
Harmonizing Cybertort Law for Europe and America

Michael L. Rustad¹ & Thomas H. Koenig²

Cite as: 5 J. High Tech. L. 13 (2005)

Abstract

In this Article, Michael L. Rustad & Thomas H. Koenig call for a globalized regime of Internet torts to protect consumers and other travelers in cyberspace. Part I of this Article lays out the procedural barriers to the development of cybertorts, focusing on the divergent paths of the law taken by the United States and its European trading partners. The United States follows a standards-driven minimum contacts regime while Europe has adopted the Brussels Regulation, which promulgated bright-line rules. The U.S. adopted a market-driven approach to choice of forum and law, whereas Europe provides mandatory protections for consumers. Part II examines differences in substantive tort law between the United States and Europe. Cybertort cases, especially for the law of defamation, privacy, and anti-spam initiatives, will result in different outcomes in Europe than in the United States because of differences in doctrine. Part III proposes a globalized regime that draws upon the salient features of European and American procedural and substantive tort law. On the procedural side of the law, the authors favor adopting the bright-line rules of the Brussels Regulation, which provides consumers with the right to file suit against Internet service providers and other online intermediaries in their home court. The American market-driven approach has left injured consumers without meaningful remedies in cyberspace. On the substantive side of cybertort law, European consumers and businesses would benefit from the American system of private enforcement through tort law.

1. Thomas F. Lambert, Jr., Professor of Law and Co-Director of Intellectual Property Law Concentration, Suffolk University Law School in Boston; LL. M., Harvard University Law School; J.D., Suffolk University Law School; Ph.D., Boston College, M.A., University of Maryland, B.A., University of North Dakota.

2. Chair of the Department of Sociology and Anthropology and Professor in the Law, Policy and Society doctoral program, Northeastern University; Ph.D., University of California, Santa Barbara; B.A., University of California, Santa Cruz.

INTRODUCTION

PART I. CAUGHT IN THE NET: PROCEDURAL BARRIERS TO CYBERLAW DEVELOPMENT

- [A] Cyber-Jurisdictional Clashes Between the U.S. & Europe
- [B] Europe's Harmonized Jurisdictional Regime
- [C] Rome II's Convention on Choice of Law for Torts
- [D] Choice of Forum in Cyberspace

PART II: DISCORDANT CYBERTORT REGIMES: EUROPE V. AMERICA

- [A] Divergent Defamation Regimes
- [B] Conflicting Internet Privacy Regimes
- [C] Deviating Anti-Spam Regimes
- [D] Conflicting Online Intermediary Law

PART III: TOWARDS A HARMONIZED CYBERTORT REGIME

- [A] Doing Nothing Is Not a Realistic Option
- [B] Eliminating Procedural Barriers for Cybertort Adjudication
- [C] Harmonizing Substantive Cybertort Law

CONCLUSION

INTRODUCTION

Cyberspace is the fastest growing free-trade zone. Internet trade is multi-hemispheric, as the sun never sets on a Web site that stands ready to communicate with customers 24 hours a day, seven days a week in all countries connected to the World Wide Web. Online contracts were estimated to total \$71 billion in 2004.³ By March of 2005, there were approximately 138 million Internet users in the United States⁴ and an estimated 888.7 million users around the world.⁵ Worldwide Internet business-to-business transactions⁶ are expected to total \$6 trillion in 2005.⁷

The Internet's blurring of national boundaries creates a variety of new cybertort dilemmas. The global Internet's legal environment makes it inevitable that "one country's laws will conflict with another's—particularly when a Web surfer in one country accesses content hosted or created in another country."⁸ National differences among the cybertort regimes of different countries connected to the Internet will inevitably lead to conflicts of law.⁹ "Which court will

3. E-Commerce & Internet Business Statistics, at http://www.plunkettresearch.com/technology/ecommerce_statistics_1.htm (last visited April 12, 2005) (estimating Internet usage as of March 24, 2005).

4. *Id.*

5. World Internet Usage & Population Statistics, at <http://www.internetworldstats.com/stats.htm> (last visited April 15, 2005) (reporting current world Internet user population as an estimated 888,681,131).

6. B2B is business to business e-commerce and it means exactly what it says: businesses selling to other businesses; factories selling to wholesalers; wholesalers selling to retailers; office suppliers selling to offices; farmers selling to markets; etc. Any deal between two businesses is B2B e-commerce. Dr. Ecommerce, *Frequently Asked Questions* at <http://www.jpb.com/drecommerce/faq.html> (visited April 12, 2005).

7. Gartner Group, *Worldwide Business-to-Business Internet Commerce to Reach \$8.5 Trillion in 2005*, at <http://www4.gartner.com/5abpit/pressroom/pr20010313a.html> (last visited Feb. 3, 2005).

8. Peter Yu, *Conflict of Laws in International Copyright Cases*, at <http://www.gigalaw.com/articles/2001/2001-04.html> (last visited April 15, 2005); *See also*, Julia Lapis, *The Internet Tort Dilemma*, IT LAW TODAY 1 (Feb. 2002) (commenting that "many countries' legal systems have struggled with the issue of personal jurisdiction and the question of whether a court can legitimately exercise jurisdiction over an individual or company with no physical presence in the judicial forum, but whose web site can be accessed from the forum state.").

9. The conflicting standards between U.S. and United Kingdom defamation law in Internet cases is illustrated by "the 1997 U.S. Court of Appeals case of *Zeran v. America Online, Inc.*, [in which] the plaintiff sued the defendant internet service provider ("ISP") for unreasonable delay in removing defamatory messages posted by an unidentified third party, refusing to post retractions, and failing to screen for similar postings thereafter. The Court held that the Communications Decency Act barred such claims by immunizing commercial interactive computer

seize the case is one issue; but which law will be applied is another. We're in Marshall McLuhan's 'Global Village' and we're inventing the roadmap."¹⁰

Yahoo!, for example, hosts auction sites, message boards, and chat rooms primarily for U.S. users.¹¹ A Paris court ruled that messages about Nazis and the sale of Third-Reich memorabilia violated the French Criminal Code.¹² Even though Yahoo!'s French subsidiary removed Nazi-related material and images, French users could still access this material by using the American Yahoo! Web site.¹³ The court issued an order, fining Yahoo! 100,000 Francs per day until they removed "all Nazi-related messages, images, and text stored on its server, particularly any Nazi relics, objects, insignia, emblems, and flags on its auction site."¹⁴ Yahoo! refused to honor the French court's order, filing a complaint in the Northern District of California, requesting a declaration that the French court's order was unenforceable since it was in conflict with the First Amendment of the U.S. Constitution.¹⁵

In *Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*,¹⁶ the California federal court refused to enforce the French order requiring the American Web site to remove Nazi-related materials. The U.S. federal court ruled that the judgment violated

service providers from liability for defamatory information posted by third parties. In contrast to the American approach, an ISP in the 1999 English High Court case of *Godfrey v. Demon Internet Ltd.* was found liable for defamation after failing to remove defamatory remarks in a posting to a Newsgroup forum following a request to do so by the plaintiff who was alleged to have been the author of the posting. The comments in the posting were obscene and smeared the plaintiff's reputation. He therefore requested their removal but the defendant company failed to do so. The High Court concluded that, since the defendant company knew about the defamatory content of the posting, they could not avail themselves of the protection of s. 1(1) of the English Defamation Act 1996." David F. Sutherland, *Defamation on the Internet*, at <http://www.adidem.org/articles/DS5.html> (last visited April 15, 2005). Similar conflicts will likely surface in regulating speech on the Internet, intellectual property, the formation of electronic contracts, as well as Internet taxation, telemedicine and the delivery of online professional services.

10. *Id.*

11. *Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme*, 379 F.3d 1120, 1122 (9th Cir. 2004).

12. *Id.*

13. *Id.*

14. *Id.*

15. *Id.* at 1123 (stating that "[t]he French court's determination that Yahoo! was in violation of French law may not be reviewed by any U.S. court. Yahoo!, however, contends that enforcement of the French court's judgment in the United States would violate Yahoo!'s First Amendment rights).

16. 169 F. Supp. 2d 1181 (N.D. Cal. 2001).

U.S. public policy that was protected by the First Amendment.¹⁷ The Ninth Circuit reversed the federal district court's declaratory judgment ruling that the court had no personal jurisdiction over the French authorities.¹⁸ A French criminal court "plans to try Yahoo and Timothy Koogle, its former CEO, for allowing Nazi memorabilia to be sold on the Yahoo! auction site."¹⁹

Regulators in European countries have legitimate reasons to institute culturally specific regulations of Web site content. The Nazi occupation of Western Europe during World War II resulted in French laws against the expression of pro-Nazi and anti-Semitic views. In the United States, the First Amendment prohibits the government from restraining political expression, no matter how distasteful. The French court's attempt to impose local rules on world wide information transmissions is analogous to treating the cross-border legal environment as a local ordinance.²⁰ While "there is no doubt that France may and will continue to ban the purchase and possession within its borders of Nazi and Third Reich related matter and to seek criminal sanctions against those who violate the law,"²¹ it is unclear how this salutary principle applies to communications going beyond its borders.

The Yahoo! case raises knotty issues of which governing authority determines what nation-state's criminal code, law of torts, and content regulations apply when information crosses hundreds of borders. Traditional concepts of jurisdiction and enforcement of judgment need to be adapted to the Internet. Transnational cybertorts have yet to address cross-border Internet tort injuries such as the

17. *Id.* at 1184.

18. *Id.* at 1127 (reversing the district court's ruling because the French authorities "LICRA and UEJF took action to enforce their legal rights under French law. Yahoo! makes no allegation that could lead a court to conclude that there was anything wrongful in the organizations' conduct. As a result, the District Court did not properly exercise personal jurisdiction over LICRA and UEJF. Because the District Court had no personal jurisdiction over the French parties, we do not review whether Yahoo!'s action for declaratory relief was ripe for adjudication or whether the District Court properly refused to abstain from hearing this case.").

19. Perkins Coie, Internet Case Digest, *France v. Yahoo, Inc.; Timothy Koogle, at* http://www.perkinscoie.com/casedigest/icd_results.cfm?keyword1=international&topic=International (last visited Feb. 10, 2005).

20. James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty and Hardwired Censors*, 66 U. CIN. L. REV. 177, 179 (1997) (quoting John Perry Barlow that "In Cyberspace, the First Amendment is a local ordinance."); See generally, David R Johnson and David Post, *Law and Borders-The Rise of Law in Cyberspace* 48 STAN. L. REV. (1996).

21. *Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*, 169 F. Supp. 2d 1181, 1186 (N.D. Calif. 2001).

invasion of privacy, computer hacking, releasing viruses²² or worms,²³ denial of service attacks, and other vulnerabilities unknown before the Internet. No comprehensive treaty or convention sets the ground rules for cybertort causes of action, Internet remedies, or the means for obtaining jurisdiction or the enforcement of judgments.

This Article examines barriers to the development of Internet torts. Part I explores the procedural hurdles to the development of a harmonized cybertort regime that will protect European and American consumers and businesses in their online activities. On the procedural side of cybertort law, issues of cross-border jurisdiction, enforcement, conflict of law, choice of forum, and differences in substantive law between Europe and America are the thorniest dilemmas impeding the further legalization of cyberspace.

Part II describes the divergent paths taken by the United States and Europe when it comes to civil wrongs. The American law of torts is based upon the common law, whereas the European law of torts, or *delict*,²⁴ is really a residual category of noncontractual relations.²⁵ The European Commission is seeking to replace the twenty-five national systems of conflicting rules with a “single set of uniform rules, which would represent considerable progress for economic operators and the general public in terms of certainty as to the law.”²⁶

Part III develops the case for increased harmonization of Internet

22. Bradley S. Davis, Note, *It's Virus Season Again, Has Your Computer Been Vaccinated? A Survey of Computer Crime Legislation As A Response To Malevolent Software*, 72 WASH. U. L. Q. 411 (2001) (describing case in which malevolent software was introduced into a company computer by an ex-employee who gained access by using his revoked password and security clearance).

23. On January 25, 2003, a virus-like attack on vulnerable computers on the Internet exploited a known flaw in popular database software from Microsoft Corp. called “SQL Server 2000.” Ted Bridis, *Virus-Like Attack Slows Web Traffic*, Associated Press, Jan. 25, 2003. “Within a few hours, the world's digital pipelines were overwhelmed, slowing down Web browsing and e-mail delivery. Monitors reported detecting at least 39,000 infected computers, which transmitted floods of spurious signals that disrupted the operations of hundreds of thousands of other systems.” *Id.*

24. Civil Code jurisdictions treat tort-like actions as delicts, a concept borrowed from Roman law. Jack Beatson, *Obituary of Peter Birks: Brilliant and Prolific Academic Lawyer Who Brought the Law of Restitution Up to Date*, THE GUARDIAN (LONDON), July 16, 2004, at 31. The law of delict is simply redressing civil wrongs by compensation. *Id.*

25. “In Europe, [c]ommon rules applicable to non-contractual obligations arising out of a tort or delict and out of an act other than a tort or delict.” Commission of the European Communities, Opinion of the European Economic and Social Committee on the Proposal for a Regulation of the European Parliament and the Council on the law applicable to non-contractual obligations (COM (2003) 427 final - 2003/0168 (COD)), 2004 OJ C 241 (June 2, 2004) (Official Journal C 241, 28/09/2004 P. 0001 – 0007) [hereinafter Rome II].

26. *Id.* (discussing Article 1 of Rome II Convention).

torts between the U.S. and Europe so that there can be greater accountability for cybertortfeasors and other creepy crawlers on the World Wide Web. While Europe moves towards harmonization of cyberlaw through the promulgation of community-wide regulations and directives, the United States has embarked upon a separate, solitary path. America's unilateral assertion of sovereignty in cyberspace is unworkable in a networked world that contains radically different legal, cultural, and economic legal traditions.

PART I: CAUGHT IN THE NET: BARRIERS TO CYBERTORT DEVELOPMENT

[A] Cyber-Jurisdictional Clashes Between the U.S. & Europe

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

Judge Nancy Gertner²⁷

An Internet presence automatically creates an international presence, triggering the potential for cross-border litigation. "When the defendant's alleged contact with the forum state occurs via the Internet, the plaintiff faces an initial hurdle in showing *where* this Internet conduct took place for jurisdictional purposes."²⁸ A growing number of U.S. courts are exercising jurisdiction over Web site activity occurring outside of the country's territorial boundaries. Conversely, U.S. companies are increasingly being sued in foreign venues for activities occurring on Web servers located in the United States. Clearly, global tort law requires harmonization. Presently, almost no case law covers international Internet jurisdiction, and no statutory solutions exist to answer the question of cross-border Internet jurisdiction.²⁹ It is theoretically possible for a U.S. business

27. *Digital Equip. Corp. v. AltaVista Tech., Inc.*, 960 F. Supp. 456, 462 (D. Mass. 1997) (J. Gertner).

