, by nature, an instrument of interstate commerce.\textsuperscript{44}

(4) The user name and e-mail address are often the only indicators of a user’s identity.\textsuperscript{45} As a result, a consumer buying goods through a web site may not be sure where the seller is located geographically.

(5) Information travels through many different paths through the internet which makes tracing difficult.\textsuperscript{46}

(6) There is no way to avoid an internet user’s message from reaching residents of any particular state.\textsuperscript{47}

Because of the internet’s decentralized and anonymous nature, determining whether a defendant has made minimum contact with a forum state is extremely difficult. Is the click of a button to enter

\textsuperscript{42} See Cyberspace Communications, Inc. v. Engler, 55 F. Supp. 2d 737, 741-45 (E.D. Mich. 1999) (describing the various unique characteristics of the internet and the consequent difficulty in establishing a party’s domicile); but see The Internet’s New Borders, ECONOMIST, Aug. 9, 2001, available at http://www.economist.com/agenda/displayStory.cfm?Story_id=730089 (arguing that old geographic borders are proving to be resilient on the internet because of the lack of consumer sophistication to manipulate their electronic location).

\textsuperscript{43} Id.

\textsuperscript{44} Id.

\textsuperscript{45} Id. at 742-43.

\textsuperscript{46} Id. at 745.

\textsuperscript{47} Id.
a web site or the mere existence of a web site enough for minimum contact? Is the state where the server is maintained to keep the web site running or the state where the recipient views the web site the forum state? Indeed, "[i]t is unique to the internet that these minimum contacts can be established without any physical presence by or on behalf of the company in a given state."\textsuperscript{48} The courts have only begun a piecemeal approach towards applying specific jurisdiction standards to internet cases.

3.1.3. Development of U.S. Case Law in Internet Jurisdiction

U.S. courts have tended to focus on the actions of the seller (or web site owner) rather than the actions of the consumer in determining whether or not specific jurisdiction has arisen. One of the most significant developments has been that of the "Zippo Continuum," or sliding scale of contact as delineated by the District Court in the Western District of Pennsylvania in Zippo Mfg. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997).\textsuperscript{49} The manufacturers of "Zippo" tobacco lighters, incorporated in Pennsylvania, sued the defendant, Zippo Dot Com, a California-based news service which obtained exclusive use of several domain names such as "zippo.com," "zippo.net," and "zipponews.com."\textsuperscript{50} The Western District of Pennsylvania Court exercised jurisdiction over the defendant, despite the fact that the news service's offices, employees and internet servers were all in


Cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location. The rise of the global computer network is destroying the link between geographical location and: (1) the power of local governments to assert control over online behavior; (2) the effects of online behavior on individuals or things; (3) the legitimacy of a local sovereign's efforts to regulate global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply.


\textsuperscript{49} Mere interactivity that allows a consumer to make a transaction through a web site does not seem to merit enough minimum contact to justify personal jurisdiction. Snyder v. Dolphin Encounters Ltd., 235 F. Supp. 2d 433 (E.D. Pa. Dec. 10, 2002).

California. Its only contact with Pennsylvania was advertising for the news service on its web site through which it gained 3000 Pennsylvania residents as subscribers. The defendant also contracted with seven internet access providers to allow their customers to access its web site, and two of those providers were based in Pennsylvania. The Court defined the Zippo continuum as a spectrum that ranges from active (where the defendant clearly does business over the internet through repeated transmissions of files over the web) to passive (where the defendant has merely made information available on the web and no interchange between the web site and visitor is allowed) with the middle ground occupied by the interactive (where a web site enables a user to exchange information with the host computer). Using this guideline, the Court held that the defendant actively intended and did conduct business in Pennsylvania, thus satisfying minimum contacts. The Zippo test has been adopted by various federal appellate circuits, as in Gator.com v. L.L. Bean, Inc., where the Ninth Circuit held that L.L. Bean’s web site presence in California via its online store operated “as the functional equivalent of a physical store,” and that the Zippo test “does not require an actual

51 Id.
52 Id.
53 Id. (citations omitted).
54 [T]he likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet. This sliding scale is consistent with well developed personal jurisdiction principles. At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involved the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. At the opposite end are situations where a defendant has simply posted information on an Internet web site which is accessible to users in foreign jurisdictions. A passive web site that does little more than make information available to those 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.

Id. at 1124.
55 Id. at 1125-27.
56 Gator.com v. L.L. Bean, Inc., 341 F.3d 1072, 1079 (9th Cir. 2003).
presence in the state. Rather, the nature of the commercial activity must be of a substantial enough nature [so as to be an equitable substitute for a physical store]." 57 As a result, L.L. Bean was subjected to personal jurisdiction in California, despite its Maine incorporation and its principal place of business and headquarters being located in Maine.

