ARTICLES

A HYBRID MODEL OF SELF-REGULATION AND GOVERNMENTAL REGULATION OF ELECTRONIC COMMERCE

Timothy D. Casey and Jeff Magenau †

I. INTRODUCTION

The world is rapidly moving towards an age of ubiquitous globally networked communications; not just communications between and among persons, but also between the electronic devices that serve them; not just between particular government leaders, but among the vast databases and other sources of information upon which regulatory regimes depend; and not just between parties to a transaction, but among the instruments of entire economies.

Eventually, terms such as "e-commerce" will become meaningless distinctions—just as we would not today refer to business conducted over the telephone as "telephone commerce." As communications and commerce and inter-governmental regulatory and law enforcement efforts conducted over networks become commonplace, the notion that government has no role to play will begin to fade. Just as the "Wild, Wild, West" of 19th century America eventually needed a sheriff to establish order, secure the people's safety, and foster predictability for business, so too will the idea of a "lawless" Internet—upon which the networked communications at issue here are currently and may always be based—seem in retrospect a shortsighted and naive concept.

† Tim Casey is a partner and Jeff Magenau is an associate in the Intellectual Property Technology Transactions and Services practice group at Fried, Frank, Harris, Shriver & Jacobson in Washington, D.C. and New York, N.Y. We are grateful to several associates and law clerks at Fried Frank who conducted virtually all of the research for and prepared early drafts of this article. In particular, we would like to thank Andrew Olek, Angela Angelovska-Wilson, Kimberly Wade, and Jane Reynolds.

Having said that, the characteristics of the Internet and other data networks, such as their architectures, render them uniquely resistant or ill-suited to the wholesale application of existing rules and regulations. For one thing, such networks scale to virtually limitless proportions; the space of "cyberspace" is essentially infinite. As such, limited resources, a driving force behind many regulatory regimes, is effectively inapplicable. For another thing, the lack of a significant, more-or-less permanent physical presence—or at least the widely distributed "locations" of content and activity on data networks (e.g., computer hard drives and servers)—raises fundamental, perhaps insurmountable difficulties for the traditional application of jurisdictional principles and enforcement mechanisms.

This article argues that in order to foster business certainty, service providers need to continue investing in network infrastructure and applications, and that a global legal regime that harmonizes the imposition of civil and criminal liability is required. Under existing laws, the "facilitators" of criminal or injurious activity engaged in by others may be held indirectly responsible for such activity in certain situations. As illegal or harmful content or activity moves to data networks (hereinafter referred to as the "Internet"), the difficulty in identifying and accessing the actual perpetrators of criminal or injurious activity gives rise to calls from governments, intellectual property owners, victims of crimes and others to hold Internet service providers responsible for the infringement of the rights of others. The unapologetic aim of placing such a burden on service providers is to encourage them to stop, or control, the illicit activity.

We argue that, in fact, the imposition of overly burdensome regulation or legal liability will instead encourage service providers to reduce investment in infrastructure and new services, or charge more for the services they do provide. Nevertheless, we feel—and recent history supports the notion—that a certain level of regulation and legal liability for acts of third parties is inevitable for service providers.[1] Thus, a regime in which service providers and others know the ground rules, and which largely leaves procedural implementation of legal requirements to service providers, can foster an environment which provides business certainty and remedies for injured parties that is acceptable to all. The service provider liability

1. Among the U.S. laws that to some extent impose and/or qualify liability on Internet service providers are the Digital Millennium Copyright Act of 1998, the Children's Online Privacy Protection Act and the Child Online Protection Act.

provisions of the Digital Millennium Copyright Act of 1998 ("DMCA")[2] have generally been successful in this respect.

We note that the elemental framework of the DMCA has found its way to other proposed federal legislation dealing with service provider liability in the U.S. Congress and in the European Union's regulatory bodies. With that as a starting point, we argue that the imposition of liability for service providers around the world should be harmonized, to the extent possible, both with respect to jurisdiction and type of content or activity.

In order to derive lessons from history and to develop workable models by analogy, we first look at prior and current responses to the development of other new technologies and assess the advantages and drawbacks of those responses.

II. RESPONSE TO OTHER NEW TECHNOLOGIES

Technological change has always been a source of problems that the regulatory and judicial systems have had to address. The development of the printing press, and the idea of education becoming available for the populace, caused Queen Elizabeth to establish the Stationers Charter in a largely successful effort to regulate the dissemination of ideas. Rapid advancements in technology elicited similar responses in the 19th century. Faced with a confusing array of new communication technologies, courts selected analogies to resolve doubtful legal issues and to establish legal treatment for each new technology. For example, the telegraph was compared and analogized to prior methods of common carriage, and the telephone thereafter compared to the telegraph. A century later the technologies of the telephone, motion pictures and broadcast media have been successfully integrated into the regulatory and legal systems of the United States. In recent years, courts and regulators have once again been faced with a similar challenge with respect to the regulation of the Internet. The history of regulation of other means of mass communications can offer valuable insight in evaluating and integrating different approaches to regulating the Internet.

2. *See generally* Digital Millennium Copyright Act, Pub. L. No. 105–304, 112 Stat. 2860 (1998).

In 21st century America, government regulation has become a natural part of our daily lives and we seldom consider why the government chooses to regulate certain industries. Different authors have suggested different economic and social policy reasons for government regulation of industry. They include consumer protection, fear of natural monopoly, promotion of market efficiencies, as well as equity and fairness.[3]

Munn v. Illinois, 94 U.S. 113 (1876), is considered the cornerstone of Supreme Court regulatory jurisprudence and, more importantly, the beginning of modern economic regulation by the government.[4] In *Munn,* the Supreme Court upheld the constitutionality of an Illinois statute regulating the price charged by grain elevators against a "takings" challenge. The Court held that a state legislature could set prices charged by monopolies, especially when the service was in the public interest.[5]

Consistent with the reasoning expressed by the Supreme Court in *Munn*, Congress created the Interstate Commerce Commission ("ICC") in 1887 specifically for rate regulation of railroads.[6] Railroads were considered a vital industry for the nation and railroad transportation was in the public interest. The creation of the ICC signaled a new era in the responsibilities of the federal government. For the first time, regulation of a vital industry was committed to an independent agency, an institutional mechanism that was untested on a national level at that time.[7] Since the formation of the ICC, the forms and purposes of regulation have changed in response to economic crises, emerging risks to public health and safety, and technological advances.

The invention of the telephone by Alexander Graham Bell marked a significant technological advancement for American

---

3. *See generally* SIDNEY A. SHAPIRO & JOSEPH P. TOMAIN, REGULATORY LAW AND POLICY (2d ed. 1998) for a discussion and analysis of economic and social regulation.

4. Robert Rabin, *Federal Regulation in Historical Perspective,* 38 STAN. L. REV. 1189, 1208 (1986); Harold Furchtgott-Roth, Before the Federalist Society, Telecommunications Practice Group, Federalist Society National Convention (Nov. 12, 1998), *available at* http://www.fcc.gov/Speeches/Furchtgott_Roth/sphfr818.txt.

5. Munn v. Illinois, 94 U.S. 113, 134–37 (1876), (Field, J., dissenting) (noting the ambiguity of the Court's justification that when private property is 'affected with a public interest' it is subject to regulatory control by the state, thereby creating an opening for regulation of virtually any private enterprise in the future).

6. Joseph P. Tomain, *American Regulatory Policy: Have We Found the "Third Way?" Symposium Papers: networkingindustries.gov.reg,* 48 U. KAN. L .REV. 829, 833 (2000) (discussing the creation of the Interstate Commerce Commission and rate regulation of railroads).