28. *Cadle Co. v. Schlichtmann*, 2005 U.S. App. LEXIS 2097 (6th Cir. Feb. 8, 2005).

29. Agne Lindberg, *Jurisdiction on the Internet-The European Perspective: An Analysis of Conventions, Statutes, and Case Law*, ABA Committee on Cyberspace Law (May 24, 2000), at

<http://www.abanet.org/buslaw/cyber/initiatives/eujuris.html> (last visited Mar. 31 2005); see also, David W. Maher, *Trademark Law on the Internet—Will it Scale? The Challenge to Develop International Trademark Law*, 16 J. MARSHALL J. COMPUTER & INFO. L. 3 (1997) (arguing for a harmonized regime for trademarks on the Internet); Graeme B. Dinwoodie, *A New Copyright Order: Why National*

to be sued in hundreds of forums in foreign countries for the same course of online conduct, but this has not yet happened due to the barriers to filing cross-border lawsuits that will be explored in this Article. As businesses use the border-defying Internet, they will increasingly become subject to conflicting procedural and substantive law.

The Internet raises unique jurisdictional issues because this new technology respects no national borders. The Internet is a new realm without a sovereign and no international treaty or convention sets the rules governing Internet jurisdiction.³⁰ Cyberspace raises inevitable jurisdictional issues because, by its very definition, the Internet involves transborder communications across hundreds of countries at the click of a mouse.

No remedy for a cybertort may be developed unless jurisdiction can be established over the defendant. In *English Sports Betting, Inc. v. Tostigan*,³¹ for example, a defendant in New York posted a defamatory statement about the English plaintiff, accusing him of committing murder.³² English Sports Betting and its owner, Atiyeh, filed defamation lawsuits “against Tostigan and the operators of two Web sites - www.playersodds.com and www.theprescription.com - that posted the articles on their sites.”³³ In that case the plaintiff Atiyeh was a citizen of Pennsylvania and owner of English Sports Betting, Inc., which was a Jamaican corporation.³⁴ One of the defendants filed a motion to dismiss for lack of personal jurisdiction contending that it lacked minimum contacts with Pennsylvania.³⁵ The

Courts Should Create Global Norms, 149 U. PENN. L. REV. 469 (2000) (arguing for globalized copyright law for the Internet).

30. “For a long time, the Internet's enthusiasts have believed that it would be largely immune from state regulation. The theory was not so much that nation states would not want to regulate the Internet, it was that they would be unable to do so, forestalled by the technology of the medium, the geographical distribution of its users, and the nature of its content.” James Boyle, *Focault in Cyberspace: Surveillance, Sovereignty and Hardwired Censors*, 66 U. CIN. L. REV. 177, 178 (1997).

31. C.A. No. 01-2202 (E.D. Pa. 2002) (summarized in Perkins Coie Internet Law Digest International), at http://www.perkinscoie.com/casedigest/icd_results.cfm?keyword1=international&topic=International (last visited Feb. 8, 2005).

32. *Id.*

33. Edward T. Rogers, *All Bets Off in Libel Suit Against Web Site Operator Offshore Gambling Article*, 226 LEGAL INTELLIGENCER (June 13, 2002) at 7.

34. “Dennis Atiyeh, who owns a Jamaican-based and Jamaican-incorporated gambling enterprise known as English Sports Betting. Atiyeh claimed that he and English Sports Betting were defamed in an article written by defendant Christopher “Sting” Tostigan reporting on Atiyeh's allegedly criminal activities.” *Id.*

35. *Id.*

court granted the defendant's motion to dismiss for lack of personal jurisdiction, contending that it lacked the necessary minimum contacts with Pennsylvania because the Web site did not conduct business, sell advertising, or own property in Pennsylvania.³⁶ The court reasoned "that Pennsylvania was not the 'focal point of the tortious conduct'" because the articles were "targeted at the international off-shore gambling community."³⁷

The court's dismissal of the action in the *Tostigan* case reflects the failure of the minimum contacts framework in determining "place" in cyberspace.³⁸ Foreign defendants are entitled to due process in American courts, but new standards are required to deal with the irrelevance of traditional tests such as the location of the principal place of business for establishing jurisdictions.³⁹

On the civil side of personal jurisdiction law, courts accord due process to foreign defendants whereas American litigants may not have parallel protections when being sued outside the United States.⁴⁰

36. *Id.*

37. *Id.*

38. *International Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945). Courts have applied the "effects test" in *Panavision International, L.P. v. Toeppen*, 938 F. Supp. 616, 621 (C.D. Cal. 1996). In general, courts use the "sliding scale test of *Zippo Manufacturing Co. v. Zippo Dot.Com, Inc.* 952 F. Supp. 1119 (W.D. 1997) to determining whether jurisdiction exists for Web site activities." However, "[t]he unique nature of the Internet highlights the likelihood that a single actor might be subject to haphazard, uncoordinated, and even outright inconsistent states that the actor never intended to reach and possibly was unaware were being accessed. Typically, states' jurisdictional limits are related to geography; geography, however, is a virtually meaningless construction on the Internet." *American Libraries Ass'n v. Pataki*, 969 F. Supp. 169, 164-67 (S.D.N.Y. 1997). *See also McDonough v Fallon McElligott, Inc.* 40 USPQ 2d (BNA) 1826, 1829 (SD Cal 1996) (stating "[B]ecause the Web enables easy world-wide access, allowing computer interaction via the web to supply sufficient contacts to establish jurisdiction would eviscerate the personal jurisdiction requirement as it currently exists").

39. *See In re Manetic Audiotape Antitrust Litigation*, 171 F. Supp. 179 (S.D. N.Y. 2001) (holding that foreign company's passive Web site did not support a finding of minimum contacts permitting jurisdiction). *Cf. Northern Light Technology, Inc. v. Northern Lights Club*, 97 F. Supp.2d 96 (D. Mass. 2000) (holding that Canadian company with Web site permitting them to combine their own name with domain names was subject to Massachusetts jurisdiction). While a court's ability to exercise personal jurisdiction is conferred by state law, the extend to which the court may exercise that authority is governed by the Due Process Clause of the Fourteenth Amendment to the Federal Constitution. *Kulko v. Superior Court of California*, 436 U.S. 84, 91 (1978).

40. The determination of whether a court has personal jurisdiction over the defendants in a cross-border case generally involves two issues: "First, does jurisdiction exist under the state long-arm statute? Second, if such jurisdiction exists, would its exercise be consistent with the limitations of the due process clause? Those two inquiries coalesce into one where the reach of the state long-arm

The American approach extends limited jurisdiction over nonresidents through the “legal fiction” of long arm statutes.⁴¹ In order to file a civil action in a U.S. court, the plaintiff must establish sufficient “minimum contacts” with the forum state so that the exercise of jurisdiction does not offend “traditional notions of fair play and substantial justice.”⁴² A British bank’s passive, informational Internet Web site was insufficient to subject the bank to general or specific jurisdiction in Utah.⁴³

In determining personal jurisdiction in cyberspace, most U.S. courts apply the sliding scale of interactivity test of *Zippo Mfg. Co. v. Zippo Dot Com.*⁴⁴ “Some cases have suggested that the availability and use of a highly interactive, transaction-oriented Web site (as opposed to an ‘essentially passive’ Web site) by itself may support long-arm jurisdiction wherever the site is available to potential customers for the purpose of doing business.”⁴⁵ In the formative years of the Internet, it made sense to base jurisdiction upon whether a Web page was passive or interactive. Other courts require factors or evidence beyond mere Internet access and interactivity to demonstrate a sufficient basis for jurisdiction.⁴⁶ American courts agree that a virtual presence alone does not subject a Web site to

statute is the same as the limits of the due process clause, so that the state limitation collapses into the due process requirement.” *Trintec Indus. v. Pedre Promotional Prods.*, 395 F.3d 1275, 1279 (6th Cir. 2005).

41. The scope of a state’s long-arm statute determines what activities that can be reached. In general, most states have broad long-arm statutes to reach as much conduct as the due process clause will allow. Prepared Testimony of D. Jean Veta, Deputy Associate Attorney General, U.S. Department of Justice, Before the House Committee on the Judiciary Subcommittee on the Courts and Intellectual Property, FEDERAL NEWS SERVICE, June 29, 2000.

42. The bellwether case of *Int’l Shoe v. Wash.*, 326 U.S. 310, 316 (1945) (articulating the minimum contacts framework followed in all U.S. jurisdictions).

43. *Soma Med. Int’l. v. Standard Chartered Bank*, 196 F.3d 1292 (10th Cir. 1999) (dismissing action by Utah account holder against British bank for breach of contract and negligence for disbursing funds upon unauthorized signature).

44. 952 F. Supp. 1119, 1124 (W.D. Pa. 1997) (formulating a sliding scale of interactivity to identify Internet activity satisfying purposeful availment test).

45. *Trintec Indus. v. Pedre Promotional Prods.*, 395 F.3d 1275, 1281 (6th Cir. 2005) (discussing *Zippo.com* reasoning in determining Internet jurisdiction); See also, *CD Solutions v. Tooker*, 965 F. Supp. 17 (N.D. Tex. 1997); *Millennium Ents. V. Millennium Music*, 33 F. Supp.2d 907 (D. Or. 1999).

46. *GTE New Media Servs. v. BellSouth Corp.*, 199 F.3d 1343, 1346 (D.C. Cir. 2000) (holding that personal jurisdiction could not be based upon “mere accessibility to an Internet site in the District” where defendants had “no other contacts with the District of Columbia”); See generally, Michael Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 16 *Berkeley Tech. L.J.* 1345, 1378-81 (2001) (questioning the effectiveness of the passive/active continuum and calling for a new technology-neutral test based upon a targeting-based model).

personal jurisdiction. Courts will dismiss Internet-related claims where the Web site is merely a “passive” advertisement permitting no interaction with the site visitor. A Web page advertisement alone was held to be an insufficient basis for jurisdiction.⁴⁷

American due process limitations on jurisdictions do not apply in foreign courts; however, functionally equivalent rules may be used. A United Kingdom Court of Appeal has ruled that a patent could be infringed in the UK even though the patented gaming system was running on offshore servers.⁴⁸ The defendant supplied its customer with a CD that allowed them to access the defendant’s gaming system operating in Antigua.⁴⁹ The UK court held that the defendant infringed the patent with this offshore system even though the servers were in Antigua, because the effects⁵⁰ of the offshore gaming system were felt in England.⁵¹

The Prince Edward Island Supreme Court ruled that a charitable lottery was illegal under Canada’s Criminal Code.⁵² Earth Future Lottery had been granted a license to operate an Internet lottery from its headquarters on Prince Edward Island. While a lottery may be legal in Prince Edward Island, an Internet lottery operating on the Web site would reach other provinces and thus violate Canada’s general laws.⁵³ The cross-border aspect of the Internet raises the question of when a country may enforce its content restrictions or other regulations over information transmitted by e-mail or Internet postings.

47. *Cybersell, Inc. v. Cybersell, Inc.*, 130 F.3d 414, 418-19 (9th Cir. 1997) (holding that Internet advertisement alone is insufficient basis for jurisdiction).

48. *Menashe Business Mercantile Ltd. v. William Hill Organization Ltd.*, [2002] EWCA Civ 1702 (United Kingdom, 2003).

49. *Id.*

50. American courts also examine the “effects” of tortious activity in determining personal jurisdiction. *See Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119, 1124 (W.D. Pa. 1997) (utilizing a “sliding scale” test for jurisdiction which considers a Web site’s level of interactivity and the nature of commercial activities conducted over the Internet). There are other courts that apply the “effects test” derived from a United States Supreme Court decision entitled *Calder v. Jones*, 465 U.S. 783 (1984) (ruling that personal jurisdiction over Florida defendants was proper in California because the foreseeable “effects” in California of the non-resident defendant’s activities); *See also Zidon v. Pickrell*, 344 F. Supp. 2d 624, 629 (2004).

51. *Menashe Business Mercantile Ltd. v. William Hill Organization Ltd.*, [2002] EWCA Civ 1702 (United Kingdom, 2003).

52. Reference Re Earth Future Lottery (P.E.I.), 2002 PESCAD 8 (Canada 2002).

53. *Id.*

[B] Europe's Harmonized Jurisdictional Regime

Europe's harmonized system of procedural and substantive law has its roots in the unifying principles of the 1957 Rome Treaty.⁵⁴ The European Union (EU) formed new legal institutions to carry out its objective of transcending national borders. The twenty-five Member States are represented on the European Council, which drafts legislation for Europe as a whole.⁵⁵ This unified approach has allowed Europe to take the lead in formulating a harmonized legal regime for the information age.⁵⁶

The European Commission is charged with developing a legal framework to advance free competition in the Single Market. The Commission has powers of initiative, implementation, management, and control, which allows it to formulate harmonized regulations.⁵⁷ In the past decade, the Commission has approved Internet regulations such as the E-Commerce Directive, E-Signatures Directive, Distance Selling Directive, Data Protection Directive, Database Protection Directive, and the Copyright Directive.⁵⁸ The European Union

54. Article 2 of the Treaty of Rome states the following principle: "The Community shall have as its task, by establishing a common market and an economic and monetary union and by implementing the common policies or activities referred to in Articles 3 and 3a, to promote throughout the Community a harmonious and balanced development of economic activities, sustainable and non inflationary growth respecting the environment, a high degree of convergence of economic performance, a high level of employment and of social protection, the raising of the standard of living and quality of life, and economic and social cohesion and solidarity among Member States." Treaty of Rome, (1957) art. 2., available at http://europa.eu.int/abc/obj/treaties/en/entr6b.htm#Article_1 (last visited Jan. 28, 2005).

55. The European Council is a key decision-making institution that is responsible for foreign affairs, farming, industry, transport, and other emergent issues. European Parliament, Institutions, *Policies & Enlargement of the European Union*, available at <http://www.europa.eu.int>.

56. The European Union is currently preparing for the accession of thirteen eastern and southern European countries, including Bulgaria, Czech Republic, Estonia, Cyprus, Latvia, Lithuania, Hungary, Malta, Poland, Romania, Slovenia, Slovakia, and Turkey. In Eastern Europe countries such as Romania and Bulgaria, computer and Internet usage rates are currently low. One of the long-term effects of accession will be a transformation in Internet usage. See Reuters, *Web A Luxury In IT Wastelands Romania, Bulgaria*, at <http://economictimes.indiatimes.com/cms.dll/xml/comp/articleshow?artid=30033789> (last visited Feb. 2, 2005).