Another test courts have used is the effects-based test which allows a court to exercise personal jurisdiction if the harm occurs in the forum state and the defendant knew that it would occur there. 58 For example, in Calder v. Jones, the plaintiff was a professional entertainer who worked in California and sued the writers who were based in Florida for libel as a result of an article they wrote that was published in the National Enquirer. 59 The Supreme Court held that California courts could exercise jurisdiction over Florida residents for the article that censured the plaintiff because the story concerned the California activities of the California resident, was drawn from California sources, and the brunt of the harm was felt in California. 60 In the effects-based test, rather than examining the specific characteristics of a web site to determine its level of contact, the court focuses on the actual effects the web site has had in the forum state. This foreseeability factor of the effects-based test, while rather expansive in theory, has been limited by a targeting requirement. 61 The targeting requirement has a three-prong test. The defendant must: (1) direct electronic activity into the forum state; (2) intend to engage in business or other interactions in the forum state; and (3) engage in activity that created under the forum state's law a potential cause of action with regard to a person in the forum state. 62 For example, in Young v. New Haven Advocate, two Connecticut newspapers posted on the

57 Id.
59 Id. at 783.
60 Id.
61 See ALS Scan, Inc. v. Digital Serv. Consultants, Inc., 293 F.3d 707, 714 (4th Cir. 2002) (adapting from the Zippo Continuum and creating a three-prong test for finding express targeting or aiming); see also Revell v. Lidov, 317 F. 3d 467 (5th Cir. 2002) (supporting the Court of Appeals for the Fourth Circuit's targeting approach); Pavlovich v. Superior Court of Santa Clara County, 58 P.3d 2 (Cal. 2002) (holding that mere foreseeability of the potential harm is not enough to establish jurisdiction under the effects-based test).
62 See ALS Scan Inc., 293 F.3d at 714 (adapting from the Zippo Continuum and creating a three-prong test for finding express targeting or aiming).
internet an article about the housing of Connecticut prisoners in Virginia and allegedly defamed a Virginia prison warden. The Fourth Circuit Court ruled that Virginia could not exercise personal jurisdiction because the Connecticut defendants did not target their web site or article at Virginia residents. Thus, in order for the effects-based test to apply, the defendant must intend to aim his web site at a particular forum state or its residents.

However, since e-commerce is still in its infancy, it is unlikely that the sliding scale test or effects-based test is the final evolution of determining jurisdiction in internet cases in the United States.

3.2. EU Approach to Internet Jurisdiction

The EU approach to internet jurisdiction is markedly different from the U.S. approach in that it is highly regulatory. The EU already suffers from a lack of skilled information technology ("IT") workers. It is a phenomenon partially attributed to the lack of incentive for Europeans to aggressively upgrade their job skills since they are guaranteed a comfortable minimal standard of living from the social safety net of benefits the EU countries provide. Rather than letting the private sector lead in developing the commercial aspects of the internet, the EU response has been to pass legislation to regulate the internet’s commercial development. The EU’s goal is to create an entrepreneurial business culture similar to the United States' culture, but retain their socially protective benefits, as well. Because the EU approach has been to establish a series of bright-line rules, this Section will only focus on B2C consumer transactions over the internet, as addressing all commercial transactions would be too vast of a topic.

63 See Young v. New Haven Advocate, 315 F.3d 256 (4th Cir. 2002) (demonstrating the effect of the targeting requirement).
66 Id. at 83.
67 Id. at 89.
3.2.1. Brussels Convention

The 1968 Brussels Convention\(^68\) dealt with the issues of jurisdiction and the enforcement of foreign judgments. Instead of the legislation becoming automatic, member states to the Convention were required to enact laws in their own countries that gave effect to the objectives of the Convention.\(^69\) According to the Brussels Convention, in a typical commercial transaction, the plaintiff would sue in the "place of performance of the obligation in question"\(^70\) or where the transaction is or should have been completed.\(^71\) Consumer transactions were dealt with differently from regular commercial transactions as it gave consumers a choice of jurisdictions. Article 13 of the Brussels Convention defined a consumer contract as B2C contract for goods and services for the purposes outside a consumer's normal trade or profession if it met the following requirements:

1. the contract was for the sale of goods on installment credit terms; or
2. a contract for a loan repayable by installments, or for any other form of credit, made to finance the sale of goods; or
3. any other contract for the supply of goods or services.\(^72\)

In addition, the conclusion of the contract had to be preceded by a specific invitation addressed to the consumer or by advertising in his state of domicile and the consumer had to take in his state of domicile the steps necessary for the conclusion of the contract.\(^73\) Article 14 gave the consumer a choice of jurisdictions between either his own domicile, or that of the supplier (e.g., web site owner).\(^74\) This bright-line rule left little room for debate. If the contract met the requirements of a consumer contract, the consumer had the option of choosing the jurisdiction in which to

\(^{68}\) Brussels Convention, supra note 3.
\(^{69}\) Id.
\(^{70}\) Brussels Convention, supra note 3, art. 5(1).
\(^{72}\) See Brussels Convention, supra note 3, art. 13 (defining consumer contract).
\(^{73}\) Id.
\(^{74}\) Id. art. 14.
litigate. A consumer could also choose to forgo the choice of jurisdiction by opting to make an agreement with the supplier as to which court would have jurisdiction before agreeing to the contract in a forum selection clause. This opt-out choice was allowed only if it fulfilled several formal requirements. The agreement had to: (1) be in writing; (2) be in a form that conformed to practices established between the parties; and (3) in international trade or commerce, be in a form that accorded with a usage of certain dignity. However, jurisdiction was an entirely different story for suppliers (e.g., sellers). In a restriction against suppliers, Article 14 only permitted suppliers to bring suit in a consumer's domicile. The restriction against suppliers also applied to non-EU suppliers who had branch offices in the EU. The Brussels Convention clearly favored consumers in its jurisdiction provisions.