7. *Interstate Commerce Commission*, Microsoft® Encarta® Online Encyclopedia 2000, *at* http://encarta.msn.com, © 1997–2000 Microsoft Corporation (last visited Aug. 1, 2002).

commerce and society in general. Bell patented the telephone in 1876.[8] The expiration of Bell's basic patents in 1893 and 1894 was a signal for open competition. The country experienced a boom in formation of new local telephone operating companies; by the end of the century there were approximately 6,000 providers offering service to 600,000 subscribers.[9] Unfortunately, there was no interconnectedness among all these telephones and a subscriber needed to have two or three instruments in order to communicate effectively with others.[10]

The first sign of significant government involvement in the telephone industry came in 1912, when the Justice Department filed an antitrust suit against AT&T, which controlled all of the long distance circuits and refused to interconnect any other telephone company to its network.[11] In response to the government threat of a break up of the company, AT&T entered into an agreement that would allow all other telephone companies to interconnect.[12] This agreement became known as the Kingsbury Commitment.[13]

By 1934, telecommunications had become so vital to the country that Congress passed the Communications Act ("1934 Act"), and, simultaneously, created the Federal Communications Commission ("FCC"). The 1934 Act created a regulatory system governing the interstate portion of the communications industry. The FCC was created "for the purpose of regulating interstate and foreign commerce in communication by wire and radio so as to make viable, so far as possible, to all the people of the United States a rapid, efficient, nation-wide, and world-wide wire and radio communication service with adequate facilities at reasonable charges."[14] The regulation of the telephone common carrier was based on market entry price controls, imposing a duty to furnish communication services upon reasonable request. Subsequent anti-competition challenges relating to AT&T's control of the local and long distance

8. Adam D. Thierer, *Unnatural Monopoly: Critical Moments in the Development of the Bell System Monopoly,* 14 CATO J. 1, 2 (1994).

9. The International Engineering Consortium, *History and Regulation of the Telephone Industry, at* http://www.iec.org/tutorials/fund_telecom/topic01.html (last visited Aug. 1, 2002).

10. *See id.*

11. *See id.*

12. Thierer, *supra* note 8, at 272 ("AT&T would sell off its $30 million in Western Union stock, agree not to acquire any other independent companies, and allow other competitors to interconnect with the Bell System"). *Id*. at 272.

13. Thierer, *supra* note 8, at 272.

14. Communications Act of 1934, Pub. L. No. 104–104, 47 U.S.C. § 151 (1934) (amended 1996).

markets by the Department of Justice and MCI Communications resulted in the break-up of AT&T in 1984 and created the regional bell operating companies ("RBOCs"), including, Bell Atlantic, Bell South, Ameritech, SouthWest Bell, Pacific Bell, and NYNEX.

Due to perceptions of inadequate competition in both the long distance and local markets, the 1934 Act was overhauled in 1996. The Telecommunications Act of 1996 ("1996 Act") created a massive shift in the telecommunications industry, deregulating markets that had been under government regulation since their inception. The seven titles of the 1996 Act cover telecommunications services, broadcast services, cable services, federal regulatory reform, obscene and violent content, and miscellaneous issues ranging from radio spectrum sales to the location of telephone poles.[15] Given the lack of current competition in the local markets of the RBOCs only a few years after its passing, the 1996 Act appears to have failed to achieve its stated goals.[16]

The histories of motion picture and broadcasting regulation offer an interesting contrast of regulatory models. In particular, the motion picture industry includes an early period of governmental regulation, followed by industry self-regulation and voluntary ratings. In contrast, the broadcast industry started out relatively self-regulated, but quickly became regulated by the government.

The first regulations of the motion picture industry came from local and state government licensing.[17] Using local business licensing laws, the state and local government regulated through the use of fees and codes.[18] In the early part of the 20th century, states began to institute government licensing schemes and prior review. This type of regulation was upheld by the Supreme Court in *Mutual Film Corporation v. Industrial Commission of Ohio*.[19] In 1921, the state of New York rejected the self-regulatory scheme proposed by the

---

15. Telecommunications Act of 1996, Pub. L. No. 104–104, § 2 tits. I–VII, 110 Stat. 56 (codified as amended at 47 U.S.C. § 336 (1996)), § 703, 110 Stat. 56 (1934) (current version at 47 U.S.C. § 224 (1996)).

16. *See* Jean F. Walker, *Paved With Good Intentions: How InterLATA Data Relief Undermines the Competitive Provisions of the 1996 Act,* 53 FED. COMM. L.J. 533 (2001); James K. Glassman, *Telecom Act Five Years Later: Re-Monopolization?* (2001), *at* http://www.newsfactor.com/perl/story/7404.html (last visited October 10, 2002); Ken McGee, *The Telecom Act Spurs Little Competition, at* http://news.com.com/2009-1033-251952.html?legacy=cnet (last visited October 10, 2002).

17. *See* RICHARD S. RANDALL, CENSORSHIP OF THE MOVIES 13 (1968).

18. *Id.* at 11.

19. Mutual Film Corporation v. Industrial Commission of Ohio, 236 U.S. 230, 242 (1915) (upholding of the pre-censorship of movies because "they may be used for evil, and against that possibility the statute was enacted").

National Board of Review and instituted its own state censorship board. The motion picture industry reacted by creating the Motion Picture Producers and Distributors of America, the industry organization that eventually became the Motion Picture Association of America.[20] With time, the abuse of power by many state censorship boards became obvious and the Supreme Court struck down the state censorship and encouraged the industry to move toward self-regulation and a ratings system.[21] The state and local governments in the 1960's began to seek different ways to inform consumers about movies through a formal rating system.[22] These early attempts at rating systems were struck down by the courts, and the movie industry moved to introduce its own rating system in 1968.[23] This industry-imposed rating system governs the movie industry today. The self-regulatory model has been subject to numerous congressional attacks for failing to be strict enough and has been revised numerous times. Similar models, subject to similar criticism, have been accepted in other areas, such as the video game industry.

The beginning of the 20th century saw an explosion in growth of wire communication mediums as well. As with numerous other technologies, there were no government regulations in the early stages of radio and television development, ultimately leading to considerable problems. The radio industry as a whole was threatened because the airwaves were flooded with stations in the same geographic territory broadcasting at the same frequencies, resulting in multiple interference problems and causing stations to increase the power of their signals to drown out competing signals.[24]

The Radio Act of 1927 ("1927 Act") created the five-member Federal Radio Commission ("FRC") to solve the interference problem. The original purpose of broadcast regulation was to ration the use of public electromagnetic spectrum and to impose a public service obligation so that the public interest and necessity would be served. [25] The 1927 Act was insufficient in some areas to keep up

20. RANDALL, *supra* note 17, at 16.

21. *See* United States v. Paramount Pictures Inc., 334 U.S. 495 (1952); Burstyn v. Wilson, 343 U.S. 495 (1952).

22. STEPHEN FARBER, THE MOVIE RATING GAME (1972).

23. *Id.*

24. *See* JOHN WITHERSPOON AND ROSELLE KOVITZ, THE HISTORY OF PUBLIC BROADCASTING (1989).

25. The Radio Act of 1927, Pub. L. No. 632, ch. 169, 44 Stat. 1162 (1927). The 1927 Act also expressly gave radio First Amendment protection from censorship.

with the demands of the communications industry, and in 1934, Congress passed the Communications Act of 1934. The newly formed FCC replaced the FRC and became the regulator of wire line and wireless technologies.

In 1996 Congress signaled its policy choice of a regulation-free zone for Internet, and information services and technologies through the Telecommunications Act of 1996.[26] Section 230 of the 1996 Act is an explicit endorsement of market self-regulation of the Internet, over government regulation. As a result, although the FCC maintains that it has the discretion to regulate Internet infrastructure and services—but has declined, so far, to do so[27]—it would currently be difficult for it to assert such authority over the express wishes of Congress.

In the area of taxation, Congress initially displayed opposition to federal regulation of the Internet, but the strength of this sentiment may be tested in the near future. The Internet Tax Freedom Act of 1998 ("ITFA") imposed a three-year moratorium on new federal, state and local taxes on Internet *access*, and a three-year moratorium on new federal taxes on services offered through the Internet.[28] The ITFA, however, does not prohibit all state sales taxes on Internet commerce and only postpones other difficult questions regarding federal taxation of Internet commerce.[29]

---

26. *See* Telecommunications Act of 1996, s*upra* note 15.

27. Beginning in the late 1960s, the FCC distinguished between so-called "basic" and "enhanced" services for purposes of the imposition of government regulation. Since that time, the FCC has consistently declined to regulate enhanced services, which include the types of information services provided over the Internet. While many believe that the FCC was expressly separating out services over which it had no regulatory authority, the agency has maintained that it has always had the discretion to regulate such services, but chose not to do so under an "infant industry" rationale—that the growth of the information services industry would be hindered by intrusive and burdensome regulatory requirements. Now that the information services industry is, by most accounts, a large and healthy one, some have argued that limited regulation is appropriate. In addition, as the networks that carry enhanced information services and the networks that carry basic telecommunications become increasingly indistinguishable—and, in fact, share infrastructure, the FCC's time-honored distinction becomes less rational in its current form. Two recent examples of challenges the FCC faces in this regard are (1) whether and to what extent Internet telephony—ordinary voice calls carried over the Internet—should be subject to telephone regulation; and (2) whether cable networks should be required to open their systems to competitors seeking to provide broadband information services.