57. *Id.*

58. Directives must be implemented by each Member State. For example, the United Kingdom's 1998 Data Protection Act implemented the EC Data Protection Directive (95/46/EC). See Council Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L281) (Nov. 23, 1995), available at <http://europa.eu.int/eur>

recognizes that e-commerce cannot flourish without revamping the legal infrastructure.⁵⁹

[1] *Brussels Regulation*

Internet jurisdiction cases in Europe follow the Brussels Regulation's⁶⁰ bright-line rules rather than standards-driven U.S. style minimum contacts approach.⁶¹ The Brussels Regulation governs jurisdiction⁶² in civil and commercial disputes between litigants and provides for the enforcement of judgments throughout the European Union.⁶³ The Brussels Regulation applies throughout Europe, while the U.S. approach has yet to be adopted or borrowed by any other legal system.⁶⁴

lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (last visited May 5, 2005). The United Kingdom repealed its Data Protection Act of 1984 and enacted more than 20 statutory implements to update its data protection. See Slaughter & May, *An Introduction to Data Protection in the United Kingdom* 2-4 (1999). As of December 2002, only two Member States had enacted legislation implementing the Copyright Directive. Europeans Miss Deadline on New Digital Copyright Law 7 *Cyberspace Lawyer* 16 (Dec. 2002).

59. European Commission Resolution on the Communication from the Commission on Globalization and the Information Society: The Need for Strengthened International Coordination, 1999 O.J. (C 104) 128. An ISP from the United Kingdom removed its server from Germany to avoid liability under Germany's strict anti-pornography laws. *Id.*

60. Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, at <http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32001R0044:EN:HTML> (last visited April 12, 2005).

61. Felicity Barringer, *Internet Makes Dow Jones Open to Suit in Australia*, N.Y. TIMES, Dec. 11, 2002, at 6.

62. Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, at <http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32001R0044:EN:HTML> (last visited April 12, 2005) [hereinafter Brussels Regulation]. The Brussels Regulation treats "'jurisdiction' not choice of law. In other words, it says which country's courts will apply to transactions, not which laws will apply." Editors, *In the Courts, Have Fun Finding Your Forum*, 16 *CYBERSPACE LAWYER* 1 (June 2001).

63. *Id.*

64. Non-European countries do not follow either the Brussels Regulation or apply the U.S. minimum contacts framework for determining personal jurisdiction. "In Japan, a court can exercise jurisdiction over a defendant based on the presence of any assets of the defendant in Japan. In addition, a court in Japan tends to recognize its international competence unless there are "extraordinary circumstances," so, in a case where a defendant is a large multi-national corporation, the exercising of international jurisdiction over the defendant can be recognized by a court as reasonable solely based on the presence of its branch in Japan, even though the case has no connection with the branch." Masaki Hamano, *Comparative Studies in the Approach to Jurisdiction in Cyberspace*, at

A judgment rendered in a European Union country may be enforceable outside of its borders.⁶⁵ The European Court of Justice, for example, ruled that the Brussels Convention⁶⁶ applied to a Canadian company in a contract action brought in a French court.⁶⁷

The new Brussels Regulation governing jurisdiction and judgments applies to all Brussels Convention signatories except Denmark, which has opted out of the new regulations.⁶⁸ The Brussels Regulation sets forth the general rule that “persons domiciled in a Contracting State shall whatever their nationality, be sued in the courts of that State.”⁶⁹ European consumers, unlike their American counterparts, have an absolute right to sue a seller or supplier if it “pursues commercial or professional activities in the Member State of the consumer’s domicile.”⁷⁰ American courts, in contrast, enforce choice of forum clauses that require the consumer to litigate in the seller’s home court.⁷¹ In tort cases, the place “where the harmful

<http://www.geocities.com/SiliconValley/Bay/6201/conclusion.html> (last visited April 12, 2005).

65. In *Air Canada v. UK* (1995) 20 EHRR 150, the European Court of Human Rights held that the seizure of an aircraft belonging to the Canadian applicant had not infringed Article 1 of the First Protocol. It was not suggested that the fact that the applicant was resident in Canada affected its rights under that provision.

66. The 1968 Brussels Convention was replaced by the Brussels Regulation in March of 2002. See Europa, Jurisdiction, Recognition, and Enforcement of Judgments, at <http://europa.eu.int/scadplus/leg/en/lvb/l33054.htm> (last visited April 10, 2005).

67. Eugene Gulland, *All the World's a Forum: Business That Benefit from the Increased Globalization of Commerce Also Face Increased Risks of Liability Abroad*, N.J.L.J. (Apr. 29, 2002) (discussing *Group Josi Reinsurance Co. S.A. v. Universal General Insurance Co.*, 2000 E.C.R. I-5925).

68. The Brussels Convention, rather than the updated Brussels Regulation, applies to Denmark, which has opted out. 3 Council Regulation (EC) No 44/2001 of 22 December 2000, OJ L 12, 16.1.2001, p. 1, replacing the Brussels Convention of 1968, of which a consolidated version was published in OJ C 27, 26.1.1998, p. 1 cited in Rome II, *supra* note 25.

69. Brussels Regulation, *supra* note 62, at Art. 2.1

70. Brussels Regulation, *supra* note 62, at Art 15. 1(c).

71. Compulsory arbitration clauses in mass-market license agreements have been enforced by a number of courts. See, e.g., *Westendorft v. Gateway 2000, Inc.*, 2000 Del. Ch. LEXIS 54 (Del. Ch. Ct., Mar. 16, 2000); *Brower v. Gateway 2000, Inc.*, 676 N.Y.S.2d 569 (1998); *Lieschke v. RealNetworks, Inc.*, 2000 U.S. Dist. LEXIS 1683 (N.D. 2000) (enforcing arbitration clauses in mass market licenses); *American Online, Inc. v. Booker*, 781 So.2d 423, 425 (Fla. Dist. Ct. App. 2001) (upholding forum selection clause in “freely negotiated agreement” and holding that the unavailability of a class action procedure in Virginia was not a sufficient basis for striking down a forum selection clause); *Caspi v. Microsoft Network, L.L.C.*, 323 N.J. Super. 118, 732 A.2d 528, 530, 532-3 (N.J. Super. Ct. App. Div. 1999) (validating forum selection clause where subscribers to online software were required to review license terms in scrollable window and to click “I Agree” or “I Don’t Agree”); *Barnett v. Network Solutions, Inc.*, 38 S.W.3d 200, 203-4 (Tex. App. 2001) (upholding forum selection clause in online contract for registering

event occurred or may occur” is the place of jurisdiction.⁷²

Any entity doing business on the Internet may be subject to divergent tort rules in distant forums. In December of 2002, the Australian High Court held that a businessman could sue Barron’s and Dow Jones for libel in the state of Victoria based on evidence that several hundred people in that state accessed the Dow Jones Web site where the allegedly defamatory article was posted.⁷³ In the *Dow Jones* case, the Australian Court reasoned that “the place of uploading of materials onto the Internet might bear little or no relationship to the place where the communication was composed, edited, or had its major impact.”⁷⁴ “This decision made Australia the only country that allows an action against a foreign defendant based solely on an Internet download in that country.”⁷⁵ The Dow Jones case ultimately settled for \$440,000 and legal fees in November of 2004.⁷⁶

In the Australian *Gutnick* case, a court exercised jurisdiction over Dow Jones for simply posting material on a Web site. The Australian Dow Jones case “created a special problem for the American media: should they clear their stories to their own tolerant standards or should they cut them back to those applied by the most restrictive jurisdiction in which they might be sued?”⁷⁷ In this defamation lawsuit by an Australian citizen against an American publishing company, the High Court of Australia rejected the defense that the U.S. single publication rule limits the jurisdiction and applicable law to where the single publication was made. The Australian court ruled

Internet domain names that required users to scroll through terms before accepting or rejecting them); *Cf. Specht v. Netscape Commun. Corp.*, 306 F.3d 17 (2d Cir. 2002) (holding that user’s downloading software where the terms were submerged did not manifest assent to arbitration clause); *Klocek v. Gateway, Inc.*, 104 F. Supp.2d 1332 (D. Kan. 2000) (declining to enforce arbitration clause on grounds that user did not agree to standard terms mailed inside computer box).

72. Article 15(3) provides that in “matters relating to tort, delict, or quasi-delict, jurisdiction is in the Member State for the “place where the harmful event occurred or may occur.” Brussels Regulation, *supra* note 62, at Art. 15(3).

73. *Dow Jones & Co., Inc. v. Gutnick*, [2002] HCA 56.

74. *Id.* at 130 (opinion of Kirby, J.).

75. Nathan W. Garnett, *Dow Jones & Co. v. Gutnick: Will Australia’s Long Jurisdictional Reach Chill Internet Speech World-Wide?*, 13 PAC. RIM L. & POL’Y 61, 61 (2004).

76. Declan McCullagh, *Dow Jones Settles Net Defamation Case*, C/Net News.com (Nov. 15, 2004), at

<http://ecoustics-cnet.com.com/Dow+Jones+settles+Net+defamation+suit/2110-1030-3-5453453.html> (last visited April 10, 2004).

77. Martin Soames, *Don’t Rely on Reynolds: Recent Rulings Prove Yet Again That English Courts Are Dangerous Places for the Press*, THE GUARDIAN (LONDON), Feb. 7, 2005, at 14 (noting reversal of Gutnick ruling by Australian appeals court).

that the residence of Internet defamation plaintiff was the place of the tort and therefore jurisdiction was proper.⁷⁸

The High Court reasoned that the defendant knew its Web site would have a worldwide reach when it made its publishing available there, and therefore the law of Australia, where damage resulting from the tort occurred, applies.⁷⁹ Cyberspace will not fulfill its promise if Web sites continue to be subject to hundreds of conflicting procedural and substantive rules simply because the material can be accessed in every nation of the globe.

[C] Rome II's Convention on Choice of Law for Torts

The European Commission has formulated a draft of the Rome II Convention concerning which laws should apply in cross-border tort disputes.⁸⁰ The Rome II Convention for torts, delicts, or noncontractual relations proposes uniform rules for resolving conflicts of law in European cross-border disputes. The Commission seeks to harmonize “conflict rules, which must be distinguished from the harmonization of substantive law.”⁸¹ The Commission believes that it is more efficient to have one set of conflict of law principles in order to reduce “the cost of litigation and boosting the foreseeability of solutions and certainty as to the law.”⁸² The Commission is divided over how Rome II interrelates with the already enacted E-Commerce Directive, which determines jurisdiction on the principle

78. Nikki Tait & Patti Waldmeir, *Australia Court Gives Landmark Ruling on Internet Law*, FINANCIAL TIMES, Dec. 11, 2002, at 15.

79. *Australian High Court Rejects Single Publication Rule for Internet Defamation*, 7 Electronic Commerce & Law Rep. (BNA) No. 48, at 1226 (December 18, 2002) (discussing *Dow Jones & Co. v. Gutnick*, [2002] HCA 56).

80. The Scope of Rome II “covers all non-contractual obligations except those in matters listed in paragraph 2. Non-contractual obligations are in two major categories, those that arise out of a tort or delict and those that do not. The first category comprises obligations relating to tort or delict, and the second comprises obligations relating to what in some jurisdictions is termed ‘quasi-delict’ or ‘quasi-contract,’ including in particular unjust enrichment and agency without authority or negotiorum gestio.” Rome II, *supra* note 25. The Brussels Regulation governs jurisdiction for contractual relations, whereas Rome II governs non-contractual relations or torts. “The proposed Regulation applies to situations involving a conflict of laws regarding non-contractual obligations in civil and commercial matters (arising out of a tort or delict and out of an act other than a tort or delict), with the exception of revenue, customs or administrative matters.” Europa, Activities of the European Union, Summaries of Legislation, Non-Contractual Relations: Rome II, at <http://europa.eu.int/scadplus/leg/en/lvb/l33211.htm> (last visited April 15, 2005).

81. *Id.*

82. *Id.*

of country of origin.⁸³

The “country of origin” approach subjects a company to regulation in only the country where the information originated irrespective of whether information is transmitted to other Member States. The country of origin rule means that a service provider or e-business need only comply with the rules and regulations in one Member State as opposed to tailoring content for all of the countries of the European Community. European regulators have only the ability to control regulations originating in their country.

The European Community must determine whether the conflict of law principles for Internet tort or *delict* actions should be based upon a *lex loci delicti*⁸⁴ or the place where goods or services were ordered.⁸⁵ Article 3(1) of Rome II adopts as the basic rule the law of the place where the direct damage arises or is likely to arise. In most cases this corresponds to the law of the injured party’s country of residence.⁸⁶ In a typical cyberspace transaction, “the place of purchase may be purely fortuitous, and under certain circumstances may even be virtually impossible to establish.”⁸⁷ Internet publishers fear that the Rome II Convention, which applies to online defamation cases, could result in publications “having to pay libel damages under the laws of 100 different countries if defamatory material is published

83. European Publisher’s Council, *Fact Sheet: Jurisdiction and Applicable Law* (Feb. 2004) at http://www.epceurope.org/issues/RomeII_LegalOpinionUKMedia.shtml (last visited April 12, 2005).

84. The concept of *lex loci delicti* refers to the law of the place of the tort. Matthew Collins, *The Law of Defamation and the Internet*, at <http://www.mattcollins.com.au/oupupdate7.htm> (last visited Mar. 21, 2005). “Admittedly, the Member States virtually all give pride of place to the *lex loci delicti commissi*, whereby torts/delicts are governed by the law of the place where the act was committed. The application of this rule is problematic, however, in the case of what are known as “complex” torts/delicts, where the harmful event and the place where the loss is sustained are spread over several countries. See Rome II, *supra* note 25.

85. The Rome II Convention considers non-contractual obligations arising out of family whether arising from tort or delict to be beyond the scope of the agreement. “Since there are so far no harmonized conflict-of-laws rules in the Community as regards family law, it has been found preferable to exclude non-contractual obligations arising out of such relationships from the scope of the proposed Regulation. See Rome II, *supra* note 25. In addition, some commentators in the United Kingdom argue that Rome II does not encompass the invasion of privacy. *Id.*

86. Commission of the European Communities, Opinion of the European Economic and Social Committee on the Proposal for a Regulation of the European Parliament and the Council on the law applicable to non-contractual obligations. See Rome II, *supra* note 25 (discussing Article 3 of the Rome II Convention).