3.2.2. Brussels I Regulation

While the Brussels Convention clearly dealt with jurisdiction, it had not anticipated the internet and the unique difficulties e-commerce would cause courts in determining where a case should be heard. As noted in Section 3.1.2, merely establishing the domicile of an internet user could be difficult. Furthermore, e-commerce in the EU clearly lagged behind the United States and much of this was attributed to lack of consumer confidence in the security of internet transactions. As a result, on December 22, 2000, the EU's Council of Ministers adopted Brussels I in an effort to modernize the Brussels Convention. Brussels I came into force in March 2002. Brussels I differed from the Brussels Convention in

---


76 Lindberg, supra note 71.

77 Brussels Convention, supra note 3, art. 14.

78 Id. at art. 13.

79 See, e.g., FRANDA, supra note 65, at 91 (“In 1999, for example, the EC [European Community] estimated e-commerce revenues for the fifteen EC nations at only $16.8 billion, compared with $71.4 billion . . . for the United States alone.”).

80 See Victorya Hong, “Brussels I” Angers EC Businesses, INDUS. STANDARD, Dec. 1, 2000 (on file with author) (quoting Leonello Gabrici, a commission spokesman, stating “[a] lack of consumer confidence is the main thing holding up the development of e-commerce”).

81 Brussels I, supra note 4.

82 Id.
adoption, for it was directly binding on the members of the EU, rather than having each country adopt its own version in its statutory code.\textsuperscript{83}

There was great debate over whether Brussels I would take a country-of-origin or country-of-destination approach in consumer transactions. The country-of-origin approach dictates that all legal disputes over transactions contracted over the internet would be determined by the law of the supplier, where the good/service originated.\textsuperscript{84} Consumers are thought to be disadvantaged by this approach because the approach subjects them to foreign laws they may not be familiar with when purchasing a product in another member state of the EU. This problem is only compounded if the seller masks his domicile on his web site.\textsuperscript{85} The country-of-destination approach applies the law of the consumer's domicile in legal disputes over internet transactions. This is advantageous for consumers,\textsuperscript{86} but it leaves sellers vulnerable to being subject to any foreign jurisdiction where their web site can be accessed.

The drafters of Brussels I chose to embrace a country-of-destination approach in the name of boosting consumer confidence in e-commerce. Article 15 of Brussels I broadened the definition of consumer transactions in Article 13 of the Brussels Convention. Whereas the Brussels Convention required that the consumer contract had to be preceded by specific advertisement or invitation and be completed in the consumer's domicile,\textsuperscript{87} Brussels I makes

\textsuperscript{83} Id. art. 76.


\textsuperscript{85} At present it is often unimportant, and sometimes impossible, to discover the geographic origin of a particular electronic communication. . . . It is easy for fraudsters to access a large number of consumers through an Internet presence which is both simple to change and difficult to link back to the fraudster.


\textsuperscript{87} See Brussels Convention, supra note 3, art. 13 (defining consumer contract).
no mention of the latter requirement that the contract be completed in the consumer's domicile\(^8\) because for the purposes of internet transactions, a consumer's physical location is difficult to ascertain.\(^8\) Furthermore, Brussels I makes clear that contracts completed via an interactive web site falls within its confines,\(^9\) thereby giving every EU consumer who buys a good/service through the internet the privilege of litigating in their own domicile. The consumer's freedom to choose which domicile she will bring a cause of action is significantly strengthened.\(^9\)

Brussels I also retained the Brussels Convention limitation that restricted a supplier's choice-of-law to bringing suit in the consumer's domicile.\(^9\) Lastly, while Article 17 in Brussels I allows for forum selection clauses,\(^9\) it does not allow any such contractual agreements to take away the consumer's right to bring suit in his home jurisdiction, unless the agreement is entered into after the dispute arises.\(^9\) Ultimately, if a seller is running a web site that is "directing its activities" towards an EU member state, under Brussels I, the seller would be under that member state's jurisdiction.\(^9\)

Brussels I unabashedly protects the consumer's choice of forum by embracing the country-of-destination approach.

### 3.2.3. Rome II Draft Proposal

While the Brussels Convention and Brussels I deal with which

---

88 Compare Brussels I, supra note 4, art. 15(1)(c) (explaining when and how a contract is concluded) with Brussels Convention, supra note 3, art. 13(3) (describing extra requirements for conclusion of a contract).

89 Commission Proposal for Council Regulation Concerning the Jurisdiction and the Recognition of Judgments in Civil and Commercial Matters, COM(99)348 final at 7 [hereinafter Commission Proposal].

90 See Brussels I, supra note 4, art. 15(c) (making clear that a supplier who pursues or directs commercial activity into a consumer's member state has taken the necessary step towards linking the transaction to the consumer's domicile).