28. *See* Internet Tax Freedom Act of 1998, Publ. L. No. 105–277, 47 U.S.C. § 151 (1998); *See also* Christopher J. Schafer, *Federal Legislation Regarding Taxation of Internet Sales Transaction,* 16 BERKELEY TECH L.J. 415 (2001); Jon Hart & Mike Hines, *Taxing the Internet: How Will Congress Interpret the Law?,* WALL ST. J., Dec. 1, 2000, *available at* http://interactive.wsj.com/articles/SB977006380777599628.htm.

29. *See id.*

In 2001, Congress extended the IFTA's moratorium on federal Internet taxes another two years, to November 1, 2003.[30] During the debate on the extension, the Senate rejected an amendment that would have allowed states to collect sales taxes on each others' behalf—a change favored by traditional retailers who believe their Internet competitors have an unfair advantage, and by state and local governments hoping to recoup $26 billion in uncollected taxes a year.[31]

By contrast, the European Union's approach represents not only greater centralization but also an attempt at worldwide control. Under an EU directive, on-line retailers—regardless of where in the world they operate—will be required to assess value-added taxes on sales made to EU customers, starting in July 2003.[32] American officials already have threatened to refer the issue to the World Trade Organization ("WTO"), fearing that the EU's rules could discriminate against non-EU companies and also serve to exclude them from the EU market.[33] Although the complexities of Internet taxation are beyond the scope of this article, the subject exemplifies the difficult questions raised by Internet commerce.

III. OTHER EFFORTS TO HARMONIZE LAWS

A. The Collision of Copyright Law and The Internet

In the view of many, the rise of the Internet posed a serious threat to the function and effectiveness of copyright law.[34] Even though the Internet existed at the time the United States Copyright Act was substantially amended in 1976, it was not considered a medium that concerned copyright law at that time. The Internet evolved as a global, distributed network of computers with no central authority or control. As such, it has no boundaries as to countries and

30. Internet Tax Nondiscrimination Act, Pub. L. No. 107–75, 115 Stat. 703 (2001).

31. Nathaniel T. Trelease & Andrew W. Swain, *Pandora's Box: Emerging Issues in the Taxation of E-Commerce,* CYBERSPACE LAW., February 2002, at 5; BBC NEWS, *US Rejects E-Tax Plan* (November 16, 2001) *at* http://news.bbc.co.uk/1/hi/business/1659345.stm.

32. Council Directive 2002/38/EC 2002 O.J. 1 (L. 128); BBC NEWS, *EU Imposes E-Commerce Tax,* (May 7, 2002), *at* http://news.bbc.co.uk/1/hi/business/1973390.stm.

33. *See* BBC NEWS, *supra* note 31.

34. *See* Scott Roland, *Internet and Copyright, at* http://www.cs.appstate.edu/~jbf/classes/cs4100/s99/cr_102/roland.html (last visited Oct. 14, 2002); Karen Coyle, Address at the San Francisco Public Library, *at* http://www.kcoyle.net/sfpltalk.html (Aug. 7, 1996); Carol Morrissey, *The 1996 WIPO Geneva Conference: Friend or Foe?, at* http://www.llrx.com/congress/010197.htm (last visited Oct. 14, 2002); Jack E. Brown, *New Law of the Internet,* 28 ARIZ. ST. L.J. 1243 (1996).

continents,[35] and countries that claim a right to regulate the Internet often have a difficult time effectively applying and enforcing their copyright laws.[36] The question often becomes what country's copyright laws should apply to which defendants located where. As of today, there is no governing body that has both international law-making capabilities and the authority to enforce them.[37]

Internet service provider ("ISP") liability for copyright infringement activities has been a difficult issue for the courts to address.[38] Although ISPs generally act as a conduit of information passing through their systems, copyright law has held service providers liable depending upon their degree of knowledge regarding the infringing activity, or their benefit from the illegal content or activity.[39] Owners of copyrights originally viewed any limitation on copyright infringement liability for ISPs as a step in the wrong direction.[40] They made several arguments against the establishment of such limits, based on their concern that it would weaken copyright enforcement over the Internet.[41] For their part, the ISPs made the argument that limitation on liability was necessary to prevent a flood of lawsuits against the ISPs themselves, or against the customers of the ISPs.[42] To many, the argument that the lack of protection from on-line copyright infringement liability could weaken entrepreneurial interest in the ISP industry did not ring true; between 1995 and 1997, revenue from providing Internet access nearly quadrupled.[43] It should be pointed out, however, that during that same period, no court handed down a decision holding ISPs strictly liable for copyright infringement without facts showing direct infringement.

In opposing limitations on liability, some looked to the publishing industry by analogy, and questioned why ISPs should be

---

35. *See* Roland*, supra* note 34.

36. *See id.*

37. *See id.*

38. *See*, Shelley M. Liberto, *New Law Limits ISP Liability For Copyright Infringement,* ORANGE COUNTY LAWYER, March 1999, *at* http://www.libertolaw.com/2-99.html; Lori E. Lesser & Vincent M. de Grandpre, *Courts Expand ISP Protection, But Pitfalls Remain: 2001 in Review,* CYBERSPACE LAW., January 2002, at 7; Hendrickson v. eBay, 165 F.Supp. 2d 1082 (C.D. Cal. 2001).

39. *See*, Liberto, *supra* note 38.

40. *See* Mark E. Harrington, Note, *On-line Copyright Infringement Liability for Internet Service Providers:Context, Cases & Recently Enacted Legislation*, 1999 B.C. INTELL. PROP. & TECH. F. 060499, ¶ 52 (Jun. 4, 1999), *at*
http://www.bc.edu/bc_org/avp/law/st_org/iptf/articles/content/1999060401.html.

41. *See id.*, at ¶ 55.

42. *See id.*

43. *See id.*

treated differently.[44] In their view, ISPs were essentially publishers, albeit in a new forum. Many argued that ISPs should bear their share of the burden like everyone else.[45] The argument was made that the ISPs performed a unique and lucrative function for the Internet, were uniquely positioned to help reduce copyright infringement by Internet users, and therefore, individual ISPs should have a legal duty to help decrease on-line piracy and a legal responsibility to monitor their users for copyright infringement.[46]

B. Initial Response: The Administration's White Paper

The Clinton Administration began addressing the issue of on-line copyright infringement during its first term.[47] In February 1993, it established the Information Infrastructure Task Force ("IITF").[48] The IITF was to implement programs that would assist in the development of what the Administration referred to as the National Information Infrastructure ("NII"), now generally called the Internet.[49] The Clinton Administration responded to complaints from music, software, and movie (collectively, "content") companies in 1995 by proposing legislation as part of a white paper report entitled *Intellectual Property and the National Information Infrastructure,* known in the industry as the "White Paper."[50] The White Paper addressed many topics including encryption, digital signatures, and on-line copyright management information, in addition to outlining the Administration's policy regarding the issue of on-line copyright infringement liability for ISPs.[51] The proposed legislation was never adopted, however, due to concerns raised by ISPs and a number of other entities. Subsequent attempts were likewise unsuccessful, until the basic concepts of the White Paper were incorporated into draft treaties being considered by the World Intellectual Property Organization ("WIPO") in 1996.[52]

44. *See id.*

45. *See* Roland, *supra* note 34; s*ee also* Hal R. Varian & Pamela Samuelson, *Information Policy in the Clinton Years* (American Economic Policy in the 1990s), May 30, 2001, *available at* http://www.ksg.harvard.edu/cbg/Conferences/economic_policy/SAMUELSON-VARIAN.pdf.

46. *See* Harrington*, supra* note 40.

47. *See id.*

48. *See id.*

49. *See id.*

50. TIMOTHY D. CASEY, ISP LIABILITY SURVIVAL GUIDE 100 (2000).

51. *See* Harrington, *supra* note 40.

52. *See* Morrissey, *supra* note 34.