87. *Id.*

over the internet.”⁸⁸ The Rome II Convention fails “to recognize the possibility of publishers in one country being subjected to the libel laws of others, causing particular problems for Internet providers.”⁸⁹

[D] Choice of Forum in Cyberspace

E-businesses reduce their exposure to unfamiliar laws by requiring all users worldwide to submit to the company’s choice of legal forum. Nokia, for example, inserts a conflict of forum clause into its mass-market contracts, requiring users to submit to arbitration in Helsinki, Finland, where Nokia has its headquarters.⁹⁰ American companies frequently require users to waive their jury rights in favor of arbitration. For example, America Online requires all of its customers to litigate any disputes in Virginia applying that Commonwealth’s law:

These Terms of Use shall be governed by and construed in accordance with the laws of the Commonwealth of Virginia, excluding its conflicts of law rules. You expressly agree that the exclusive jurisdiction for any claim or action arising out of or relating to these Terms of Use or your use of this site shall be filed only in the state or federal courts located in the Commonwealth of Virginia, and you further agree and submit to the exercise of personal jurisdiction of such courts for the purpose of litigating any such claim or action.

Similarly, MCI requires all users to arbitrate any dispute under the law of New York, while forbidding arbitrators from awarding consequential damages or punitive damages. The agreement shortens

88. *‘Rome II’ European Privacy Law Set to Invade UK Media*, EUROPE INTELLIGENCE WIRE: THE LAWYER, Feb. 16, 2004 (stating that “[a] UK-based publication about a businesswoman with an international reputation could result in a UK court having to apply, and award damages, from over 100 different legal systems, even though the publication might be lawful under the law of England and Wales”) (quoting Periodical Publishers Association Legal Affairs spokesman).

89. John-Paul Ford Rojas, *Peers Unhappy with EU Plans on Civil Disputes*, Press Association, April 7, 2004 (citing House of Lord’s Subcommittee Report on proposed Rome II Convention).

90. Nokia’s choice of law and forum clause states: “This Agreement is governed by the laws of Finland. All disputes arising from or relating to this Agreement shall be settled by a single arbitrator appointed by the Central Chamber of Commerce of Finland. The arbitration procedure shall take place in Helsinki, Finland in the English language. If any part of this Agreement is found void and unenforceable, it will not affect the validity of the balance of the Agreement, which shall remain valid and enforceable according to its terms. This Agreement may only be modified by a writing signed by an authorized officer of Nokia, although Nokia may vary the terms of this Agreement.” *Jurisdictional Clauses in Shrinkwrap and Clickwrap Contracts*, at <http://www.cptech.org/ecom/ucita/licenses/jurisdiction.html> (last visited Mar. 23, 2005).

91. *AOL.com Terms and Conditions of Use*, at <http://www.aol.com/copyright.adp> (last visited Mar. 23, 2005).

the statute of limitations to a period of one year.⁹² The rules for enforcing choice of forum clauses in cross-border e-commerce disputes have yet to be formulated.⁹³

The validity of e-commerce mass-market license agreements is due in part to the U.S. Supreme Court's willingness to legitimate one-side forum selection clauses as decided in *Carnival Cruise Lines, Inc. v. Shute*.⁹⁴ In *Carnival Cruise*, a Washington resident who was injured on a cruise ship argued that a Florida forum selection clause contained in her ticket was unenforceable because of the expense and inconvenience of litigating in Florida.⁹⁵ The Court rebuffed this argument, holding that the forum selection clause was reasonable and enforceable even though the litigants were physically and financially incapable of pursuing their claims in Florida.⁹⁶

Most American courts extend the principles of *Carnival Cruise* into cyberspace.⁹⁷ A few U.S. state and federal courts, however,

92. MCI's terms and conditions require disputes to be "governed by the substantive laws of the State of New York, excluding its conflicts principles. Any dispute arising out of or related to these terms and conditions or your use of the Software, which cannot be resolved by good faith negotiation, shall be submitted to J.A.M.S./Endispute for final and binding arbitration in accordance with the J.A.M.S./Endispute Arbitration Rules, as amended by these terms and conditions. Each party shall bear the fees and costs it incurs in preparing and presenting its case. This provision shall be subject to the United Arbitration Act, 9 U.C.S. § 1-16 ("USAA"). The arbitrator shall have no authority to award punitive, exemplary, or consequential damages. The award may be confirmed and enforced in any court of competent jurisdiction. All post proceedings shall be governed by the USAA. Any cause of action you may have with respect to this Agreement or the Software must be commenced within one (1) year after the claim or cause of action arises or such claim or cause of action is barred." *Id.*

93. Compare John R. Schmertz, Jr. & Mike Meier, *Applying French Data Protection Laws*, INT'L L. UPDATE, Dec. 1998 (citing French company's pursuit of antitrust dispute in U.S. on Internet basis against French defendant) with *Global Roundtable: Taking On The World: If the Future of Business Is Global, So, Too, Is the Business of Law*, AMERICAN LAWYER, Nov. 1998, at 97 (noting foreign companies' desire to avoid American jurisdiction). For an example of international forum shopping, see *Filetech S.A. v. France Telecom S.A.*, 157 F.3d 922, 925 (2d Cir. 1998) (describing French telecommunication antitrust dispute in U.S. court on basis of Internet presence).

94. 499 U.S. 585 (1991) (enforcing arbitration clause for dispute arising out of cruise even though the contractual agreement to arbitrate was only noted on the reverse of a ticket stub).

95. *Id.* at 596.

96. *Id.* at 590.

97. *In re RealNetworks, Inc.*, Privacy Litigation, 2000 U.S. Dist. LEXIS 6584 (N.D. Ill. May 11, 2000) (stating that click through agreement with arbitration sufficient to dismiss class action request); *Decker v. Circus Circus Hotel*, 49 F. Supp. 2d 743 (D. N.J. 1999) (enforcing forum selection clause in case involving consumer booking hotel room from Web site); *Celmins v. America Online*, 748 So. 2d 1041 (Fla. Dist. Ct. App. 1999) (validating AOL's forum selection clause); *Barnett v. Network Solutions, Inc.*, 38 S.W.3d 200 (Tex. App. 2001) (enforcing

police one-sided forum selection clauses.⁹⁸ In *Williams v. America Online, Inc.*,⁹⁹ the Massachusetts Superior Court refused to enforce America Online's standard clickwrap terms of service agreement that includes a forum selection clause. The *Williams* court held that the forum selection clause was unenforceable because AOL's license agreement had no reasonable method for the potential licensee to manifest assent. The requirement that consumers litigate in Virginia to seek redress was found to be, in effect, no remedy. In *America Online, Inc. v. Superior Court*,¹⁰⁰ a California court also concluded that a forum selection clause requiring consumers to litigate in Virginia courts was unenforceable as a matter of California public policy.¹⁰¹ The requirement that Member States follow the Brussels Regulation makes it unlikely that European courts will enforce one-sided shrink-wrap or mass-market licenses. The development of e-commerce will be seriously impeded if nations continue to follow their individual divergent legal paths.

PART II: DISCORDANT CYBERTORT REGIMES: EUROPE VS. AMERICA

I wonder how serious we are about not subjecting U.S. citizens to the constitutional reasoning of foreign courts, and I think this is going to become a big issue with Internet defamation lawsuits, which are all the rage right now and have very troubling implications for the First Amendment.

Justice Antonin Scalia.¹⁰²

Americans and Europeans have fundamentally different legal

forum selection clause in user agreement).

98. *Miles v. Am. Online, Inc.*, 202 F.R.D. 297 (M.D. Fla. 2001) (refusing to enforce AOL's forum selection clause).

99. 2001 WL 135825 (Mass. Super. Ct. February 8, 2001) (holding that AOL's choice of forum clause was unenforceable because the software user could download the agreement without first viewing the terms of the license agreement). *See also*, *Miles v. Am. Online*, 202 F.R.D. 297 (M.D. Fla. 2001) (declining to enforce AOL's choice of law clause).

100. 108 Cal. Rptr. 2d 699 (Cal. Ct. App. 2001) (concluding that a forum selection clause limiting litigation to Virginia courts was in effect a waiver of all contract remedies and therefore unenforceable under California public policy).

101. *See, e.g.*, *Comb v. PayPal, Inc.*, 218 F. Supp. 2d 1165 (N.D. Cal. 2002) (rejecting a motion to compel arbitration because the user agreement was unconscionable); *Am. Online, Inc. v. Pasiaka* 870 So. 2d 170 (Fla. Dist. Ct. App. 2004) (rejecting AOL's motion to compel enforcement of its forum selection clause).

102. United States Association of Constitutional Law Discussion, *Constitutional Relevance of Foreign Court Decisions*, FEDERAL NEWS SERVICE, Jan. 13, 2005, at LexisNexis' European News Sources database (quoting U.S. Supreme Court Associate Justice Antonin Scalia).

traditions that reflect their unique national histories. The common law approach of creating law around precedent is found only in the Anglo-American legal tradition. Despite the dominance of civil codes that are derived from Roman law in all of the continental European countries, there are many national differences. Sweden and Norway for example, have a well-established ombudsman tradition for resolving disputes,¹⁰³ which is not found in France. In the field of products liability, there are several divergent doctrinal paths that have survived the European Community's adoption of a Products Liability Directive.¹⁰⁴ The European Community is seeking greater

103. "Sweden's consumer ombudsman, who is responsible for enforcing the country's ban, said he would welcome a Europe-wide ban in order to thwart children's advertising being beamed into the country via satellite." John Tylee, *Sweden Declares Plans to Extend Kid's Ad Ban*, CAMPAIGN, Nov. 26, 1999; *Interested Parties: What They Want*, THE IRISH TIMES, Dec. 2, 2003, at 7 (describing Irish use of Swedish ombudsman concept to mediate disputes); Christine Wade, *Consumer Enforcers Clean Up Web in Worldwide Sweeps*, OFFICE OF FAIR TRADING, HERMES DATABASE, Oct. 8, 2004 (discussing role of Norwegian ombudsman in resolving consumer complaints).

104. The Europeans based their Products Liability Directive on the Restatement (Second) of Torts, §402A entitled "Special Liability of Seller of Product for Physical Harm to User or Consumer," adopted in all but a few American jurisdictions. THOMAS H. KOENIG & MICHAEL L. RUSTAD, IN DEFENSE OF TORT LAW 57 (New York University Press, 2001). In a products liability case, the underlying policy rationale is that the manufacturer is in the best position to protect the user and should shoulder the burden of precaution. *Id.* Products liability is generally subdivided into three general types: (1) manufacturing flaws; (2) design defects; and (3) failure to warn or instruct. *Id.* A plaintiff has the burden of proving three elements: "(1) the injury resulted from a condition of the product; (2) the condition was an unreasonably dangerous one; and (3) the condition existed at the time the product left the defendant's control." *Id.* The Europeans follow a similar regime though there are significant national variations in the implementation of the Products Liability Directive. Commission of the European Communities, Report from the Commission on the Application of Directive 85/374 on Liability for Defective Products, COM (2000) 0893 final, (Jan. 31, 2001). In every products liability action, a plaintiff must establish a causal connection between the product defect and the injury sustained. *Id.* In Sweden, the judge establishes the causal connection and is given the discretion to base a finding on a mere probability. *Id.* In Finland, a judge has the discretion of easing the plaintiff's burden in establishing either defect or causal connection depending upon the availability of evidence. *Id.* In U.S. products liability cases, plaintiffs will sometimes use the doctrine of *res ipsa loquitur* to create an inference of negligence where direct evidence is not available. In order to prove *res ipsa*, a plaintiff must demonstrate: "[1] Evidence of the actual cause of the injury is not obtainable; [2] The injury is not the kind that ordinarily occurs in the absence of negligence by someone; [3] The plaintiff was not responsible for his or her own injury; [4] The defendant, or its employees or agents, had exclusive control of the instrumentality that caused the injury; and [5] The injury could not have been caused by any instrumentality other than that over which the defendant had control." The Bocardio Law Firm, L.L.P., *Medical Malpractice: Res Ipsa Loquitur*, at <http://bocardio-version2.lawoffice.com/CM/FSDP/PracticeCenter/>

harmonization through the use of Directives, which are broad legal principles that require implementing legislation in each individual Member State.¹⁰⁵

While Part I dealt with procedural barriers to worldwide cyberlaw development, this section focuses on how substantive differences in the law of torts prevent effective legalization of cyberlaw. The countries that follow the Anglo-American common law tradition share much common ground, but there are substantial differences even within their shared legal heritage. Tort law in the United States is chiefly state law and the jurisdictions differ widely in the rights and duties recognized. Part II explores some of these differences in substantive civil codes.

[A] Divergent Defamation Regimes

Defamation is a common law tort action when a false oral or written statement has been made that lowers the plaintiff's reputation in the community.¹⁰⁶ The Internet raises complex substantive legal conflicts as to what constitutes a defamatory statement and how reputation is to be measured for Internet transmissions. With hundreds of countries connected to the Internet, it is unclear as to whose community standards apply.¹⁰⁷ The English definition of

Personal-Injury/Medical-Malpractice.asp?focus=topic&id=4 (lasted visited Feb. 15, 2005). In Spain, courts apply a doctrine functionally equivalent to the American doctrine of *res ipsa loquitur*. Spanish judges are permitted to make presumptions about product defects in cases where the original product that caused injury or death is destroyed or lost. Commission of the European Communities, Report from the Commission on the Application of Directive 85/374 on Liability for Defective Products, COM (2000) 0893 final, (Jan. 31, 2001). Similarly, jurists in the Netherlands have the discretion to "overthrow the burden of proof in exceptional cases, e.g. in the case of the defect in the product." *Id.*

105. The European Community has already formulated rules for the conflicts of law for contracts (Rome I Convention) and the proposed Rome II governing torts or non-contractual relations. The Europeans view Rome II rules as the first step toward a broader unified European procedural law. "Contributors suggest including rules on the entire law of obligations, including not just contract and tort (delict) but also restitution (unjust enrichment), and rules on property, including assignment, intellectual property and intangible property generally as well as security interests, the latter as a priority, and trusts." Communication from the Commission to the European Parliament and the Council - A more coherent European contract law - An action plan, 2003 O.J. (C 63) (Feb. 12, 2003).