91 Id. art. 16(1).

92 Id. art. 16(2).

93 Forum selection clauses are agreements between both parties of a contract to select a predefined jurisdiction to resolve any potential conflicts arising from the contract.

94 Brussels I, supra note 4, art. 17.

court has jurisdiction over a case, the 1980 Rome Convention ("Rome I") deals with the substantive choice of law that applies once a court is chosen to hear the contractual dispute in B2B or B2C transactions.\textsuperscript{96} It permitted consumer contracts to include a forum selection clause, as long as the consumer was not denied protections of his local consumer law.\textsuperscript{97} This consumer protection was allowed, provided that the contract was preceded by a specific advertisement or invitation targeted at the consumer or the consumer's member state and that the contract was concluded in the consumer's domicile.\textsuperscript{98} In a similar move to update Rome I, the EU has drafted a proposal, Rome II, which is intended to harmonize the member states' rules regarding conflict of laws.\textsuperscript{99} While Rome I applied to both contractual and non-contractual matters, Rome II applies to non-contractual matters only.\textsuperscript{100} Specifically, Rome II would apply to cross-border liability for disputes in which there are no contracts. Its tentative proposal also embraces a country-of-destination approach\textsuperscript{101} and applies the law of the country where the injured person (consumer plaintiff) resides in non-contractual obligations.\textsuperscript{102}

Rome II has not yet passed, for its subject—substantive choice-of-law—is a more complicated issue to find agreement. As Mark Bohannon of the Software and Information Industry Association remarks, "Rome II deals with substantive law. The notion that they're going to be able to transpose the country-of-destination rule into a substantive law theory is going to be much different than when you're talking about, basically, a venue-jurisdiction

\textsuperscript{96} Rome I, supra note 5.
\textsuperscript{97} Rome I, supra note 5, art. 5.
\textsuperscript{98} These provisions are similar to those mandated in Brussels I. Rome I, supra note 5, art. 5(2).
\textsuperscript{99} Rome I, supra note 5.
\textsuperscript{100} Dr. ECommerce, Apr. 29, 2001, available at http://europa.eu.int/ISPO/ecommerce/drecommerce/answers/000331.html.
\textsuperscript{101} But see Green Paper, supra note 6, at 31 (explaining how streamlining Rome II with Brussels I is still difficult because of the bifurcation between non-consumer and consumer categories); see also Dickie, supra note 85, at 131 ("[T]he divergence of foci within Community law between consumer-protection measures and non-consumer-protection measures reduces its coherence.").
question.”\textsuperscript{103} In July 2003, business representatives from the International Chamber of Commerce (“ICC”) expressed serious reservations about the Rome II draft and its country-of-destination approach.\textsuperscript{104} As Michael Hancock, an internet law expert who co-heads ICC’s work on e-commerce jurisdiction issues, comments, “Companies providing services to customers outside the European Union could be sued under a variety of laws, depending on where the claimant happened to live or simply has a product.”\textsuperscript{105} As a result, “[Rome II] would be a nightmare for any business offering services on the internet,” says Jonas Astrup, ICC’s policy manager for Commercial Law and Practice.\textsuperscript{106}

4. WEAKNESSES OF THE U.S. AND EU APPROACHES TO INTERNET JURISDICTION AND THE DIFFICULTY OF A HYBRID APPROACH

While the United States has relied on its courts and the EU has relied on legislation to determine jurisdiction in cases involving consumers’ internet transactions, there are significant weaknesses with each approach that become significantly compounded when a trans-Atlantic approach is attempted for uniformity purposes.

4.1. Weakness of the U.S. Approach to Internet Jurisdiction

The fundamental weakness of the U.S. approach is its lack of predictability. As opposed to bright-line rules established in the EU, businesses must interpret whether or not their web sites reach the level of interactivity courts will find to suffice for minimum contacts. Because judicial decisions are the only measure by which businesses have to go by, the infancy of e-commerce means that the two current tests, Zippo Continuum and effects-based, are unlikely to be permanent or bright-line rules. As Thomas Vartanian, former chair of the American Bar Association Global Cyberspace Jurisdiction Project, noted:

“Anyone doing business in cyberspace needs to know what

\textsuperscript{103} Anandashankar Mazumdar, EU Actions on Jurisdiction, Choice of Law Watched Closely by E-Commerce Interests, 7 BNA, INC. ELEC. COM. & L. 251 (2002).


\textsuperscript{105} Id.

\textsuperscript{106} Id.
laws to obey, whether it be a question of what taxes are due and where, or what consumer protections apply to the sale of their products or services. . . . [A] legal infrastructure that can provide the requisite elements of certainty and predictability . . . will allow electronic commerce to flourish as efficiently as market forces dictate.\textsuperscript{107}

Because the United States relies on its private sector to push the boundaries on what should and should not be regulated in this internet sector,\textsuperscript{108} legal rules are constantly in flux.