C. The Digital Millennium Copyright Act ("DMCA")

By the time the WIPO treaties were presented to the United States for ratification,[53] members of Congress had begun to understand the intricacies of the ISP liability issue and had agreed that the treaties needed to be implemented.[54] This led to negotiation sessions between major copyright owners and communications companies.[55] The outcome of all of this work was Title II of the DMCA, which was signed into law in the United States in October, 1998.[56] This legislation accomplished three main objectives: 1) codified into statutory law the rule that passive automatic acts cannot be the foundation for a finding of on-line copyright infringement; 2) made it harder to establish a case of contributory or vicarious copyright infringement against an ISP; and 3) in cases where ISPs take action against alleged copyright violators, protected ISPs from lawsuits when they acted to aid copyright owners in restricting or impeding infringement.[57] The law does not establish an unqualified exemption to copyright infringement liability;[58] it is a restriction on liability, and the restriction takes the form of a statutory change in the remedies that the plaintiff has available, rather than by establishing a legal exemption to copyright infringement liability.[59]

The DMCA provides that a service provider shall not be liable for copyright infringement caused by the storage at the direction of a user of material that is on a system or network controlled or operated by or for the service provider, if the service provider: 1) does not have knowledge that the material is infringing, is not aware of facts or circumstances from which the infringing activity is apparent, or after being made aware of such facts or circumstances, acts expeditiously to remove or disable access to the material; 2) does not receive a financial benefit directly related to the infringing activity in a case where the service provider has the right and ability to control the

---

53. Principally, the Copyright Treaty, adopted by WIPO on December 20, 1996. This treaty responded to a widely-held belief that the copyright laws of many countries inadequately addressed the issues raised by the digital distribution of works over computer networks. The treaty's preamble "[r]ecogniz[es] the profound impact of the development and convergence of information and communication technologies on the creation and use of literary and artistic work." *See* Morrissey, *supra* note 34.

54. CASEY, *supra* note 50, at 103.

55. *See id.*

56. *See id.*

57. *Id.*

58. *See id.*

59. *Id.*

activity; and 3) upon notice of infringement, expeditiously removes or disables access to the allegedly infringing material.[60]

Title II of the DMCA was the first law specifically written to address the liability of on-line service providers, and it has formed the basis for many of the laws that have followed and will unquestionably influence the world's legal direction on this issue long into the future.[61] It generally limits liability of Internet service providers for a range of activities including transitory digital network communications, system caching, referring or linking users to sites containing infringing materials, and the storage of copyright infringing material on their systems.[62] Prior to the DMCA, ISPs were potentially liable for direct and contributory infringement attributable to their own actions, as well as subject to vicarious liability for the acts of subscribers who were directly infringing.[63]

The DMCA specifically provides that nothing in the statute should be construed to condition its protections on monitoring a service or pursuing facts indicating infringing activity unless pursuant to a standard technical measure.[64] The DMCA also provides that ISPs are not obligated to gain access to, remove, or disable access to material in cases where doing so would be forbidden by law.[65] The legislation is not intended to discourage service providers from monitoring their services for infringing material; however, in deference to privacy concerns, ISPs are specifically not required to monitor.

The service provider liability provisions of the DMCA amount to a compromise between what can generally be classified as the content industry and ISPs. In the end, the major content owners—movie studios, record labels, and others—compromised on their initial insistence that ISPs be subject to liability for the infringements of their customers or other users of their networks, and ISPs compromised on their initial insistence that ISPs be wholly exempt from such liability. What this compromise offers is some recourse

60. Digital Millennium Copyright Act of 1998, 17 U.S.C. § 512(c)(1)(A)(iii) (2002).

61. CASEY, *supra* note 50, at 17.

62. *See* Jason M. Anderman & Mauricio F. Paez, *Digital Music and the Digital Millennium Copyright Act: Copyright Piracy, Liability and Licensing,* MP3.COM, *available at* http://www.mp3.com/news/267.html (last visited October 14, 2002); Digital Millennium Copyright Act of 1998, 17 U.S.C. § 512(a)–(d) (2002); Lesser & de Grandpre, *supra* note 38.

63. *See* Anderman & Paez, *supra* note 62.

64. *See* Digital Millennium Copyright Act of 1998, 17 U.S.C. § 12(m); CASEY, *supra* note 50, at 117.

65. *See* Digital Millennium Copyright Act of 1998, *supra* note 64.

and some protection for both sides. In addition, and perhaps most importantly, it offers greater predictability for both industries at a time when fast-changing technologies, markets, and business methods are forcing companies to turn on a dime and often "bet the ranch" on their next move.

Although it is difficult to predict how each industry's current business decision might be different had the DMCA greatly favored one side or the other, we note that both industries are investing with abandon in new technologies and in new ways of doing business. We believe that the thoroughly debated, well-balanced outcome of the DMCA's service provider liability provisions serve as a powerful example of a workable solution to what once seemed like an insurmountable problem.

IV. HARMONIZED INTERNATIONAL AGREEMENT FRAMEWORK

As of this writing, even though the EU has adopted a Directive "on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market" ("E-Commerce Directive")[66] that limits the liability of ISPs, the EU is considering legislation[67] that could make service providers liable for unauthorized copies of protected works made as part of an automated process in routers and cache servers solely for the purpose of efficient network transmission. Shortly after the EU adopted its E-Commerce Directive in 2000, it issued a directive on harmonizing copyright laws.[68] This copyright directive includes a specific exemption from liability for copyright infringement for "temporary reproduction" that occurs during network transmission and that has no separate economic value. The exemption protects ISPs from liability for the copying that occurs during automated routing and caching processes on their servers,[69] provided the ISPs meet certain conditions including, when necessary, taking certain actions to prevent or discourage infringing activities.[70] These conditions may include the requirement that ISPs remove or prevent the transmission of data that copyright owners claim infringe their works. In many cases, however, such temporary copies occur so

66. Council Directive 2000/31/EC, 2000 O.J. (L 178).

67. Council Directive 2001/29/EC, 2001 O.J. (L 178).

68. *See id.*

69. *See id.* art. 5.1; SCADPlus, *Copyright and Related Rights in the Information Society*, *available at* http://europa.eu/int/scadplus/leg/en/lvb/126053.htm (last updated July 17, 2001).

70 *See* Sanna Heikkinen, *On the Service Provider Liability for Illegal Content, available at* http://www.tml.hut.fi/Studies/T-110.501/2001/papers/sanna.heikkinen.pdf, at 9 (last visited October 15, 2002); Paul O'Hare & Dean Stelfox, *EU Copyright Directive: Halfway to Harmony,* CYBERSPACE LAW., July–Aug. 2002, at 9.

quickly that they are imperceptible. As a practical matter, it is difficult to understand how ISPs could manage the burden of fulfilling such a requirement and thereby avoid liability. For one thing, there are no national or international on-line databases containing all the copyrighted material in the world that can be checked to confirm copyright protection and authorizations.[71] But, even if there were such databases, it would be unreasonable for a service provider to be expected to check the myriad of packets passing through routers and cache servers against the database for infringing material. For another thing, in the context of temporary transmissions of small, digitized portions of a single work—as opposed to the storage on a server of an entire work—it would be administratively overwhelming, if not technically impossible, to comply with demands by copyright owners that such temporary transmissions be stopped or prevented.

An international agreement on copyright protection of individual expressions in a digital arena has to be the solution. Even with no additional treaty to deal with the Internet and with the protection of intellectual property on-line, it is necessary for those who wish to ensure protection throughout the world to find a way to bring all of those countries that are not members of the Berne Convention or other treaties into the mix. However, even reliance upon an international copyright protection scheme will not resolve all the problems of copyright infringement lurking on the Internet. As noted, the Internet does not have physical boundaries. The combination of fast-moving technology, the complexities of copyright law, and policy-makers who are not familiar with those complexities, will continue to place strains on copyright law and frustrate Internet users now and in the future.

Nevertheless, seeking a flexible framework, balancing the interests of all concerned parties and taking advantage of lessons learned in the past, is a worthwhile endeavor. When evaluating the optimal regulatory structure for electronic commerce and other Internet activity, it may be helpful to analyze previous attempts to harmonize regulations in a variety of subject areas, in addition to examining previous efforts to impose regulatory structures upon the Internet. The analysis below categorizes existing or proposed international regulatory structures into four types: (1) unilateral governmental efforts with far reaching effects; (2) attempts at global or wide-spread regulatory structures; (3) efforts to harmonize among

71. CASEY, *supra* note 50, at 101.

key players; and (4) self-regulation. The categories are discussed in descending order of "external coercion," a phrase understood as "control or influence by governments or other external actors." While e-commerce businesses may reflexively seek to pursue the policy of pure self-regulation, this analysis will question whether such a policy is a realistic and workable solution and whether another one of the categories might better serve such businesses in the long run.