106. PROSSER AND KEETON ON THE LAW OF TORTS §111, at 773 (W. Page Keeton et al. eds., West Group 1984).

107. There is little case law on Internet-related defamation in civil law jurisdictions. Some commentators have proposed a unified defamation regime to resolve conflicts over Internet defamation. See Barry J. Waldman, *A Unified Approach to Cyber-Libel: Defamation on the Internet, a Suggested Approach*, 6 RICH. J. L. & TECH. 9 (1999).

defamation was a communication to a third person that “tends to hold the plaintiff up to hatred, contempt, or ridicule or to cause him to be shunned or avoided.”¹⁰⁸ What would be considered to be defamatory in England may be protected expression in the United States.

The controversial boxing promoter Don King, who resides in Florida, filed suit against Lennox Lewis, a world champion boxer, a promotions company, and a New York attorney based upon an allegedly defamatory Internet posting that charged King with being Anti-Semitic.¹⁰⁹ King chose the United Kingdom to file suit even though the statements were posted on California-based Web sites because that country’s defamation laws are decidedly more pro-plaintiff.¹¹⁰ In the United States, this lawsuit would be dismissed on summary judgment since King is a public figure.¹¹¹ In Britain, however, where there is no such doctrine, his lawsuit could go forward.¹¹² In the United States there is a “qualified privilege” that serves as a defense to libel “where a party is under a legal, social or moral duty to communicate certain facts in the public interest.”¹¹³ English law does not recognize a public policy-based defense in relation to public figures.¹¹⁴ Under the English law of defamation, an

108. *Parmiter v. Coupland*, 151 Eng. Rep. 340, 342 (1840).

109. Kate O’Hanlon, *Thursday Law Report: Claim Form Could be Served Out of the Jurisdiction*, Nov. 11, 2004; *King v. Lewis and others*, THE INDEPENDENT, Nov. 11, 2004, at 1.

110. *Id.*

111. *Id.*

112. *Id.* (noting that “It was common ground that by the law of England the tort of libel was committed where publication took place, and that a text on the internet was published at the place where it was downloaded. There was therefore no contest but that, subject to any defenses on the merits Mr. King had been libeled in the English jurisdiction.”).

113. Michael Evans, *Media Law: An Ocean Apart: Amazon’s UK Web site Refuses to Sell a Book about the Bush Family’s Links to the House of Saud. Yet its U.S. Counterpart has no Such Qualms*, THE GUARDIAN (LONDON), Aug. 9, 2004, at 10.

114. The constitutionalization of defamation law in the United States began with *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964). In the *Sullivan* case, the Court reversed a defamation verdict rendered in an Alabama state court against civil rights leaders who published a paid advertisement accusing the Police Commissioner of Montgomery, Alabama, of violent actions toward demonstrators. *Id.* The Court constructed a “public official” doctrine that applied to issues of public importance. *Id.* The Court held that a state’s power to award damages for libel in actions brought by public officials against critics of their official conduct requires proof of actual malice to satisfy the constitutional standard. *Id.* at 279-280. The *Sullivan* holding as to public officials was expanded to include public figures in *Curtis Publ’g Co. v. Butts*, 388 U.S. 130 (1967). Public figures may be celebrities such as movie stars, athletes, or other well-known individuals. As with elected or appointed public officials, a celebrity must prove that a defamatory statement was made with malice. Finally, there is the limited public figure where

Internet Web site would have the burden of verifying rumors about public figures.

In *Loutchansky v. The Times Newspapers Limited*,¹¹⁵ a court in the United Kingdom ruled on an article that was first published in a print publication and later posted on the Internet. In *Loutchansky*, an article accused a Russian businessman of money laundering.¹¹⁶ A second article linked the trader to the Russian Mafia.¹¹⁷ In this case, there was not a substantial dispute as to the defamatory nature of these statements.¹¹⁸ The English court was asked to resolve the conflicting law of defamation under Russian law as well as under the United Kingdom's Defamation Act of 1996 in the context of the Internet.¹¹⁹

The Court of Appeal held that a newspaper's online archive did not have a qualified privilege to post a story containing defamatory content. The court acknowledged a qualified privilege for the print publication, because the articles were on a matter of public concern, but ruled that this privilege did not extend to the Web site.¹²⁰ The *Loutchansky* court ruled that the Web site was also liable for defamation on a republication theory every time the site was accessed by visitors.¹²¹ While there is no parallel case, it is likely that a U.S. court would find the qualified privilege extended to all media given the U.S. emphasis on the First Amendment, which promotes the free exchange of ideas on matters of public interest.¹²²

In Internet defamation cases, a fair balance must be struck between the domestic tort law and rights of free expression that vary between countries. Information posted on the Internet may be protected in North America while violating contemporary community standards in less developed countries. An Islamic fundamentalist female might be publicly shamed by being depicted on a Web site that shows her unveiled face. A Hindu might be humiliated by being placed

the plaintiff has thrust himself or herself into a public controversy in order to influence its outcome. *Gertz v. Robert Welch, Inc.*, 418 U.S. 323 (1974). The United Kingdom does not recognize any of these categories making it a more favorable forum for plaintiffs in libel actions.

115. 2001 EWCA Civ. 1805 (CA, 2001).

116. *Id.* at ¶5.

117. *Id.* at ¶6.

118. *Id.* at ¶7.

119. *Id.*

120. 2001 EWCA Civ. at ¶8.

121. *Id.* (stating that "each article foreseeably prompted republication of the libelous matter").

122. Alexander Gigante, *Ice Patch on the Information Superhighway: Foreign Liability for Domestically Created Content*, 14 CARDOZO ARTS & ENT. L. J. 523, 528 (1996).

unwittingly in a hamburger chain's online advertisement. Even within the Anglo-American tradition, there is sharp divergence in defamation law. The United States has carved out special tort rules making it difficult for public officials or public figures¹²³ to sue for defamation.¹²⁴

Due to stronger American protections for free speech, a "plaintiff with a transatlantic reputation in both the United States and the United Kingdom will find obvious advantages in bringing a defamation suit in the United Kingdom."¹²⁵ In *Dow Jones & Co., Inc. v. Harrods, Ltd.*, for example,¹²⁶ *The Wall Street Journal* was the defendant in a United Kingdom lawsuit over its republication of an April Fool's Day prank press release that was disseminated by Harrods Department Store on its Web site and print editions. The English firm issued a mock press release stating that it planned to "float" its department store by building a ship version of the store and offered to sell shares in the venture.¹²⁷ Upon learning the announcement had been a prank, the *Journal* countered with a story stating: "If Harrods, the British luxury retailer ever goes public, investors would be wise to question its every disclosure."¹²⁸

Harrods and its owner, Al Fayed, filed suit in London's High Court of Justice seeking damages for libel.¹²⁹ Dow Jones, the owner of the *Wall Street Journal*, filed for a declaratory judgment, seeking to preclude the plaintiffs from pursuing their defamation claims.¹³⁰ Dow Jones alleged that an action for defamation based on the *Journal*

123. *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964) (holding that there were constitutional protections for speech and press limiting a state's power to award tort damages in a libel action brought by a public official against critics of his role). Three years later the Court extended the *Sullivan* rule to public figures in *Curtis Pub'g Co. v. Butts*, 388 U.S. 130 (1967).

124. *Gigante*, *supra* note 122, at 525-526.

125. *Id.* at 528.

126. 237 F. Supp. 2d 394 (S.D.N.Y. 2002).

127. *Id.* at 400. The fictitious press release on March 31, 2002, was headlined "Al Fayed Reveals Plan to 'Float' Harrods." The release stated that Al Fayed, Harrods' Chairman and effective owner, "would issue on the following day an important announcement 'about his future plans for the world-famous store,' including 'a first-come-first-served share option offer.' Journalists seeking further comment were directed to contact "Loof Lirpa" at Harrods. In fact, 'Loof Lirpa' is 'April Fool' spelled backward. On April 1, 2002, the planned announcement posted on the designated Web site described Al Fayed's decision to 'float' Harrods by building a ship version of the store to be moored in London on the embankment of the Thames River. The announcement included a limited offer of 'shares in this exciting new venture.' Persons who registered on the Web site by noon that day, 'the first of April!' were promised 'a share certificate.'" *Id.*

128. *Id.* at 401.

129. *Id.* at 402.

130. 237 F. Supp. 2d 394 (S.D.N.Y. 2002).

article “would be summarily dismissed under federal and state constitutional law of any American jurisdiction because the publication comprised only the author’s non-actionable expression of opinion based on true statements.”¹³¹ The U.S. court refused to grant Dow Jones preemptive relief against Harrods’ cause of action.¹³²

In another cybertort case that would have been decided differently under U.S. law, a British court ordered an Internet service provider (ISP), Demon Internet, to pay money damages to a scientist who had been defamed by a posting on one of their newsgroups.¹³³ The judge in that case “acknowledged that Demon (the ISP sued by Godfrey) was not the publisher of the libel, but found the statutory defense was not available once Godfrey had sent a fax alleging that the postings about him were defamatory.”¹³⁴ In the United Kingdom, the defense of “innocent dissemination” protects bookstores and printers from liability, but only if they promptly remove the offending materials upon notification.¹³⁵ The ISP was found liable and paid damages of \$475,000 because they had failed to remove the defamatory posting after receiving notice.¹³⁶

[B] Conflicting Internet Privacy Regimes

Internet technologies raise critical issues about tracking individuals on the World Wide Web. In the United States, the tort action for privacy had its genesis in a law review article written by Samuel D.

131. *Id.* The Journal argued that its “cause of action in the United Kingdom would be nullified not only in the United States but, under the American ‘single publication rule,’ *anywhere else in the world, including the U.K. itself.*” *Id.* at 410. “Dow Jones asserts that under British law: (1) the burden of proving truth of defamatory statements falls on the defendant; (2) defamation is a strict liability tort and plaintiff need not prove that the defendant acted with any fault, in contrast with the ‘actual malice’ standard that applies under American First Amendment principles; (3) protection for expression of opinion is severely limited; (4) only limited protection is available for statements about public officials or public figures; (5) aggravated damages are permitted for asserting certain defenses, for example, a defendant’s seeking to justify the publication; (6) plaintiff’s attorneys fees and costs must be paid by the unsuccessful defendant; (7) multiple, repetitive suits are allowed for each individual publication, for example, for different media or various places of publication.” *Id.* at 403 n. 18.

132. *Id.* at 412.

133. *Godfrey v. Demon Internet, Ltd.* 4 All E.R. 342 (1999). *See also* Terri Judd, *Internet Providers Get Legal Protection Against Vigilantes*, THE NEW ZEALAND HERALD, July 11, 2001.

134. Evans, *supra* note 113, at 10.

135. Judd, *supra* note 133.

136. No damages would have been assessed in the United States against the provider because of the absolute publisher’s immunity accorded under 47 U.S.C. § 230 (2000).

Warren and Louis D. Brandeis.¹³⁷ New York was the first state to recognize the tort of invasion of privacy, in 1902.¹³⁸ William Prosser divided privacy-based torts into four categories: [1] intrusion upon seclusion; [2] public disclosure of private facts; [3] false light; and [4] the right of publicity.¹³⁹ Unlike Europe, there is no real codification of privacy rights in U.S. law. Some states have codified privacy in statutes and other jurisdictions rely upon common law decisions.¹⁴⁰ The Framers of the U.S. Constitution did not explicitly address privacy as a fundamental right.¹⁴¹ The American law of privacy has evolved in a crazy quilt of piecemeal statutes at the federal and state levels. The path of U.S. privacy law has been to “limit governmental intrusion into a sphere of personal conduct and relations by defining the boundaries between the individual and the government.”¹⁴²

With the rise of the Internet, national variations in substantive tort law become increasingly important. The privacy rights of the individual vary significantly under different legal regimes. French law, for example, differs markedly from U.S. privacy-based torts. “While the public activities of such persons necessarily subject more of their lives to legitimate public scrutiny, a public official or figure may shield from inquiry and intrusion those aspects of private life not related to the conduct of the public activities.”¹⁴³ Under French law, public officials and public figures may choose to protect their autonomy by withdrawing “from the public arena and return to the private domain personal information previously divulged.”¹⁴⁴

In a United Kingdom case, the court ruled that sharing of personal information on an electoral register was a violation of the European Union Data Protection Directive.¹⁴⁵ In *Robertson v. Wakefield*

137. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

138. *Roberson v. Rochester Folding Box Co.*, 64 N.E. 442 (N.Y. 1902).

139. William Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).

140. “Unlike claims based on the common-law tort of invasion of privacy, civil actions based on Fla. Stat. Ann. §794.03 require no case-by-case findings that the disclosure of a fact about a person's private life was one that a reasonable person would find highly offensive.” *Florida Star v. B. J. F.*, 491 U.S. 524, 539 (1989).

141. “Constitutional privacy law has evolved largely from textual and inferential construction of the ‘Bill of Rights’; in particular, the First, Fourth, Fifth, and Ninth Amendments, as well as the Fourteenth Amendment.” MADELEINE SCHACHTER, *INFORMATIONAL AND DECISIONAL PRIVACY* 8 (Cardina Academic Press, 2003).

142. *Id.* at 25.

143. Gigante, *supra* note 122, at 544.

144. *Id.* at 544.

145. *Robertson v. Wakefield Metro. Council*, 2002 EWHC Admin., 915 (Q.B. 2002). Summarized in PERKINS COIE INTERNET DIGEST (INTERNATIONAL), *available at*

Metropolis Council, the plaintiff filed suit against his local election authority over the disclosure of personal information on the electoral register.¹⁴⁶ The United Kingdom's Highest Court held that the local governmental authority violated both the UK Data Protection Directive and the European Convention on Human Rights by disclosing personal information.

Since October 1998, the European Member States have been enacting national privacy statutes to comply with the Data Protection Directive. The European approach to Internet privacy is a command and control model with precise rules governing the handling of personal information, in sharp contrast to the U.S. legal system that relies largely upon a market-based solution to privacy. The European Data Protective Directive is designed to create uniformity in the processing of personal information across member states.¹⁴⁷ This Directive gives data subjects control over the collection, transmission, or use of personal information. Moreover, the data subject has the right to be notified of all uses and disclosures about data collection and processing.

A company is required to obtain explicit consent as to the collection of data on race/ethnicity, political opinions, union membership, physical/mental health, sex life, and criminal records. The Data Protection Directive requires that personal information be protected by adequate security. Data subjects have the right to obtain copies of information collected as well as the right to correct or delete personal data. It is important that consent be obtained from the data subject prior to entering into the contract.¹⁴⁸ Personal data may not be transferred to other countries without an "adequate level of protection."¹⁴⁹ Member States are required to provide that a transfer of personal data to a third party takes place only if there is assurance of an adequate level of data protection. A company is liable for civil or criminal penalties for the unlawful processing of personal data.

http://www.perkinscoie.com/casedigest/icd_results.cfm?keyword1=international&opic=International (last visited Feb. 10, 2005).