4.2. Weakness of the EU Approach to Internet Jurisdiction

While the EU's Brussels I and draft Rome II proposal both emphasize bright-line rules for consumer transactions, there remain significant weaknesses with this regulatory approach. First, the statutes, as they are written, still remain ambiguous in their interpretation as applied to the internet. Second, the country-of-destination approach hampers the growth of e-commerce in the EU which is precisely the opposite effect intended by the EU.\textsuperscript{109}

4.2.1. Ambiguity of the "Directed" Intent

Article 15 of Brussels I requires that a supplier specifically direct advertising or invitation towards a consumer.\textsuperscript{110} In addition, the Commission's proposal made clear that consumer contracts that were entered into via an interactive web site activated Brussels II's special consumer protection clauses.\textsuperscript{111} Essentially, these country-of-destination protections were to prevent the passive consumer from becoming subject to foreign jurisdiction and foreign laws merely by participating on the web. However, "e-
commerce blurs the definition of the passive consumer."\(^{112}\) It could be argued that the typical passive consumer is the person who is solicited by email to purchase a product made by a foreign supplier. But what about the internet user who arrives at a foreign web site by clicking on various links? Is she deemed to be a passive consumer worthy of special consumer protection under Brussels I or actively making foreign contact?

Michael Cordera, in his comment titled *E-Consumer Protection: A Comparative Analysis of EU and US Consumer Protection on the Internet*, argues that the drafters of Brussels II misinterpreted the nature of e-consumer transactions and subsequently, wrote an overly broad regulation in Brussels II when they adopted the country-of-destination approach.\(^{113}\) First, the concept that a contract entered into via an interactive web site qualifies as having been "directed" towards a consumer is flawed. Cordera uses the example of a German consumer responding to an advertisement placed by a French seller in a German newspaper.\(^{114}\) Under Brussels I, article 15 would apply. However, if the advertisement were placed in an international newspaper like the *Financial Times*, the special consumer transaction rules would not apply.\(^{115}\) One could make the argument that placing a web site on the internet is more analogous to placing an advertisement in the *Financial Times* than in a German newspaper.\(^{116}\) Second, not all consumer contracts entered interactively are *directed* at those consumers completing such contracts. Consumers could click through various links to reach a foreign web site and complete a contract that would qualify for special consumer protection under Brussels II, but it could not be said that the foreign web site owner directed any of his activities towards those consumers.\(^{117}\) A consumer has greater capability to determine the seller's location than a seller has to determine the consumer's location.\(^{118}\) As a result, the consumer

\(^{112}\) See Benoit De Nayer, *The Consumer in Electronic Commerce: Beyond Confidence*, in CONSUMER L. INFO. SOC., 117, 121 (Thomas Wilhelmsson et al. eds., 2001) (arguing that the latter consumer also deserves protection because by being invited to click through various web links, he has lost any initiative in the buying process).

\(^{113}\) Cordera, *supra* note 75, at 249.

\(^{114}\) *Id.*

\(^{115}\) *Id.*

\(^{116}\) *Id.*

\(^{117}\) *Id.* at 250.

\(^{118}\) See Council and Parliament Directive 97/7, art. 4, 1997 O.J. (L 144) 19, 22
should carry the risk of being subject to foreign jurisdiction since he is more likely to be aware that he is availing himself of goods/services provided by a foreign web site than the web site owner to be aware that the consumer resides in a foreign member state.

It is assumed that mere accessibility to a web site in another member state is not enough to mean the web site is directing its activities towards another member state. However, other seemingly harmless actions can mean this. According to the Consumer & Competition Policy Directorate in the United Kingdom ("U.K."), advertising in magazines meant for all EU member states, offering a choice of languages on the web site, or giving prices in Euros can all serve as indicators that a web site was directing its activities to another member state.\footnote{\textit{Cross Border Consumer Contractual Disputes within the European Union: Which Country Has Jurisdiction?} – Frequently Asked Questions, U.K. Dep’t of Trade and Industry Web site, \textit{at} http://www.consumer.gov.uk/ccp/topics1/guide/jurisdiction_faq.htm (last visited Mar. 2, 2004).} Furthermore, providing in the contract’s Terms and Conditions that the goods/services on the web site are not meant for purchase outside the U.K., for example, is not enough to protect a seller from being subject to litigation in a foreign consumer’s forum state.\footnote{\textit{Id.}}

Ultimately, the country-of-destination approach embraced in all consumer contracts taking place through interactive web sites is overly broad and an unfair burden on sellers.

\textit{4.2.2. Hampering of E-Commerce}

There is significant criticism of the country-of-destination approach adopted in Brussels I and the draft proposal of Rome II. Because this approach subjects sellers to increased litigation costs, sellers may be tempted to pass these costs on to consumers by way of higher prices. Sellers may also choose to decrease the number of choices available to consumers by limiting the use of their web sites to certain consumers through closed computer systems, or by simply shutting down their web presence. For an example of increased litigation harassment, in Germany, consumer protection groups such as the Federation of German Consumer Organizations ("VB") surf the web to see which web sites are not in compliance

\textit{(requiring the seller provide the consumer with the identity of the seller and other contract information).}
with the new laws that regulate distance sales. Then, VB sues the
web site companies for failing to meticulously comply with
regulations in which the web site owners are not well-versed.\textsuperscript{121} It
does not even matter if the web site \textit{does not sell} anything.\textsuperscript{122}