The category of regulation described as unilateral governmental actions represents a type of regulation that had been thought to be on the wane. Increased liberalism in trade policies, advanced through processes such as "rounds" of the General Agreement on Tariffs and Trade ("GATT") and institutions such as the newly-created World Trade Organization ("WTO"), has, in the last 50 years, led to a decrease in both tariff and non-tariff barriers to trade. One of the principal reasons for this downward pressure is that, while governments of individual states remain the ultimate sovereigns in the international system, the increasing volume of cross-border trade has made it possible for parties to avoid states with regulatory regimes that were deemed too costly or restrictive.[72] The interconnectedness of the Internet throws a considerable wrench into any form of unitary action—especially one based on border controls. The purchaser of goods or services on the Internet, the provider of Internet access services to that purchaser, the seller's principal place of business, state of incorporation, web site hosting facility, and warehouse, may all be located within different jurisdictions and no one jurisdiction may be able to control activity taking place outside its borders. As a result, significant questions have been raised about the application of laws to the Internet, such as who may issue and enforce regulations regarding Internet activity, where disputes may be resolved, and what law applies to disputes.[73] Attempts by businesses to comply with the laws of every state or jurisdiction that could possibly be implicated in conducting global electronic commerce would prove to be incredibly costly.[74]

One particularly troublesome example of the global effects of unilateral actions is the November 20, 2000 ruling of a French judge,

---

72. *See* Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in Ratcheting up of U.S. Privacy Standards,* 25 YALE J. INTL. L. 1, 5 (2000).

73. *See* American Bar Association Cyberspace Law Committee, *Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet*, 55 BUS. LAW. 1801, 1812 (2000). This report is the product of the American Bar Association (ABA) Global Jurisdiction Project, empanelled in 1998 under the title, "Transnational Issues in Cyberspace: A Project on the Law Relating to Jurisdiction."

74. *See id.* at 1813.

holding that the U.S. Internet portal company Yahoo! must block French users from viewing and purchasing Nazi memorabilia on its U.S.-based auction web site or face a daily fine of 100,000 French Francs (approximately $14,000).[75] Judge Jean-Jacques Gomez based his ruling on an existing French law that prohibits the display of objects that incite racial hatred.[76] The company had already removed these items from its French-language and French-domain named auction site, "http://fr.auctions.yahoo.com/," but not its U.S.-based auction site "http://auctions.yahoo.com/."[77] The Judge received advice from a panel of Internet experts regarding the ability of filtering techniques to block French users from accessing the allegedly offensive content.[78] Two of the three experts were Vint Cerf, one of the founders of the Internet, and the current Chairman of the Internet governing body, the Internet Corporation for Assigned Names and Numbers ("ICANN"); both expressed dismay about the effects of the ruling.[79] The implications for e-commerce jurisdiction are significant, as businesses seeking to avoid regulation in a foreign country may be forced not only to refrain from purposefully directing prohibited content at nationals of the regulating country, but could actually be required to install protective measures to prevent nationals from a regulating country, even those speaking another language than their native tongue, from accessing a site not specifically directed at them. Cerf stated bluntly that the judge ignored the experts' observation that "if every jurisdiction in the world insisted on some

75. *See Vive la Liberte!,* ECONOMIST, Nov. 23, 2000, *available at* http://www.economist.com/business/displayStory.cfm?Story_ID=434168; Keith Perine, *Yahoo! Asks U.S. Court to Rule French Court Out of Bounds,* THE INDUSTRY STANDARD, Dec. 21, 2000, *available at* http://www.thestandard.com/article/display/0,1151,21026,00.html; John Tagliabue, *French Uphold Ruling Against Yahoo! On Nazi Sites,* N.Y. TIMES, Nov. 21, 2000, at C8.

76. *See Yahoo!'s French Connection,* ECONOMIST, Nov. 23, 2001, *available at* http://www.economist.com/displayStory.cfm?Story_ID=431328; Andy McCue, *Caught Up in a Legal Net,* COMPUTING, Nov. 30, 2000, at 22.

77. *See* Lori Enos, *Yahoo! Ordered to Bar French from Nazi Auctions,* E-COMMERCE TIMES, (Nov. 20, 2000), *at* http://www.ecommercetimes.com/news/articles2000/001120-4.shml; *see also* Lisa Guernsy, *Mainstream Sites Serve as Portals to Hate,* N.Y. TIMES, Nov. 30, 2002, at G1.

78. *See Vive la Liberte!, supra* note 75; Enos, *supra* note 77.

79. *See* Internet Corporation for Assigned Names and Numbers (ICANN), *ICANN Board of Directors Biographies, Vinton G. Cerf, at* http://www.cann.org/biog/cerf.htm (last updated Nov. 1, 2000); Steffan Heuer, *Chief of Protocol,* INDUSTRY STANDARD, Jan. 15, 2001, *available at* http://www.thestandard.com/article/display/0,1151,21386,00.html; Mark Ward, *Experts Question Yahoo! Auction Ruling,* BBC NEWS, (Nov. 29, 2000), *at* http://news.bbc.co.uk/hi/english/sci/tech/newsid_1046000/1046548.stm; Tom Perrota, *Cerf: Yahoo! France Ruling is Flawed,* INTERNET WORLD, Jan. 1, 2001.

form of filtering for its particular geographic territory, the world wide web would stop functioning."[80] Several European businesspersons immediately decried the judgment, suggesting that its effect would be to embolden special interests seeking to regulate the Internet, to cause businesses operating on the Internet to take their assets out of France, and to promote a situation where Internet businesses might be subject to the regulations of every country.[81] Yahoo! responded to the French court order by filing suit in U.S. District Court in San Jose, California, asking for a declaratory judgment that the French court's verdict violates the First Amendment to the U.S. Constitution and provisions of the Communications Decency Act that immunize ISPs from third party conduct, and that the French decision would be unenforceable because it would be technically impossible for the company to block French purchases of Nazi material.[82] At about the same time, Yahoo! announced that it would ban hate-related materials from its U.S. web site, a decision which it claims is unrelated to the French opinion, but one which would preserve its right to go forward in U.S. courts while possibly providing a way of complying with the effect of the French order.[83] Some commentators have suggested that the success of the plaintiffs in the Yahoo! case of achieving much of their desired result may embolden others to undertake similar suits in foreign courts aiming to censor American on-line speech.[84]

In 2001, a federal district judge ruled that the French order violated Yahoo!'s First Amendment rights and was therefore unenforceable in the United States.[85] The French plaintiffs have

---

80. Ward, *supra* note 79.

81. *See supra* note 76; David Pringle, *Some Worry France's Ruling on Yahoo! Will Work to Deter Investments in Europe,* WALL ST. J., Nov. 22, 2000, *available at* http://interactive.wsj.com.

82. *See* Keith Perine, *Yahoo! Asks U.S. Court to Rule French Court Out of Bounds,* INDUSTRY STANDARD, Dec. 21, 2000, *available at* http:www.thestandard.com/article/display/0,1151,21026,00.html (last visited Aug. 1, 2002); *Yahoo! Tries to Block French Ruling,* CYBERSPACE LAW, Feb. 2001, at 23; *Yahoo! Seeks Ruling That it Need Not Obey French Court Order,* E-Business Law Bulletin, Feb. 2001, at 17.

83. *See* Kristi Essick, *Yahoo Bans Nazi Goods,* THE INDUSTRY STANDARD, Jan. 3, 2001, *at* http://www.thestandard.com/article/display/0,1151,21184,00.html; Lisa Guernsey, *Yahoo to Try Harder to Rid Postings of Hateful Material*, N.Y. TIMES, Jan. 3, 2001, at C2.

84. *See* Carl S. Kaplan, *Experts See Online Speech Case as Bellwether,* N.Y. TIMES, Jan. 5, 2001, *available at* http://www.nytimes.com/2001/01/05/technology/05CYBERLAW.html; Charlie Cray, *The Enforcers: The Hague Convention and the Threat to Internet Freedoms and Consumer Protection; Corporate Capture of the Internet,* MULTINATIONAL MONITOR, Mar. 1, 2002, at 9.

85. Yahoo!, Inc. v. La Ligue Conre le Racisme et l'Antisemitisme, 169 F. Supp. 2d 1181 (N.D. Cal. 2001); Troy Wolverton, *Court Shields Yahoo*! *From French Laws,* CNET NEWS.COM, (Nov. 8, 2001), at 85, *at* http://news.com.com/2102-1017-275564.html.

appealed the case to the Ninth Circuit, but if the ruling stands, it will, in the words of a Yahoo! lawyer, prevent Internet content operators from having to operate in accordance with "a lowest common denominator standard for protected speech on the Net."[86] In 2002, the French courts responded, agreeing to try Yahoo!'s former CEO on criminal charges of condoning war crimes, carrying the maximum sentence for such a conviction of five years in prison and a $39,800 fine.[87] The French court ruled that French law applied to Yahoo!'s English-language sites even though they are based elsewhere.