146. *Id.*

147. The data protection traditions varied significantly across Member States. Germany, France, and United Kingdom had a tradition of strong protection of privacy versus non-existent regulation in Greece. RONALD MANN & JANE WINN, *ELECTRONIC COMMERCE* 187 (New York: Aspen Law and Business, 2002).

148. Council Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L281) (Nov. 23, 1995) at Art. 7 available at <http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML> (hereinafter Data Protection Directive) (last visited May 3, 2005).

149. *Id.* at Art. 25.

Damages may be assessed for the collection or transmission of information without a data subject's consent.¹⁵⁰

The European Union Data Protection Directive seeks to establish a regulatory framework that guarantees free movement of personal data. However, each individual is guaranteed a basic level of privacy by requiring each provider or transmitter to adhere to a set of guidelines.¹⁵¹ In contrast, the United States prefers that the business community develop industry standards such as BBBOnline privacy seals or other certification programs. The United States seeks to develop a transnational online privacy seal that can be earned by adherence to industry norms.¹⁵²

The Data Protection Directive requires Member States to assure that the transfer of personal data to a third country may take place only if the third country in question ensures an adequate level of protection.¹⁵³ No transfers of personal information of Europeans may be made to countries not having an adequate level of protection and complying with the notice and choice principles.¹⁵⁴ Organizations are required to ascertain whether third parties subscribe to the principles of the Directive before transferring information to them. Few sectors of the U.S. economy comply with the minimum data protection principles required by European Data Protection Directive.¹⁵⁵ The United States Commerce Department negotiated a "safe harbor"¹⁵⁶ with the European Union by agreeing to adhere to

150. *Id.* at Art. 23.

151. The six legal grounds defined in the Directive are "consent, contract, legal obligation, vital interest of the data subject or the balance between the legitimate interests of the people controlling the data and the people on whom data is held (i.e. data subjects)." European Commission Press Release: IP/95/822, *Council Definitively Adopts Directive on Protection of Personal Data*, (July 25, 1995), at http://www.privacy.org/pi/intl_orgs/ec/dp_EC_press_release.txt (last visited Feb. 12, 2005).

152. MICHAEL RUSTAD & CYRUS DAFTARY, *E-BUSINESS LEGAL HANDBOOK* 8-53, 8-54 at §8.02(c) (3d ed. 2003).

153. Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, 2000 OJ L 215 (July 26, 2000) (Official Journal L 215, 25/08/2000 P. 0007 – 0047).

154. U.S. Department of Commerce, *Safe Harbor Privacy Principles*, at <http://www.export.gov/safeharbor/shprinciplesfinal.htm> (last visited Feb. 12, 2005).

155. The Europeans were generally satisfied with U.S. privacy protection policies for the personal information of medical patients.

156. The basis of safe harbour protection was that if the U.S. complied with notice and choice principles of the Federal Trade Commission and also publicly disclosed their privacy policies, Europeans would allow person data of individuals to be transferred to American entities." Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on

reasonable precautions protecting data integrity.¹⁵⁷ The European Commission required U.S. companies to adopt adequate level of protection for the privacy of individuals.¹⁵⁸ The United States has no long-term choice but to harmonize their data collection policies with the European Data Protection Directive.

[C] Deviating Anti-Spam Regimes

Spam is “unauthorized bulk e-mail advertisements.”¹⁵⁹ An OECD Report estimates “that worldwide cost to Internet subscribers of spam is in the vicinity of \$ 12.5 billion a year.”¹⁶⁰ In the United States, Congress enacted a federal statute called “Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003,” popularly known as the CAN-SPAM Act.¹⁶¹ This federal statute requires e-

the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, 2000 OJ L 215 (July 26, 2000) (Official Journal L 215 , 25/08/2000 P. 0007 – 0047) (discussing Opinion 2/99 on the Adequacy of the “International Safe Harbor Principles” issued by the US Department of Commerce on 19 April 1999).

157. The United States is lobbying international organizations to convince them to adopt America’s self-regulatory approach to privacy. U.S. Government Working Group on Electronic Commerce, *Third Annual Report: Leadership for the New Millennium*, 40 (2000), available at <http://www.lib.umich.edu/govdocs/pdf/ecommerce2000anal.pdf> (last visited April 3, 2005). The United States is participating in the Platform for Privacy Protection (P3P), which is an industry standard developed by the World Wide Web Consortium that will enable visitors to express privacy preferences through their browsers. *Id.*

158. 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C (2000) 2441) (Text with EEA relevance) 2000 OJ L 215 (July 26, 2000).

159. *Am. Online, Inc., v. IMS*, 24 F. Supp. 2d 548, 549 (E.D. Va. 1998).

160. Aznul Hague & Ajay Shaw, *Throwing A ‘Spam’-Mer In The Works* - DSK Legal, Mondaq: All Regions, (Mar. 5, 2004), available at http://www.mondaq.com/;_article.asp_Q_article;d_E_24515 (last visited April 3, 2005).

161. The CAN-SPAM federal statute “requires unsolicited commercial e-mail messages to be labeled (though not by a standard method) and to include opt-out instructions and the sender’s physical address. It prohibits the use of deceptive subject lines and false headers in such messages. David Sorkin, *CAN-SPAM Act of 2003* (S. 877), available at <http://www.spamlaws.com/federal/summ108.html#s877> (last visited Feb. 16, 2005). The FTC is authorized (but not required) to establish a “do-not-email” registry. *Id.* “State laws that require labels on unsolicited commercial e-mail or prohibit such messages entirely are pre-empted, although

mail recipients to “opt-out” of receiving unwanted commercial e-mail by sending notice to the e-mailer. In contrast, the Europeans have an opt-in approach placing the burden on the commercial e-mailer to obtain consent before sending bulk e-mails. An alliance of America’s four leading e-mail and Internet service providers filed CAN-SPAM Act enforcement actions against hundreds of large-scale spammers in March of 2004.¹⁶²

In the United States, large Internet service providers deploy tort theories such as the trespass to chattels to restrain unsolicited, bulk e-mail. The first court to apply trespass to chattels to contain spam was *CompuServe v. Cyberpromotions, Inc.*¹⁶³ In that case, CompuServe filed for a preliminary injunction against Cyberpromotions, a bulk e-mailer. The *CompuServe* court ruled that there is no First Amendment constraint on applying the tort of trespass to chattels to enjoin spam.¹⁶⁴

In *America Online, Inc. v. LCGM* widespread spamming was held to be a trespass to chattels as well as a violation of the Computer Fraud and Abuse Act and a trademark violation.¹⁶⁵ In many of the U.S. spamming cases, the courts awarded damages as well as injunctive relief under causes of action based upon personal property torts. In *American Online, Inc. v. Nat’l Health Care Disc., Inc.*,¹⁶⁶ the court found the commercial e-mail actions to constitute trespass to chattels as well as a violation of state and federal computer abuse laws as well other causes of action. The court calculated damages by charging the spammer \$2.50 per thousand messages for a total of \$337,500.

The state of Virginia’s heavy cybertort caseload is primarily due to America Online’s filing of hundreds of anti-spam cases in the Northern District of Virginia, its venue of choice.¹⁶⁷ AOL files these

provisions merely addressing falsity and deception would remain in place. The CAN-SPAM Act takes effect on January 1, 2004.” *Id.*

162. Press Release, *America Online, Earthlink, Microsoft and Yahoo! Team up to File First Majority Industry Lawsuit Under New Federal Anti-Spam Law* (Mar. 10, 2004), at http://media.aoltime Warner.com/media/newmedia/cb_press_view.cfm?releae_num=55253838 (last visited Feb. 13, 2005).

163. 962 F. Supp. 1015 (S.D. Ohio 1997).

164. *Id.* The rationale was that CompuServe was not a state actor and therefore the First Amendment did not apply to private Internet service providers. *Id.* at 1026.

165. 46 F. Supp. 2d 444 (E.D. Va. 1998).

166. 174 F. Supp. 2d 890 (N.D. Iowa 2001).

167. Dozens of anti-spam cases filed in the Eastern District of Virginia are reported in America Online’s legal Web site, at

cases under the theory that the spammers are trespassing on their Web sites by exceeding the ISP's terms of service.¹⁶⁸ Anti-spam remedies vary significantly across the countries connected to the Internet.¹⁶⁹ The European Parliament has adopted a Directive on unsolicited commercial e-mail that is diametrically opposed to the U.S. approach. Under the European directive, consumers will not receive spam unless they "opt in" or agree to receive it. Commercial e-mail cannot be sent without evidence that the consumers requested the receipt of the Internet communication.

The European E-Commerce Directive requires ISPs to implement policies designed to track down spam e-mailers by requiring them to provide contact information such as a verifiable business address and other authenticating information.¹⁷⁰ Austria, Denmark, Finland, France, Germany, Greece, Hungary, Italy Norway, Poland, and Romania had all adopted national anti-spam legislation by 2003.¹⁷¹ The European Commission's Directive on Privacy and Electronic Communications applies to unsolicited e-mail sent to residents of all European countries.¹⁷² Other anti-spam initiatives include the Commissions Directives on Misleading Advertising,¹⁷³ E-Commerce

<http://legal.web.aol.com/decisions/dljunk/johndoes1-40.html> (last visited April 15, 2005).

168. See, e.g., *America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444 (E.D. Va. 1998).

169. The Ontario Superior Court of Justice in *1267623 Ontario, Inc. v. Nexx Online, Inc.*, [1999] O.J. No. 2246, Court File No. C20546/99 (June 14, 1999) (ruling that spamming breached "netiquette" justifying the termination of Internet service).

170. Cliff Saran & Daniel Thomas, *IT Directors Face Challenge as E-Commerce Directive Becomes Law*, IT Management: E-Business (Aug. 21, 2002), at <http://www.computerweekly.com/Article115154.html> (last visited Feb. 15, 2005).

171. Digital Civil Rights in Europe, *Update on Anti-Spam Legislation* (March 12, 2003), at <http://www.edri.org/edriagram/number4/spam> (last visited Feb. 15, 2005).

172. The Directive on Privacy and Electronic Communications "extends controls on unsolicited direct marketing to all forms of electronic communications including unsolicited commercial e-mail (UCE or Spam) and SMS to mobile telephones; UCE and SMS will be subject to a prior consent requirement, so the receiver is required to agree to it in advance, except in the context of an existing customer relationship, where companies may continue to email or SMS to market their own similar products on an 'opt-out' basis." Euro News, *Newsletter of the UK Network of Euro Info Centres, Spam: The Factsheet* (Aug. 2004), at <http://www.waleseic.org.uk/euronews/july2004/article3.htm> (last visited Feb. 15, 2005).

173. Directive 84/450 on Misleading Advertising.

Directive¹⁷⁴ and the Data Protection Directive.¹⁷⁵

The Europeans have adopted a more consumer-friendly approach to regulating spam than the United States' deference to free market principles. In a Dutch case, XS4ALL, an Internet service provider, sued a commercial e-mailer for sending its subscribers massive quantities of unsolicited bulk e-mail.¹⁷⁶ The lawsuit alleges violations of the EU Personal Data Protection Act, the Dutch Telecommunications Act, as well as invasion of privacy and trademark infringement. XS4ALL is seeking an injunction to force Abfab to 1) cease infringing on XS4ALL's trademark and 2) adopt a policy whereby Internet users must affirmatively "opt-in" before they are sent spam.¹⁷⁷ The Advocate General has recommended that the Dutch Supreme Court sustain a Court of Appeals judgment against the spammer. "The Lower House of the Dutch Parliament has recently given its agreement to a legal ban on spam which looks set to come into force within a few months."¹⁷⁸

The Court of Rotterdam held that a spammer using a Web site was "bound by the site's terms and conditions even if the user has not accepted them before entering the site."¹⁷⁹ The Dutch firm, Netwise, operates a free directory of e-mail addresses but stipulates the terms and conditions of use.¹⁸⁰ The spammer accessed the Web site's registry without clicking agreement to the terms and conditions but was still held liable for violating the terms of usage.¹⁸¹

The court reasoned that there was an implied contract since "registries of this sort generally do not allow their email addresses to be used for spam."¹⁸² In a similar case, a French court ruled that ISPs

174. E-Commerce Directive, 2000/31.

175. Data Protection Directive 95/46.

176. XS4ALL News, XS4ALL and Spam, *Latest News, Recommendation to the Supreme Court in AbFab Case: Xs4All Can Defend Itself Against Spammers* (Nov. 19, 2005), at http://www.xs4all.nl/uk/news/overview/spam_e.html (last visited Feb. 8, 2005) (noting that the "Advocate General, in certain cases XS4ALL does not have an obligation to convey e-mail, 'if XS4ALL puts forward sufficiently legitimate reasons for taking such a decision, and the decision is based on a reasonable assessment of the interests involved'").

177. *Id.*

178. *Id.*

179. Perkins Coie, Internet Law Digest, *Netwise v. NTS, Court of Rotterdam* (Netherlands, 2003), available at

http://www.perkinscoie.com/casedigest/icd_results.cfm?keyword1=international&opic=International (last visited Feb. 8, 2005).

180. *Id.*

181. *Id.*

182. *Id.*

had the right to terminate the accounts of abusive spammers. The judge ruled that “spamming is contrary to the Internet community’s codes of conduct and allowed the ISP to block the customer’s access.”¹⁸³ This is diametrically opposed to the American “opt out” approach where consumers receive commercial e-mail unless they request not to receive it. The difference between opt-in or opt-out regimes is so fundamental that it is certain to create cross-border conflicts.

[D] Conflicting Online Intermediary Law

The Electronic Commerce Directive “seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States.”¹⁸⁴ The purpose of the Directive is to create legal framework ensuring “the free movement of information services.”¹⁸⁵ Member States are required to develop national legislation implementing the E-Commerce Directive.¹⁸⁶ Article 9 of The Electronic Commerce Directive affirms Member States’ obligation to remove obstacles to the use of electronic contracts.¹⁸⁷ The Directive also covers topics such as the liability of intermediary service providers, unsolicited commercial e-mail, and the prohibition of Internet-related surveillance.¹⁸⁸

This legal regime institutes ISP liability rules not only for torts but also for all types of illegitimate activities in cyberspace that are “initiated by third parties on-line (e.g. copyright piracy, unfair

183. Perkins Coie, *Internet Case Digest*, at http://www.perkinscoie.com/casedigest/icd_results.cfm?keyword1=international&topic=International (last visited Feb. 8, 2005).