In Spain, the government recently decided to require all
Spanish-based web sites engaged in commerce to register with the
government in the name of consumer protection.\textsuperscript{123} As a result,
more than 300 web site owners have taken their pages offline.\textsuperscript{124}
Some have merely suspended their web presence temporarily in
protest, but others have left for good.\textsuperscript{125} As Georgeos Diaz-
Montexano, the owner of a web site providing an online course in
Egyptian hieroglyphics, says, "With this law, as always, it's the
little guy that gets hurt."\textsuperscript{126} The International Chamber of
Commerce in response to the Spanish law published a statement
remarking that "\textit{[e]xcessive domestic regulation of internet content}
creates significant uncertainties for business operating in this
global medium, and has a chilling effect on commercial
communication."\textsuperscript{127}

The EU approach significantly affects small- and mid-sized
companies which may view the internet as the perfect medium to
grow their businesses. Large conglomerates that operate
throughout the EU or on a global basis can more easily afford legal
expertise to avoid the various legal pitfalls involved with a
worldwide practice. Small- and mid-sized companies do not have
that same luxury and may choose to shut down their web sites in
light of the potential for increased litigation where the cost of even
one lawsuit in a foreign jurisdiction may cause them to go out of
business. Ironically, a measure meant to promote consumer

\textsuperscript{121} See Thomas Schmitt, \textit{Internet Retailers Feel Brunt of New Law}, FRANKFURTER
ALLGEMEINE ZEITUNG, Jan. 10, 2003 (describing how consumer groups are taking
active measures to ensure web site owners comply with new regulations), \textit{at}
http://www.faz.com/in/intemplates/efaz/archive.asp?rub={F040FFD3-897B-
46DF-9603-752DD6405389}&doc={978682B0-061B-4E82-BF1D-E1985EA42554}.

\textsuperscript{122} Id.

\textsuperscript{123} See ICC, \textit{New Spanish Internet Law Will Stymie E-Commerce}, Nov. 22, 2002
(arguing that the Spanish law inhibits e-commerce growth), \textit{at}

\textsuperscript{124} Associated Press, \textit{Spanish Net Law Sparks Protests}, Wired News, Oct. 25,

\textsuperscript{125} Id.

\textsuperscript{126} Id.

\textsuperscript{127} Astrup, \textit{supra} note 123.
confidence in internet transactions then actually reduces consumer choices.

4.3. Difficulty of a Hybrid Approach to Internet Jurisdiction

While the United States and EU have adopted different approaches in determining jurisdiction over consumer internet transactions, the largest obstacle concerns trans-Atlantic, or global transactions. If a French consumer purchases a product from an American web site or vice versa, where should a dispute be heard? The obvious solution is for the United States and the EU to cooperate and develop an international framework to follow. The first issue is whether disparate substantive laws between the United States and the EU can be forged into an international framework. The second issue is whether two fundamentally different approaches towards governing the internet and e-commerce development can be reconciled to reach consensus.¹²⁸

4.3.1. Risk of an International Regime

Three cases involving Yahoo! Incorporated ("Yahoo!"), a search engine and auction web site, Dow Jones, a publisher, and Kazaa, a music-sharing company, demonstrate the risks posed by the creation of an international framework.

In 2000, a French court required Yahoo!, a U.S. company, to remove Nazi memorabilia from its auction web site because it violated French criminal law which barred the public display of Nazi-related materials in France.¹²⁹ This decision ignored Yahoo!'s claim that the French court had no jurisdiction because Yahoo!'s servers housing its web site were located in the United States.¹³⁰ Yahoo! subsequently counter-sued in the United States,¹³¹ claiming that the French judgment was unenforceable because obeying the French order would violate free speech guaranteed by the First Amendment.¹³² The Northern District of California granted a

¹²⁸ See FRANDA, supra note 65, at 83 (demonstrating how the United States is content to let the private sector play a leading role in developing e-commerce, whereas the EU prefers to regulate such development).
¹³⁰ Id.
¹³¹ Id.
¹³² U.S. CONST. amend. I.
motion for summary judgment in favor of Yahoo!. However, civil liability was not the only penalty for Yahoo!. Yahoo!’s former executive, Timothy Koogle, was prosecuted for criminal violations in France, as well. If found guilty, France would ask the United States to extradite Koogle, which the U.S. State Department would allow only if Koogle was found to have broken a similar U.S. law, which is not the case.

The U.S. protection of free speech guaranteed by the First Amendment is much more liberal than many European nations allow within their own countries. If an international framework adopts the substantive law of a nation like France, U.S. companies could be subject to similar foreign liabilities, whereas if an international framework adopts American law, companies could directly contravene European laws.

While an international framework is easy to pontificate, the reality of creating laws that both the United States and EU can live by is much more difficult. There is evidence of resentment in foreign courts about American hegemony and dominance and adherence to U.S. law which ought to worry U.S. companies with an internet presence. Last December in Dow Jones v. Gutnick, the


134 See French Prosecutor Argues for No Sentence for Former Yahoo! Boss on Trial, Jan. 8, 2003 (reporting that Koogle risked a possible fine of 46,000 euros and five years’ imprisonment if found guilty), available at http://sg.news.yahoo.com/030107/1/36ajx.html.