Fears of further assertions of extraterritorial jurisdiction may be well-founded as German prosecutors began a criminal prosecution of Yahoo! in 2000 for allegedly selling the forbidden book *Mein Kampf*, by Adolf Hitler, on Yahoo!'s auction site, to consumers in Germany.[88] The criminal prosecution of Yahoo! in Germany was subsequently dropped, and the German court noted that as a supplier of internet services, Yahoo! was not responsible for the site's content.[89] In India, a magistrate has found sufficient evidence of violations of the country's pornography laws to begin a trial of directors of a company whose on-line service allows users to find other web sites, some of which may be pornographic, by means of a search engine.[90] The complaint alleges that the company failed to properly screen out pornographic material and allowed users to follow hyperlinks to pornographic web sites, which are believed to be located in the United States.[91]

Another recent example of a unilateral action by a governmental body having significant effects outside its borders is the EU Directive

86. Kaplan, *supra* note 84.

87. *See* Reuters, *Yahoo Case Taken to Criminal Court,* CNET NEWS.COM, (Feb. 26, 2002), *available at* http://news.com.com/2102-1023-856698.html; Steven Bonisteel, *French Court Picks 2003 Date for Yahoo!'s Nazi Trial,* NEWSBYTES, May 7, 2002; Alan Krauss, *Yahoo Headed for Trial in France,* N.Y. TIMES, Feb. 27, 2002, at C2.

88. *See* Steve Gold, *Germany Probes Yahoo Sale of "Mein Kampf"*, NEWSBYTES, Nov. 28, 2000, *at* http://www.newsbytes.com/news/00/158658.html; Thomas Vartanian & James Munchmore, *It is a Brave New World of On-Line Liabilities*, N.Y. L.J., May 1, 2001, at 5; *See also* Kurt A. Wimmer, *Internet Jurisdiction*, NAT'L L. J, March 26, 2001, at A12 (discussing German court's exertion of jurisdiction over Australian in criminal suit against website publisher).

89. *See* James Connell, *Yahoo and Germany,* INT'L HERALD TRIB., March 27, 2001, at 15.

90. *See* Mumbai, *Porn Troubles Rediff, Satyam, and Indiaworld,* ZDNET INDIA, (December 2, 2000), *at* http://www.zdnetindia.com/news/breaknews/stories/8591.html; R. Savitha, *India: Rediff Purveying Pornography,* BUS. LINE, Nov. 30, 2000, at 2000 WL 30106706.

91. *See* Mumbai, *supra* note 90.

95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data ("EU Privacy Directive"), which became effective on October 24, 1998.[92] The EU Privacy Directive sets standards for transfers of personal information within the EU, as well as for transfers to third countries that are not members of the EU.[93] The effect is to significantly restrict businesses located in non-EU member states from electronic commerce with states in the EU, if these non-EU businesses do not meet the EU privacy standards. The United States did not respond with a matching regulatory structure, but instead negotiated a "safe-harbor" provision that still leaves most of the burden on individual companies to comply with the EU Privacy Directive's "adequacy" standard.[94] The EU regulations have significant effects on corporations, compelling them to establish "principles" and "guidelines" to comply with the terms of the EU Privacy Directive and possibly foregoing business opportunities that they might otherwise take in the absence of such regulation.[95] The EU's action was the result of pressure from member states with significant data protection laws, such as France, to prohibit transfers of data to other member states, such as Italy, without such protections.[96] As of July 2002, 220 American companies have self-certified as falling within the safe harbor provisions.[97]

In 2002, a German court ruled that deep linking—hypertext links that bypass the front page of a Web site—to stories on a newspaper's Web site violated the EU's 1996 Database Directive.[98] That regulation prohibits the "unfair extraction" of materials contained in a database.[99] The ruling reaches the opposite result from that of an American court that looked at the same issue in 2000. In the U.S. case, a federal district court ruled that hyperlinks do not, by

92. *See* Shaffer, *supra* note 72, at 5.

93. *See id.* at 3.

94. *See id.* at 24–28; *See also* U.S. DEPT. OF COMMERCE, SAFE HARBOR OVERVIEW, *available at* www.export.gov/safeharbor (last visited Oct. 14, 2002).

95. *See id.* at 72–74.

96. *See id.* at 10.

97. U.S. DEPT OF COMMERCE, SAFE HARBOR LIST, SAFE HARBOR, *available at* http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list (last visited July 31, 2002).

98. Michelle Delio, *Deep Linking Takes Another Blow*, WIRED NEWS, (July 25, 2002), *at* http://www.wired.com/news/pring/0,1294,54083,00.html; Marydee Ojala, *Deep Thinking Eludes Deep Linking Detractors,* ONLINE MAG., Sept. 1, 2002, at 5; *Foreign Courts Against Deep Linking,* THE QUILL, Sept. 1, 2002, at 8.

99. Database Directive 96/9/EC, 1996 O.J. (L 77).

themselves, violate copyright laws.[100] The judge analogized linking to using a library's card index to refer to particular items.

Although the EU is a regional organization, with no jurisdiction outside its member states, its rule-making action, conducted without the significant participation of outside countries, has had significant effects outside its boundaries. One effect of this unilateral action is to allow disparate jurisdictions to create a fragmented patchwork of regulation that would effectively allow any jurisdiction to attempt to regulate the entire Internet.[101] This would reverse the criticism of trade-liberalization as a "race to the bottom" and instead create an environment that would cause global electronic commerce companies to respond, inefficiently, to the highest common denominator of regulation.

The establishment of a free trade regime where states voluntarily submit to dispute settlement by the WTO would support the assertion that one should not be overly concerned about the EU's Privacy Directive. After all, states would then have the recourse against significant non-tariff barriers to trade and significant alternative markets in which to conduct commerce without submitting to regulations such as those imposed by the EU.[102] One might expect this resulting flight of potential commerce and investment capital to provide an incentive for the EU to avoid such regulation. However, because of the size of the EU economy, relative to the other economies of the world, the opportunity for it to exert its influence in international commerce, even if arguably contrary to its self-interest, is a possibility that should concern other potentially affected states.[103]

100. Ticketmaster Corp. v. Tickets.com, Inc., 54 U.S.P.Q.2d 1344, 1346 (C.D. Cal. 2000); Michelle Finley, *Attention Editors: Deep Link Away,* WIRED NEWS, (Mar. 20, 2000), *at* http://www.wired.com/news/politics/0,1283,35306,00.html.

101. *See* Thomas P. Vartanian, *Whose Internet is it Anyway? The Law of Jurisdiction in Cyberspace: Achieving Legal Order Among the Nations,* Presentation to the George Mason University 2000 Global Internet Summit, March 13–14, 2000, *available at* http://www.ffhsj.com/bancmail/jur_over.htm; David Johnson & David Post, *Law and Borders–The Rise of Law in Cyberspace,* 48 STAN. L. REV. 1307 (1996).

102. *See* WTO, *Trading Into the Future: Introduction to the WTO, The Agreements*, *at* http://www.wto.org/english/thewto_e/whatis_e/tif_e/agrm0_e.htm (last modified Sep. 24, 2001); *See* WTO, *Trading Into the Future: The Organization, Members and Observers, at* http://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm (last modified Oct. 2, 2002).

103. *See* European Union, Delegation of the European Commission to the United States, *Facts and Figures on the European Union and United States, at* http://www.eurunion.org/profile/facts.htm (last visited Aug. 1, 2002) (the EU claims that in 2000 its Gross Domestic Product (GDP) was $7.84 Trillion compared with a United States 2000 GDP of $9.9 Trillion); *See also*, European Report, *FBE Alludes to Return of Parity Between Euro and the Dollar*, Dec. 2000 (discussing the growing strength of the European economy and

An example of the negative consequences resulting from the imposition of unilateral regulations is represented in the "Brussels Regulation" or "Brussels 1" regulation. This provision, which European Justice Ministers signed November 30, 2000, would allow European consumers who order goods or services over the Internet from a business in another EU country to sue that business in the consumer's home country.[104] Supporters of the regulation hailed it as a measure that would increase consumers' confidence in e-commerce because they would be protected by the same consumer protection laws that are applicable when shopping off-line.[105] Representatives from various business interests were harshly critical of the measure though, suggesting that on-line merchants may purposefully avoid EU countries and observed that such regulation may fragment the EU's common market.[106] Some European organizations are "furious" with the apparent inconsistencies between the Brussels 1 Regulation[107] and the EU E-Commerce Directive.[108] The controversy over this jurisdictional regulation could also foreshadow similar opposition to an initiative to update the Rome Convention on choice of law to apply to e-commerce disputes.[109]

Some unilateral actions by foreign governments complement on-going efforts by the U.S. government. Congress considered an anti-spam bill in 2002 that would have imposed criminal penalties for the transmission of unsolicited commercial e-mail that contained false or misleading header information.[110] The bill also required spammers to include identifying, opt-out, and physical address information in any

---

the Euro).