184. *Id.* at Art. 1.

185. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

186. In addition, Member States are required to enact enabling legislature to enact Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for Electronic Signatures, 2000 O.J. (L.13) 12 (“Digital Signatures Directive”). The Digital Signature Directive validates and develops legal infrastructure for electronic signatures. *Id.*

187. Directive 2000/31/EC, art. 9 of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information services, in particular electronic commerce, in the Internal Market, 2000 O.J. (L.178) 1, 11.

188. Directive 2000/31/EC, 2000 O.J. (L.178) 1.

competition, misleading advertising).”¹⁸⁹ The European Union’s Electronic Commerce Directive’s “notice, take-down and put-back” regime¹⁹⁰ would compel an ISP to remove tortious or other objectionable material. The Directive supplements national takedown policies already in force in some European countries.¹⁹¹ Tennis star Steffi Graf, for example, prevailed in a lawsuit against Microsoft after the Internet Service Provider refused to remove doctored digital images of her in pornographic poses on its “Celebrities” chat room.¹⁹²

The *Graf* court found Microsoft to be “responsible for the content posted to its server because it provided the infrastructure, established the topic, permitted the posting over its own Web pages, and established the basic rules.”¹⁹³ In the United States, Section 230 of the Communications Decency Act (CDA)¹⁹⁴ would have immunized Microsoft for merely permitting a posting on its services.¹⁹⁵ Similarly, in *Godfrey v. Demon Internet*,¹⁹⁶ a service provider claimed it was entitled to an innocent disseminator defense under the United Kingdom’s 1996 Defamation Act. The court stripped the ISP

189. European Parliament, *Liability for Online Content: What has the E-Commerce Directive Achieved?* (July 10, 2002), available at <http://www.eping.org/minutes10072002.html> (last visited Feb. 12, 2005).

190. “It must also be kept in mind that the Directive only provides for a system of liability exemptions for ISPs. Thus, if an ISP does not qualify for an exemption under the Directive, its liability will be determined by the national laws of the respective Member States.” Pablo Asbo Baistrocchi, *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce*, 19 SANTA CLARA COMPUTER & HIGH TECH. L.J. 111, 118 (2002).

191. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’) Official Journal L 178, 17/07/2000 P. 0001 – 0016. Cf. *Action Internationale pour la Justice v. Societe General Communications Inc.* (France 2001) (refusing to compel ISP to takedown racist material), available at http://www.perkinscoie.com/casedigest/icd_results.cfm?keyword1=international&opic=International (last visited Feb. 9, 2005).

192. *Graf v. Microsoft GmbH, OLGZ Cologne*, No. 15 U 221/01 (Germany 2002), available at http://www.perkinscoie.com/casedigest/icd_results.cfm?keyword1=international&topic=International (last visited Feb. 10, 2005).

193. *Id.*

194. 47 U.S.C. § 230 (2000).

195. 47 U.S.C. § 230(c)(1) (2000).

196. Q.B. No. 1998-G-No. 30, March 26, 1999 (London High Court, United Kingdom, March 26, 1999), available at http://www.perkinscoie.com/casedigest/icd_results.cfm?keyword1=international&opic=International (visited Feb. 10, 2005).

of its immunity since it did not take down defamatory material even after being notified three times.¹⁹⁷ In the United States, no court has held a service provider liable for failing to expeditiously remove defamatory material. In this British case, the ISP settled the defamation claim for approximately “\$25,000 in damages plus plaintiff’s costs and fees (likely to be several hundred thousand dollars).”¹⁹⁸

In *Lefebure v. Lacambre*,¹⁹⁹ a French court found an ISP liable for publishing erotic images of the plaintiff on its Web site. “Under French law, an Internet Service Provider is responsible for the morality of the content distributed via the client-operated Web sites it hosts, and may be liable for violations of privacy.”²⁰⁰ The French plaintiff contended that “the ISP violated her privacy and damaged her professional reputation by allowing a subscriber to publish nude photographs of her on a Web site.”²⁰¹ The French court ordered the offending Web site be shut down under the threat of a fine of 100,000 francs per day.²⁰²

In contrast, American online intermediaries enjoy what is, in effect, an absolute immunity for content posted by third parties and have no obligation to remove objectionable material. Congress expressly provided ISPs with protection from online defamation claims for publisher’s liability when it enacted Section 230 of the Communications Decency Act of 1996 (CDA).²⁰³ Congress did not

197. *Id.*

198. *Id.*

199. Tribunal de Grande Instance de Paris, Ref. 55181/98, No. 1/JP (France, June 9, 1998), *available at*

http://www.perkinscoie.com/casedigest/icd_results.cfm?keyword1=international&topic=International (visited Feb. 8, 2005).

200. *Id.*

201. *Id.*

202. *Id.*

203. “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” 47 U.S.C. § 230 (c)(1) (2000). Section 230 was enacted as part of the Telecommunications Act of 1996 (Telecommunications Act) in order to protect minors from ‘indecent’ and ‘patently offensive’ communications on the Internet. *Id.* Title V of the Telecommunications Act of 1996, Pub. L. No. 104-104, is known as the Communications Decency Act (CDA). The primary goal of the CDA was to control the exposure of minors to indecent material. See Pub. L. No. 104-104, Title v. (1996); see also H.R. Rep. No. 104-458, at 81-91 (1996); S. Rep. No. 104-230, at 187-193 (1996); S. Rep. No. 104-23, at 9 (1995). Section 230 of the CDA states that providers and users of interactive computer services shall not be treated as publishers of any information provided by another information content provider.

address the larger question of whether ISPs were also immunized from online defamation liability when they are acting as mere distributors of defamatory statements. American courts have stretched the CDA to abolish ISP's common law liability as distributors even when ISPs know or have reason to know of the underlying defamatory content.²⁰⁴

PART III: TOWARDS A HARMONIZED CYBERTORT REGIME

Internet law must become a moving stream rather than a stagnant pool, evolving to meet the new risks and dangers in the twenty-first century's age of information.²⁰⁵ Further harmonization between Europe and America is essential to surmount the growing substantive and procedural barriers²⁰⁶ to cross-border Internet-related tort

Finally, Section 230 authorizes providers and users of interactive computer services to remove or restrict access to inappropriate materials without being classified as publishers. 47 U.S.C. § 230 (2000).

204. See Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335 (2005).

205. Professor Thomas Lambert, Jr., frequently used the image of tort as a moving stream contrasted to a stagnant pool. This metaphor applies equally well to the evolving common law in cyberspace. However, it will be difficult to harmonize cybertort law. "Harmonization has proven difficult enough even in relatively uncontroversial areas like trademark law, however. It may well be impossible to harmonize laws where there is less agreement on principles among nations—laws relating to free speech...The prospect of being subject to litigation in a number of different countries is likely to be extremely daunting to individuals and even small and medium-sized businesses." MARK LEMLEY, ET AL., *SOFTWARE AND INTERNET LAW* 617 (2003)

206. For example, the Anti-Cybersquatting Consumer Protection Act (ACPA) recognizes an *in rem* remedy useful in obtaining jurisdiction over foreign defendants. The Fourth Circuit affirmed the lower court's dismissal of the automobile manufacturer's *in rem* action in *Porsche Cars N. Am, Inc. v. Porsche.net*. 2002 U.S. App. 17531 (4th Cir., Aug. 23, 2002). On February 23, 2001, the Virginia district court found that it had jurisdiction over the British domain names under the ACPA. Just three days before the scheduled trial in Virginia, the owner of the British domain names notified the court that their registrant had decided to submit to personal jurisdiction in California. The district court ruled that *in rem* was lost as the result of the registrant's action. The circuit court disagreed ruling that Porsche.net waited too long to object to *in rem* jurisdiction. If it did, *in rem* jurisdiction could be lost even long after a court has made the requisite statutory finding. The Fourth Circuit vacated the district court's order dismissing the case and remanded for consideration of the ACPA, without reaching the question of whether there was a basis for *in rem* jurisdiction premised by Porsche's trademark-dilution claims. Since the Porsche.net case, courts have seldom found for the plaintiff in ACPA *in rem* cases. In many cases, the plaintiff's

litigation.²⁰⁷ Global Internet law must develop effective mechanisms to facilitate cross-border enforcement of national judgments. Just as the leading Western nations cooperated to create a unified law of the sea,²⁰⁸ advances in cyberspace technology are creating international problems that need to be addressed through a coherent cross-national legal regime.

Internet law must harmonize but not homogenize procedural and substantive tort principles.²⁰⁹ In 1982, the United Nations

attorney failed to comply with the statutory requirements of the ACPA by filing in the wrong federal district court.

207. In *Int'l Bancorp, L.L.C. v. Societe Des Bains De Mer Et Du Cercle Des Etrangers*, a Monaco trademark infringement action involved the plaintiff Casino de Monte Carlo against off-shore defendants who had registered 53 “.com” and “.net” domain names that incorporated, in various ways, the name “Casino de Monte Carlo.” 192 F. Supp. 2d 467 (E.D. Va., 2002). The plaintiff claimed that the companies’ use in American commerce of the term “Casino de Monte Carlo” in the disputed domain names and on various Web sites constituted trademark infringement in violation of the Lanham Act. *Id.* The court concluded that the companies’ use of 43 domain names created a likelihood of confusion because the plaintiff’s mark had secondary meaning.

208. Tommy Koh, *A Constitution for the Oceans*, available at http://www.un.org/Depts/los/convention_agreements/convention_overview_convention.htm (visited Feb. 15, 2005).

209. Europe’s community wide products liability law contains a variety of national variations responsive to local conditions, which is like the law of torts in the various U.S. states. In products liability actions in Portugal, for example, the Public Prosecutor’s Office and consumers’ organizations may intervene in private proceedings over product injuries that have a public interest. European Commission, Report from the Commission on the Application of Directive 85/374 on Liability for Defective Products (Jan 31, 2001) (COM/2000/0893 final). In Austria, a private plaintiff may elect to pass “his/her liability claim to a consumers’ association.” *Id.* “In Belgium, plaintiffs with similar but separate claims can institute proceedings before the same court and then ask the court to handle their claims at the same hearing, without joining them.” *Id.* Greece has a mechanism to permit products liability actions on behalf of consumer groups as does Denmark. *Id.* While there are no class actions in France for mass products liability actions, there is a provision for enabling consumer associations to collectively defend consumers. *Id.* “In Germany, in the event of a series of accidents, there is a ‘trial action which will subsequently form the basis of compensation between industry and the injured persons.’” *Id.* “In Ireland, the rules of court provide a procedure whereby one or more of persons having the same interest in a single claim may bring or defend the claim on the behalf of all those interested.” *Id.* Italy is an exception to the general rule that consumers’ associations “can act on behalf of injured persons.” *Id.* The divergent procedural devices for joining claims share much common ground even though they may differ in form. *Id.*

Convention on the Law of the Sea²¹⁰ produced the first international agreement on developing principles of navigation, conservation, pollution, transit passage, and marine scientific research.²¹¹ This Treaty, signed by 147 nation states, resolved the “plethora of conflicting claims by coastal States...with universally agreed limits on the territorial sea.”²¹² A Treaty for Cyberspace could be modeled on the mandatory system of dispute settlement adopted for the Law of the Sea.²¹³ No elegant utopian solution to the conflicting procedural and substantive tort law is likely to ever emerge. Any convention on cybertorts will not satisfy the interests and objectives of every interest group in the United States and Europe.

Travelers on the World Wide Web require uniform procedural and substantive remedies for cross-border civil wrongs. Similarly, the international business community will be handicapped if it is subject multiple conflicting procedural and substantive ground rules. Cross

210. “The United Nations Convention on the Law of the Sea was opened for signature at Montego Bay, Jamaica, on 10 December 1982. It entered into force 12 years later, on 16 November 1994. A subsequent Agreement relating to the implementation of Part XI of the Convention was adopted on 28 July 1994 and entered into force on 28 July 1996. This Agreement and Part XI of the Convention are to be interpreted and applied together as a single instrument.” International Tribunal for the Law of the Sea, *Overview*, at http://www.itlos.org/start2_en.html (last visited Feb. 14, 2005).

211. Koh, *supra* note 208.

212. *Id.*

213. “Part XV of the Convention lays down a comprehensive system for the settlement of disputes that might arise with respect to the interpretation and application of the Convention. It requires States Parties to settle their disputes concerning the interpretation or application of the Convention by peaceful means indicated in the Charter of the United Nations. However, if parties to a dispute fail to reach a settlement by peaceful means of their own choice, they are obliged to resort to the compulsory dispute settlement procedures entailing binding decisions, subject to limitations and exceptions contained in the Convention. The mechanism established by the Convention provides for four alternative means for the settlement of disputes: the International Tribunal for the Law of the Sea, the International Court of Justice, an arbitral tribunal constituted in accordance with Annex VII to the Convention, and a special arbitral tribunal constituted in accordance with Annex VIII to the Convention. A State Party is free to choose one or more of these means by a written declaration to be made under article 287 of the Convention and deposited with the Secretary-General of the United Nations (declarations made by States Parties under article 287). If the parties to a dispute have not accepted the same settlement procedure, the dispute may be submitted only to arbitration in accordance with Annex VII, unless the parties otherwise agree. *International Tribunal for the Law of the Sea, Overview* http://www.itlos.org/start2_en.html (last visited Feb. 14, 2005).

national trade requires a large degree of legal uniformity, settled expectations about the rules of commerce and the process by which those judgments are enforced.

[A] Doing Nothing Is Not a Realistic Option

Judge Frank Easterbrook sees no urgency in harmonizing either the procedural or substantive Internet law. He argues that Internet law is nothing more than everyday cases whose only common element is the incidental use of a new technology.²¹⁴ In Easterbrook's opinion, devoting time and effort to studying "the law of the Internet" makes as much (or as little) sense as studying "the law of the horse."²¹⁵ He explains that: "Lots of cases deal with sales of horses; others deal with people kicked by horses; still more deal with the licensing and racing of horses, or with the care veterinarians give to horses, or with prizes at horse shows. Any effort to collect these strands into a course on 'The Law of the Horse' is doomed to be shallow and to miss unifying principles."²¹⁶

Judge Easterbrook concludes that Internet law is not a proper subject for empirical study and that we should "let the world of cyberspace evolve as it will, and enjoy the benefits."²¹⁷ Similarly, Joseph Sommers contends that "[e]ven if the Internet or personal computer has the promised transformative social impact, they are unlikely to generate a characteristic body of law."²¹⁸ Scholars such as Lawrence Lessig strongly disagree, arguing that there is a compelling reason to understand "how law and cyberspace connect."²¹⁹ We support this position. The governance of the Internet is too central to the future of the world economy to sit by idly while cyberspace law "evolves as it will."