135 Id. But the situation may be different if Koogle were to travel to France for any reason, including vacation, whereupon France could claim personal jurisdiction and arrest him.

136 Quoting an amicus curiae brief filed by several public interest groups,

If French law can be enforced here, Yahoo could likewise be required to block access to information that ‘sabotages national unity’ in China, undermines ‘religious harmony and public morals’ in Singapore, offends ‘the social, cultural, political, media, economic and religious values’ of Saudi Arabia, fosters ‘pro-Israeli speech’ in Syria, facilitates viewing unrated or inappropriately rated Web sites in Australia, or makes available information ‘offensive to public morality’ in Italy . . .”

High Court of Australia ruled that an Australian plaintiff could bring suit in Australia against Dow Jones, a U.S.-based publisher who allegedly posted defamatory statements on the web.\textsuperscript{137} The Court held that an internet article is "published" wherever it is read, instead of adopting the United States "single publication" rule that says an internet article is published only once at a particular time and place.\textsuperscript{138} This case signals the willingness of foreign courts to apply local standards to cases involving American parties when it is believed that the harm suffered in the dispute is local.\textsuperscript{139} Given that U.S. companies dominate the e-commerce canvas, the trend to ignore American law and principles can negatively impact e-commerce's growth should these companies deign to go offline.\textsuperscript{140}

\textsuperscript{138} Id.
\textsuperscript{139} Quoting David R. Johnson of Wilmer, Cutler & Pickering,

[The Australian High Court] did show some recognition of the fact that in some sense that either American law was going to be imposed on Australia or Australian law was going to imposed on the U.S. It's an important case in part because there is an inescapable tension between the jurisdictions and there is no global supremacy clause to solve that.


Andrew Meldrum, an American reporter, was prosecuted this year by Robert Mugabe's repressive government in Zimbabwe for 'publishing a falsehood' in an article published on the web site of the Guardian. . . . It is the possibility of global liability, in both criminal and defamation law, which now worries big media companies.


\textsuperscript{140} [T]he ruling has thrown internet publishers into disarray and left them facing a choice between two equally costly and undesirable options: restricting access to their web sites to prevent people in potentially difficult legal jurisdictions reading them; or employing international legal teams to vet all content to ensure that it complies with the libel laws in each of the countries it is likely to be read.

However, U.S. companies are not the only ones that have reason to be concerned with the risks of an international legal system. In a recent decision, U.S. District Judge Stephen Wilson held that a lawsuit could proceed against Sharman Networks, the parent company of Kazaa,\textsuperscript{141} despite Sharman being headquartered in Australia and incorporated in the Pacific Island nation of Vanuatu.\textsuperscript{142} While Sharman expanded its commercial activities and advertising within the Kazaa program, it backed away from a plan to offer a paid subscription service as many of the potential subscribers would have been U.S. residents.\textsuperscript{143} That move failed to protect it from liability in the United States since the Court found that the number of Kazaa users in the United States satisfied minimum contact to justify the Court's exercise of personal jurisdiction against Sharman.\textsuperscript{144}

The risk accompanying the creation of an international legal framework to determine jurisdiction is that the law adopted in that framework may be less advantageous than a company's current forum state. While predictability may be of some comfort to companies, one could also argue that the lack of uniformity currently protects companies from exploding global liability.

\textit{4.3.2. Different Ideological Stances between the United States and EU}

Assuming that a common legal framework is desired, it is still extremely difficult for the United States and the EU to come to an agreement as to how that framework should be and what that framework should look like. An example of this predicament is the proposal to revise the Hague Convention.\textsuperscript{145} The proposed Hague Convention on Jurisdiction and Foreign Judgments was first proposed in 1992 and, if passed, would be significant because there are potentially fifty signatory countries ranging from China to the United States and the EU.\textsuperscript{146} The private sector has raised

\textsuperscript{141} Kazaa is a popular online file-swapping software service.


\textsuperscript{144} \textit{Id.}

\textsuperscript{145} Hague Convention Draft Revision, \textit{supra} note 7.

\textsuperscript{146} \textit{See Risks to an E-Business of Being Sued Abroad Under Foreign Law} (giving a "brief overview of what currently determines when a foreign court will accept
several concerns that the Draft Proposal of the Hague Convention would impede the growth of e-commerce.\textsuperscript{147} While the U.S. delegation originally initiated the impetus for a revision of the Hague Convention in order to allow individuals who won judgments in American courts to enforce them in Europe, as the global impact of e-commerce has expanded, it has quickly backpedaled and tried to limit the scope of the revision.\textsuperscript{148} Currently, the delegations have scaled back the scope of the Hague Convention by limiting it to B2B transactions,\textsuperscript{149} but there is no guarantee that any final revision will pass.