104. *See* Brandon Mitchener, *EU Approves E-Commerce Law, Prompting Concerns Over Impact,* WALL ST. J., Dec. 1, 2000, *available at* http://interactive.wsj.com/articles/SB975616575701214705.htm; *Europe: Business Attacks EU Websites Move,* FIN. TIMES, Dec. 1, 2000, *available at* http://www.ft.com; Paul Meller, *Online Buyers Gain Ability to Sue,* N.Y. TIMES, Dec. 1, 2000, *available at* http://www.nytimes.com/2000/12/01/technology/01NET.html; Keith Regan, *EU Oks E-Commerce Dispute Law,* E-COMMERCE TIMES, (Dec. 1, 2000), *at* http://www.ecommercetimes.com/perl/story/5635.html; Victorya Hong, '*Brussels 1' Angers EC Businesses,* INDUSTRY STANDARD, Dec. 1, 2000, *at* http://www.thestandard.com/article/display/0,1151,20531,00.html.

105. *See* Meller, *supra* note 104.

106. *See id.*

107. Council Directive 2001/44/EC, 2001 O.J. (L 175), *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/1_17520010628en00170020.pdf.

108. *See* Hong, *supra* note 104.

109. *Id.*

110. *See* Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2001, S. 630, 107th Cong. (2001) (a Senate committee reported the bill favorably on May 17, 2002).

unsolicited commercial e-mail. While the FTC or state attorneys general could bring claims on behalf of the public, the bill would also permit an ISP to file a civil action and to recover treble damages for harm caused to its network. Opponents of strong anti-spam legislation include corporations such as Citicorp and Procter & Gamble, as well as commercial associations such as the National Retail Federation and the American Insurance Association, who argue that the bills would restrict e-mail marketing and disadvantage electronic commerce.[111] Although many states have their own anti-spam laws, these measures suffer from difficulties in coverage, enforcement, and jurisdiction, increasing the significance of federal action.[112] The European Union approved an anti-spam directive in 2002 that establishes a default opt-in rule, meaning that consumers must give permission to marketers before being sent commercial e-mail.[113]

The opposite of unilateral actions are global or near-consensus agreements that take into account a multitude of views. One of the problems with such consensus mechanisms is that often in areas such as content regulation, intellectual property protection, privacy and security, where several parties may have very different interests; it is exceptionally difficult to develop principles agreed to by all. Additionally, even if the parties can agree on the rules that are to govern a given regime, constructing an enforcement mechanism that is binding on international parties and accepted by domestic governments has been one of the most significant challenges in international relations. One example of the difficulty in reaching consensus is in the area of copyright protection. The Convention for the Protection of Literary and Artistic Works ("Berne Convention"), signed in Berne, Switzerland on September 9, 1886, represented an early attempt to create an international regime for copyright protection.[114] However, the rigid adherence of the U.S. to the

111. *See* Letter from Securities Industry Association on Behalf of Multiple Industry Associations of May 15, 2002 to Sen. Ernest F. Hollings, Chairman of the Senate Commerce, Science and Transportation Committee [hereinafter "Letter from Securities Industry Association"] *available at* http://www.sia.com/2002_comment_letters/pdf/AntiSpam.pdf; *See generally* Jennifer Lee, *Spam: An Escalating Attack of the Clones,* N.Y. TIMES, June 27, 2002, at G1.

112. *See* Letter from Securities Industry Association, *supra* note 111.

113. *See* Directive 2002/58/EC, 2002 O.J. (L 201); Christopher Saunders, *EU Oks Spam Ban, Online Privacy Rules,* INTERNETNEWS.COM, (May 31, 2002), *available at* http://www.internetnews.com/IAR/print.php/1154391.

114. MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 17.01 [B][1] (2000); CRAIG JOYCE ET AL., COPYRIGHT LAW 21 (Matthew Bender & Co. ed. 5th eds. 2000).

requirement of copyright notice, specifically the use of the ©, or "circle C" symbol, prevented the country from joining the Berne Convention for over 102 years.[115] Several of the functions of the Berne Convention were carried out through the Universal Copyright Convention (which the U.S. joined in 1955) and through the "backdoor to Berne" access, and ultimately the United States did join the Berne Convention and the 1996 WIPO Copyright Treaty. Nevertheless, the example of Berne demonstrates the difficulties with relying on multilateral agreements to establish order.[116] An example of intractable differences that would prohibit certain agreements is "content regulation," what many Americans derisively refer to as "censorship." While multiple jurisdictions may agree on the criminality of certain forms of expression on the Internet, such as child pornography, the Yahoo! dispute demonstrates how differing domestic laws can make agreement impossible. In France, the prevention of racial hatred takes precedence over unrestrained speech, whereas in the U.S. the First Amendment of the Constitution prohibits Congress from making such a choice.[117]

Although obtaining the consensus required to conclude international agreements has proven difficult, once achieved, the agreements have significantly contributed to the creation of regimes that facilitate order.[118] After adoption by the U.S. and a total of over 140 countries, the Berne Convention ultimately has progressed towards the goal of "universalizing" copyright law through the establishment of "minimum standards" with which countries adhering to the treaty comply in their domestic law. [119] The treaties push countries toward consistency of treatment by including a requirement for "national treatment," which gives nationals the same protection in other countries that they receive in their own country.[120]

Achieving effective enforcement of international treaties has been consistently hampered by the failure to obtain the consent of sovereign states to such agreements that are binding upon them. Two notable examples from U.S. history are the failure to ratify the League of Nations Treaty and the withdrawal of the U.S. from compulsory jurisdiction of the International Court of Justice ("ICJ") following

---

115. JOYCE ET AL., *supra* note 114, at 21.

116. *See* NIMMER & NIMMER, *supra* note 114, at §§ 17.01 [B][1]–[2], [C][1][b]; JOYCE, ET AL., *supra* note 114, at 33–34.

117. *See* Yahoo, Inc. v. La Ligue Contre Le Racisme et l'Antisemitisme, *supra* note 86; *Yahoo!'s French Connection, supra* note 77.

118. *See* NIMMER & NIMMER, *supra* note 114, at § 17.01[B].

119. *Id*. at § 17.01[B][1][a].

120. *See id.*

United States v. Nicaragua (Nicaraguan Harbors).[121] The recent creation of an intellectual property regime following the Uruguay Round of the General Agreement on Tariffs and Trade ("GATT") increases prospects for an enhanced enforcement regime for intellectual property, beyond that of previous treaties dealing with intellectual property. The protocol on Trade-Related Aspects of Intellectual Property Rights ("TRIPs") provides a method for enforcement in addition to national treatment and minimum standards, and use of a WTO adjudicatory panel.[122] Possible sanctions authorized under the WTO's Dispute Settlement Understanding ("DSU") include retaliatory sanctions, e.g., cross-sector sanctions against an area other than intellectual property.[123]

Given the problems of unilateral action and the difficulties of multilateral agreements, much greater emphasis has been placed on the "harmonization" of electronic commerce laws by developing model codes or uniform laws that would be enacted in multiple jurisdictions. One of the current efforts to do this is through the United Nations Commission on International Trade Law ("UNCITRAL") Model Law on Electronic Commerce ("Model Law").[124] The Model Law does not seek to become a detailed "code" that would specify every rule applying to electronic commerce, but instead, attempts to provide general principles and procedures from which states may draw their own codes tailored to their individual circumstances and preferences.[125] The ultimate goal of such an effort is to give to electronic transactions similar treatment as that received by paper-based communications.[126] An additional example of a consensus agreement that articulates only broad principles and guidelines is the Organization for Economic Cooperation and Development's ("OECD") Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ("OECD Guidelines").[127] This

121. Military And Paramilitary Activities (Nicar. v. U.S.) 1986 I.C.J. 14, 25 I.L.M. 1023 (merits); U.S. Statement on the U.S. Withdrawal from the Proceedings Initiated by Nicaragua in the International Court Of Justice, 24 I.L.M. 246, January 18, 1985; S*ee also* Military And Paramilitary Activities (Nicar. v. U.S.), 24 I.L.M. 59 (1985) (jurisdiction).