A focus on the unique features of Internet Law is justified by the enormous impact of cyberspace on everyday life. "Our transformation from a non-computerized world to one in which virtually all business, professional and entertainment activities are

214. Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207.

215. *Id.* at 208.

216. *Id.* at 207.

217. *Id.* at 216.

218. Joseph H. Somers, *Against Cyberlaw*, 15 BERKELEY TECH. L.J. 1145, 1155 (2000).

219. Lawrence Lessig, *Commentary: The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 502 (1999); see also LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* (1999).

influenced, if not dominated, by electronic information systems occurred rapidly.”²²⁰ Hardly a day goes by without a court decision extending traditional civil law to adjudicate a cyberspace dispute. Cyberspace is too important, both economically and culturally, to simply allow market forces to shape its development.

[B] Eliminating Procedural Barriers for Cybertort Adjudication

[1] American Law Institute/UNIDROIT Transnational Civil Procedure

The traditional principles underlying jurisdiction, which have been based upon the “exercise of physical coercive control over that territory by the sovereign,” are becoming obsolete in a networked world.²²¹ The rules for transnational jurisdiction for the countries connected to the Internet have yet to be formulated.²²² The American Law Institute and UNIDROIT have drafted a promising proposal for forging new Principles and Rules of Transnational Civil Procedure.²²³ While these principles have yet to be finalized or adopted by any country, they serve as a possible model for harmonizing cyberlaw procedure.

The model ALI/UNIDROIT statute proposes four bases for asserting transborder jurisdiction: (1) designation by mutual agreement of the parties; (2) in which a defendant is subject to the compulsory judicial authority of that state, as determined by principles governing personal jurisdiction or by international convention to which the state is a party; or (3) where fixed property is located; or (4) in aid of the jurisdiction of another forum in which a Transnational Civil Proceeding is pending.²²⁴ These rules have the virtue of being generally accepted principles for jurisdiction in both

220. Raymond T. Nimmer & Patricia Krauthaus, *Electronic Commerce: New Paradigms in Information Law*, 31 IDAHO L. REV. 937, 937 (1995).

221. Henry Perritt, *Traditional Legal Concepts: Basics from Three Experts*, ILPF, 1999 Annual Conference, Jurisdiction: Building Confidence in a Borderless Medium, Montreal, Canada (July 26, 1999), available at <http://www.ilpforg/events/jurisdiction/transcript/conf99d1.htm> (last visited Feb. 23, 2005).

222. See Jean Eaglesham, *Laying Down Cyberlaw*, FINANCIAL TIMES (LONDON), June 23, 1999, at 22 (discussing absence of uniform Internet rules).

223. American Law Institute, ALI/UNIDROIT Principles and Rules of Transnational Civil Procedure (Discussion Draft No. 2, Apr. 12, 2001) (draft circulated by ALI Council for discussion and comment).

224. *Id.*

the U.S. and Europe.

[2] *Brussels Regulation*

Another possible approach to jurisdiction would be for the United States to enter into a treaty with the European Community countries, which would make the Brussels Regulation the prevailing rule. The Brussels Regulation generally endorses a freedom of contract in commercial contracts, but provides special protections for consumers.²²⁵ American consumers would greatly benefit from the Brussels regulation because it designates the choice of law, choice of forum and jurisdiction as the consumer's home court.²²⁶ U.S. companies operating in any country of the European Union are already subject to the Brussels Regulation's consumer rule. An American company domiciled in a Member State can be sued in that state. American online providers have been steadfastly opposed to the Brussels Regulation because they favor mass-market licenses, which require consumers to litigate in their home court and according to their rules.²²⁷

[3] *The Hague Convention on Jurisdiction and Foreign Judgments*

Delegates to the Hague Convention on Jurisdiction and Foreign

225. "Under the Convention one of the main exceptions applies to consumer contracts. If certain conditions are fulfilled they are permitted to sue suppliers in their own courts instead of the supplier's courts. The exception takes precedence over any terms included in the contract to the contrary and it cannot be excluded. Article 13 of the Brussels Convention defines a 'Consumer Contract' as including the supply of goods or services where: In the consumer's home state, the conclusion of the contract was preceded by a specific invitation addressed to him or by advertising; and the consumer took the steps necessary to conclude the contract in the consumer's home state." *Where Can We Be Sued? - The Implications Of The New Jurisdiction Rules Under The Brussels Regulation For Online Consumer Contracts*, MODAQ, Dec. 21, 2001.

226. The Brussels Regulation gives consumers the right to sue suppliers in their country of residence if a business "pursues commercial or professional activities in the Member State of the consumer's domicile." Brussels Regulation, *supra* note 62, at art. 15(1). In tort, delict, or quasi-delict litigation, a person domiciled in a Contracting State may be sued in the jurisdictions where the harm took place. Brussels Regulation, *supra* note 62, at art. 5(3).

227. "Business would like to keep the 'freedom of contract' as open as possible," ...a battle that was "lost" when the Brussels Regulation on jurisdiction, recognition and enforcement of judgments in civil and commercial matters was approved late in 2000. The Brussels Regulation "created a very big fuss in the online community." European Commission Eyes Revamp of Contract Law Treaty, 4 WASHINGTON INTERNET DAILY 1, Jan. 15, 2003.

Judgments in Civil and Commercial Matters are in the process of drafting transnational rules to resolve jurisdictional clashes and provide more certainty in the enforcement of judgments.²²⁸ The delegates have drafted a proposed regime that would address many of the cross-border issues that impact electronic commerce. The Hague Convention will apply to most civil and commercial judgments but does not address disputes over revenue, customs, or administrative matters covered by other bodies of law.²²⁹ The proposed Convention provides that if a court has jurisdiction, it has exclusive jurisdiction in order to avoid parallel proceedings.²³⁰ A court is expected to exercise comity if another court has exercised jurisdiction.²³¹ As with the Brussels Regulation, the Convention permits parties to choose their own forum.²³²

If the exclusive forum is in a nation state that is not a Hague Convention signatory, courts in contracting states should either decline jurisdiction or suspend proceedings.²³³ The Hague Convention applies to a wide range of substantive fields in nearly every civil and commercial substantive field. This Convention mirrors the Brussels Regulation in favoring mandatory rules that protect consumers.²³⁴ While the Convention enforces a broad range of judgments, it gives courts the discretion not to enforce judgments considered to be “manifestly incompatible with that country’s public policy.”²³⁵ American companies and a number of other Internet stakeholders oppose the United States becoming a signatory to the Convention.²³⁶ Commercial entities, however, will benefit by being

228. RUSTAD & DAFTARY, E-BUSINESS LEGAL HANDBOOK, *supra* note 152, at § 8.02[C].

229. Civil Law, *RAPID: Commission of The European Communities*, Doc:00/33 (Dec. 20, 2000).

230. Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters at Art. 4(1).

231. *Id.*

232. *Id.*

233. *Id.*

234. RUSTAD & DAFTARY, E-BUSINESS LEGAL HANDBOOK, *supra* note 152, at 8-49.

235. Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters, *supra* note 228, at Art. 28(f).

236. “Several trade associations representing Internet service providers issued an open letter to delegates who are drafting an international convention on the jurisdiction over and enforcement of foreign judgments, including those in e-commerce. The groups object to language that they argue is unnecessarily vague and would adversely impact their member companies.” *Internet Providers*

able to file suit against defendants in the plaintiff's country of habitual residence, assuming there is no choice of law or forum clause in their contracts.²³⁷

[C] Harmonizing Substantive Cybertort Law

Europe's community-wide directive and convention approach is one possible model for harmonizing substantive Internet law. Directives have the virtue of creating uniformity in terms of basic principles, while permitting local variations to be incorporated into the law. As a result, each Member State of the European Community follows a dual system of regulation: European-wide rules and national variants.²³⁸ European Union regulations tend to be more rule-oriented than U.S. law, which results in less indeterminacy.

The purpose of uniform laws throughout Europe is to facilitate commerce and reduce transaction costs in cross-border e-commerce. Directives are formulated by the European Commission and finalized by the European Parliament and the Council. The United States is experimenting with adopting some features of European cyberspace law. America, for example, has joined eleven European nations in a pilot project to use ombudsmen to mediate Internet disputes.²³⁹ The Consumer Ombudsman will monitor the development of consumer problems connected with electronic commerce and work together with officials in other countries to develop common solutions.²⁴⁰

Europe is also importing some American tort remedies. The European Commission's Products Liability Directive is inspired in

Challenge Parts of Jurisdiction; Treaty, NATIONAL JOURNAL'S TECHNOLOGY DAILY (Dec. 5, 2003).

237. Article 2 defines the habitual residence. *Id.* at Art. 3(2)(a)(d). The test for a habitual residence of a corporation is multi-factorial, including variable such as where it has its statutory seat, where it was incorporated, where it has central administration, or its principal place of business. *Id.*

238. When an EU Directive is approved, each of the Member States must enact legislation implementing a directive, generally within a three-year period. One of the difficulties of complying with European contract law is that each country must enact national legislation that adapts the directive to its local legal culture.

239. "eConsumer.gov is a joint project arranged by the International Marketing Supervision Network, IMSN, which includes authorities in the OECD countries." See Federal Trade Commission, FTC Announcement of e-Consumer Government, at http://www.usembassy.it/file2001_04/alia/a1042615.htm (visited April 10, 2005).

240. *Id.*

large part by products liability developments in the United States.²⁴¹ The Product Liability Directive covers all “moving parts, electricity, raw materials, and components for final products, and holds the manufacturer liable for all damages. If the manufacturer cannot be identified, each supplier of the product becomes liable.”²⁴² The European Commission’s Green Paper on products liability contends that the expansion of strict products liability should be extended to all products including software and computer systems.²⁴³

Countries with intrusive content regulation could benefit from the American tradition of balancing torts against the First Amendment. The doctrines of public official, public figure, and the limited public figure that thrust speakers in the public arena will be useful legal transplants for cyberspace. European laws that require providers to take down illegal or infringing content have gone too far in limiting expression on the Internet.²⁴⁴ Similarly, international Internet law could progress by adopting tort-like concepts that permit consumers to redress injuries against powerful corporate stakeholders. The first step toward harmonizing cybertort law is to agree upon the broad principles of what constitute a legally protected interest on the Internet. Without an international agreement to protect personal, property or reputational interests, cyberwrongs will go on undeterred

241. The European Commission enacted a directive in 1985 and in 1999 it adopted Directive 99/34/EC. Since this Directive was promulgated, each of the European countries has enacted national legislation implementing these principles. “In most Member States, the national rules implementing the Directive are applied alongside other liability regulations in the majority of the cases. In Austria nearly all product liability cases are solved on the sole basis of the system provided by the Directive. Plaintiffs use other liability systems (contractual or tort law) mainly because they provide for compensation which is more protective (it covers namely damages under 500 Euro, non-material damages, damages to the defective product itself and to property intended for professional use; prescription periods are longer). In Germany case law constantly interprets applicable provisions of tort law in such a way that they come close to a no-fault based liability. Another reason for parallel application is that the ‘traditional’ legislation is better known given that settled case law exists.” Report from the Commission on the Application of Directive 85/374 on Liability for Defective Products, COM/2000/0893 final, (Jan. 31, 2002).

242. Consultants Europe and Rosalie Verhoef, *Product Liability and CE Marking*, available at <http://www.elcina.com/ce4.html> (visited Feb. 15, 2005).

243. RUSTAD & DAFTARY, *E-BUSINESS LEGAL HANDBOOK*, *supra* note 152, at 8-74.

244. MICHAEL L. RUSTAD & THOMAS H. KOENIG, *REBOOTING CYBERTORT LAW*, *supra* note 204.

and unpunished.²⁴⁵

CONCLUSION

The Internet has produced a network of “user groups, bulletin boards, and Web sites [that] have constructed a new arena wherein political and social norms are proposed, debated, and determined.”²⁴⁶ It is no exaggeration to conclude that the content on the Internet is “as diverse as human thought.”²⁴⁷ Such groundbreaking advances in communications technology have always required the reworking of legal doctrine.

Regulatory and common law once again must be fundamentally reshaped because the Internet is shattering existing precedent by redefining distance, time, privacy and the meaning of territoriality. The phenomenal growth in traffic on the World Wide Web requires that established legal principles for all branches of the law be adapted to cyberspace. In 2001, there were an estimated 149 million Internet users in the United States and more than 500 million users worldwide.²⁴⁸ By the end of 2004, the number of worldwide Internet users skyrocketed to 6.4 billion.²⁴⁹ A decade ago, the U.S. dominated the Internet, but today only one in four Internet users are North

245. One possible model is a Convention on Cybertorts that parallels cybercrimes. See *Convention on Cybercrime*, ETS No. 185, available at <http://conventions.coie.int/Treaty/en/Reports/HTML/185> (last visited Feb. 12, 2005). See generally Michael L. Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier*, 11 S. CAL. INTERDIS. L.J. 63 (2001) (discussing proposed Cybercrime Convention).

246. Julie Mertus, *From Legal Transplants to Transformative Justice: Human Rights and the Promise of Transnational Civil Society*, 14 AM. U. INT’L L. REV. 1335, 1349 (1999).

247. *American Civil Liberties Union v. Reno*, 929 F. Supp. 824, 830 (E.D. Pa. 1996).

248. Computer Industry Almanac, Inc., *Internet Users Will Top 1 Billion in 2005; Wireless Internet Users Will Reach 48% in 2005*, available at <http://www.c-i-a.com/pr032102.htm> (last visited Jan. 22, 2005).

249. The highest rates of Internet usage growth are occurring in the less developed world. The Middle East leads the world in the percentage increase of new Internet users from 2000-2004. Internet Usage and Population Statistics, *Internet Usage Statistics: The Big PictureWorld*, available at <http://www.internetworldstats.com/stats.htm> (last visited Feb. 1, 2005). The number of new Internet users in Latin America more than tripled during the past five years. Africa had the third largest increase of 187% followed by Asia (126%) Europe (124%), Oceania/Australia (107%), and North America (106%). *Id.*

Americans.²⁵⁰ Judge Easterbrook's advice to simply ignore cyberspace law is unrealistic in the borderless Internet economy. We cannot simply enjoy the benefits of cyberspace without participating in global Internet law harmonization. The stakes are simply too high.

250. The continents of Europe and Asia each have substantially more Internet users than North America. *Id.*