5. BUSINESS STRATEGIES TO AVOID JURISDICTIONAL DISPUTES

There are several strategies e-businesses can employ in an attempt to either limit or avoid foreign liability. A company could write into its Terms and Conditions of the contract that a good/service is only intended for sale in certain countries or both the consumer and seller could agree to a forum selection clause.\textsuperscript{150} However, Terms and Conditions may not allow a seller to avoid EU regulations, such as Brussels I.\textsuperscript{151} In a twist of irony, however, U.S. state laws that have restricted the reach of out-of-state internet web sites by prohibiting shipments of wine from such internet retailers are now being found unconstitutional and in violation of the U.S. Constitution’s Commerce Clause.\textsuperscript{152} So while it is clear that individual retailers can restrict the reach of their business, governments cannot.\textsuperscript{153}

\textsuperscript{147} Haines, supra note 86, at 6.
\textsuperscript{150} Frascogna, Jr. et al., supra note 1, at 150-51.
\textsuperscript{151} Cross Border Consumer Contractual Disputes, supra note 19.
\textsuperscript{152} U.S. Const. art. I, § 8, cl. 3.
regulatory arbitrage that "involves exploiting differing rules in different jurisdiction—for a profit."\textsuperscript{154} For a fee, regulatory arbitrage companies will determine where a company should incorporate, headquarter, and store its server and data to best take advantage of different rules and regulations in various jurisdictions. There has been no conclusion on whether this is effective, though wealthy individuals have taken advantage of offshore jurisdictions for decades.

If a company knows what material on its web site is offensive in another jurisdiction (e.g., Yahoo! and France), it can employ filtering technology to search for and block out key words or phrases.\textsuperscript{155} In the Yahoo! case, filtering technology could block out words related to Nazi memorabilia such as "Nazi," "Third Reich," or "Hitler." The problem with filtering is that it is imperfect. Too much information travels on the internet\textsuperscript{156} and to search all of it is time consuming. In the example provided, a more creative search could still turn up Nazi memorabilia prohibited in France if one used the words "Aryan" or "supremacy." A company could also simply delete the material that foreign governments find offensive, as Google.com, a search engine, has been doing from its French and German domains (google.fr and google.de).\textsuperscript{157} The long-term effect of this could be significantly detrimental and, taken to an extreme, the internet could become the most censored publication in the world.

Technology that can be employed to restrict web site use to specific consumers is called "blocking." Blocking is software that either grants or denies a user access based upon its IP address. For example, Yahoo! dropped access to its auction sites in Britain, France, Germany, Italy, Ireland and Spain rather than appeal the


\textsuperscript{155} But see Am. Library Ass'n v. United States, 201 F. Supp. 2d 401, 405 (E.D. Pa. 2002) (ruling that the Children's Internet Protection Act requiring public libraries to install filtering programs that prevent minors from accessing information on the internet harmful to minors is unconstitutional).


\textsuperscript{157} See Declan McCullagh, Google Excluding Controversial Sites, CNET NEWS.COM, Oct. 23, 2002 (reporting that Google has been deleting web sites from its German and French domains, google.de and google.fr, when it receives specific complaints from foreign governments), at http://news.com.com/2100-1023-963132.html.
French judgment.\textsuperscript{158} The unfortunate effect of this is that consumer choices become limited. For example, as a result of the \textit{Dow Jones v. Gutnicken} case, "many U.S. websites [will block] access to non-American readers, destroying a rich resource for the rest of the world."\textsuperscript{159}

The most drastic strategy to employ is to simply go offline altogether. This move is most detrimental to small- and mid-sized businesses. These businesses rely upon the internet to grow their sales volume and increase their market share. Unfortunately, one lawsuit or a drawn-out litigation dispute could easily bankrupt these businesses, as well. For business owners who refuse to "bet the company" on this possibility, avoiding a presence on the internet is the easiest way to avoid any potential liability from foreign jurisdictions. However, the profits from putting a company online may outweigh the increased risk of being sued,\textsuperscript{160} so while going offline is absolute protection from foreign liability, it could be detrimental to the growth of the business.

6. CONCLUSION

The technological composition of the internet and its decentralized nature makes it extremely difficult to establish clear rules on jurisdiction or even determining the domicile of a party. The U.S. approach towards jurisdiction has been piecemeal, focusing on the Zippo sliding scale of interactivity and the effects-based test, while the EU approach has been regulatory, embracing the country-of-destination approach that seems to favor consumers. Neither approach is particularly satisfying to companies with a web presence, but then, formulating an integrated framework is equally, if not more, difficult, as proven by the lack of agreement on the Hague Convention. There are various contractual, entrepreneurial and technological strategies that can

\textsuperscript{158} See French Prosecutor Argues for No Sentence for Former Yahoo! Boss on Trial, Jan. 8, 2003 (reporting that Koogle risked a possible fine of 46,000 euros and five years' imprisonment if found guilty), at http://sg.news.yahoo.com/030107/1/36ajx.html.

\textsuperscript{159} See Fickling & Miller, \textit{supra} note 140, (quoting Ian Brown, director of the London-based internet think tank, the Foundation for Information Policy Research).

be employed to limit or avoid legal liability from foreign jurisdictions, but aside from taking a business offline, there is no absolute avoidance of increased legal liability. Companies may, as a result of foreign courts being more willing to assert jurisdiction over international non-residents, choose to simply deny access to their web site to internet users not located in their local jurisdiction as best technology can detect. Ironically enough, this may mean that the internet will be as bordered as traditional geographic boundaries are today.