122. *See* NIMMER & NIMMER, *supra* note 114, at §§ 18.06, 18.06 [B][2]–[B][3].

123. *See id.* at § 18.06[B][3].

124. *See* UNCITRAL Model Law on Electronic Commerce with Guide to Enactment (May 2000), *available at* http://www.uncitral.org/en-index.htm.

125. *See* A. Brooke Overby, *Will Cyberlaw be Uniform? An Introduction to the UNCITRAL Model Law on Electronic Commerce,* 7 TUL. J. INT'L & COMP. L. 219, 222 (1999).

126. *See id.*

127. Organization for Economic Cooperation and Development (OECD), *Guidelines*

farsighted document articulates general principles that one might use in constructing privacy regulations. It has been cited as an influence in the development of privacy regulations in member countries, yet it has no binding authority on any OECD member.[128]

Technological developments will also affect the legal battles over applying national laws worldwide. "Geographical zoning" software has the potential to determine an Internet user's physical location, so that Web sites can block or limit the content accessible according to local laws.[129] Widespread use of such technology would force ISPs to reevaluate their policies for access and their roles in acting as "mere conduits" for information.

The creation of the UNCITRAL Model Law may be compared and contrasted with the attempts in the United States to update the Universal Commercial Code ("UCC") to address electronic commerce and electronic data transmission.[130] The UCC has heretofore been considered a successful uniform code, having been implemented in some form in every state of the United States.[131] The Uniform Computer Information Transaction Act ("UCITA") began as an attempt to create a UCC Article 2B that would specifically address choice of law and contract issues relating to digital information or digitally delivered services.[132] UCITA has been embroiled in controversy regarding standard form contracts and mass-market licenses as well as the lack of certain consumer protections.[133] As of August 2002, UCITA had only been adopted by two states, Maryland and Virginia.[134] Some commentators suggest that the UNCITRAL

Governing the Protection of Privacy and Transborder Flows of Personal Data, available at http://www.olis.oecd.org/horizontal/oecdacts.nsf/linkto/C(80)58 (last visited Aug. 1, 2002); *See also* Barbara Cruthcfield George, Patricia Lynch, & Susan Marsnik, *U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive,* 38 AM. BUS. L.J. 735 (2001) (providing a general background of the OECD Guidelines).

128. *See e.g.* Federal Trade Commission (FTC), *Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress* 4, 43 n.25, (May 2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

129. Lisa Guernsey, *Welcome to the Web. Passport Please?*, N.Y.TIMES, Mar. 15, 2001, at G1.

130. *See* Overby, *supra* note 125, at 227.

131. *Id.* at 228.

132. *See* Raymond T. Nimmer, *Contract Law in Electronic Commerce,* 587 PLI/PAT 1127, 1142 (2000).

133. *See* Raymond T. Nimmer, *UCITA: A Commercial Contract Code,* 17 NO. 5 COMPUTER LAW. 3, 12–15 (2000).

134. *See* National Conference of Commissioners on Uniform State Laws, *A Few Facts About the Uniform Computer Information Transactions Act, available at* http://www.nccus1.org/nccus1/uniformact_factsheets/uniformacts-fs-ucita.asp, (last visited Oct. 17, 2002). Maryland and Virginia adopted non-uniform versions of UCITA in 2000, and

process, which is more flexible than that of the UCC and minimizes intrusion into domestic law, will be more successful than UCITA.[135] However, the experience of the United Nations Conference on the Law of the Sea (which was hindered for several years by the persistent efforts of developing nations to affect a wealth redistribution system concerning the mining of mineral nodules from the seafloor) is suggestive of the difficulties to be encountered in enacting regulations at a global level.[136]

In addition to harmonization efforts that aspire to global application, such as UNCITRAL, another approach to creating governance structures is to begin with an agreement between a small number of key actors, then slowly build consensus. This approach was implemented with significant success in the establishment of capital adequacy standards for international banks in a framework commonly known as the "Basle Accord."[137] The Basle Accord began as a bilateral agreement between the United States and United Kingdom and expanded to include the Group of Ten ("G-10") countries.[138] However, because the Basle Accord has limited its membership to the G-10, it has been able to better reflect the interests of the primary banking institutions and to avoid becoming sidetracked by the concerns of minor banking players. An electronic commerce agreement forged between the G-10 countries would similarly be able to focus on the concerns of the most significant countries involved in electronic commerce. However, countries excluded from the process would likely protest their lack of input. One solution to this problem would be to specify a minimum volume of electronic commerce to become a participant in such a regime. That way, small countries with a significant amount of e-commerce activity would not be

legislation has been introduced in seven other states, the District of Columbia, and the U.S. Virgin Islands. The National Conference of Commissioners on Uniform State Laws continues to consider amendments to UCITA. In 2001, the attorneys general of thirty-two states sent a letter to NCCUSL expressing continued opposition to UCITA as "fundamentally flawed in its scope and approach." *Id.*

135. *See* Overby, *supra* note 125, at 234.

136. *See* NATIONAL INTELLIGENCE COUNCIL, LAW OF THE SEA: THE END GAME, 3–7 (1996).

137. *See* Wolfgang H. Reinicke, GLOBAL PUBLIC POLICY: GOVERNING WITHOUT GOVERNMENT? 103 (1998).

138. *See* Basle Committee on Banking Supervision, *International Convergence of Capital Measurement and Capital Standards*, (July 1998), *available at* http://www.bis.org/publ/bcbs04a.htm; *See generally,* Lawrence Lee, *The Basle Accords as Soft Law: Strengthening Int'l Banking Supervision,* 39 VA. J. INT'L L. 1 (1998).

excluded on non-relevant factors such as population or geographic size.

One regulatory structure that has worked very effectively in an environment of decentralization and complexity that is similar to that of electronic commerce is the one found in the domestic regulation of securities: self-regulation with government supervision. In the United States, much of the regulation of securities markets is conducted by industry-created self regulatory organizations ("SROs"), including the National Association of Securities Dealers ("NASD") and the New York Stock Exchange ("NYSE"), which are themselves overseen by the Securities and Exchange Commission ("SEC").[139] Imposition of such a regulatory structure for e-commerce would likely involve the creation of industry-sponsored self-regulatory organizations to regulate privacy issues and consumer fraud concerns, with oversight provided by an existing federal body such as the U.S. Federal Trade Commission, which has shown that it is not afraid to get involved in policing electronic commerce.[140]

The evolution of the Basle Accord has also begun to fit into this model, with rigid rules on capital levels being replaced by models that allow self-assessment of risk and reward effective self-analysis with reduced stringency of regulation.[141] This evolution of the Basle Accord was an innovative industry response to what began as a more rigid regulatory regime. Electronic commerce companies may be able to implement such a strategy if they find themselves under inflexible laws and regulations where industry self-regulation offers a more effective alternative that is acceptable to regulators.

Pure self-regulation reflects the current state of supervision in many areas of electronic commerce, such as privacy. However, there are several reasons to suggest that this framework either may not last, or may not be the optimal environment for businesses attempting to conduct electronic commerce. The governmental efforts to regulate electronic commerce, including the EU Privacy Directive, UNCITRAL, and UCITA, discussed above, as well as other actions, such as the U.S. Children's' Online Privacy Protection Act ("COPPA"), suggest that belief in the continued existence of self-

---

139. *See* THOMAS LEE HAZEN, THE LAW OF SECURITIES REGULATION, 1–19 (3d ed. 1996).

140. *See* Federal Trade Commission (FTC), *Going, Going, Gone: Law Enforcement Efforts To Combat Internet Auction Fraud*, (February 2000), *available at* http://www.ftc.gov/bcp/reports/int-auction.pdf. *See FCC Instant Messaging Compromise Draws Criticism,* WASH. INTERNET DAILY, Jan. 16, 2001.

141. Remarks at the Conference on Credit Risk Modeling and Regulatory Implications Sept. 22, 1998, *at* http://www.newyorkfed.org/pihome/news/speeches/mcd980922.html; Lee, *supra* note 138.

regulation may simply be an unrealistic expectation in many areas of electronic commerce. Congress, which once chanted the mantra "we're not going to regulate the Internet," has changed its tune and proposed and implemented a whole slew of new invasive regulations.[142] Additionally, doubts can be raised about the effectiveness of industry self-regulation. The case of Toysmart.com, which attempted, as part of its bankruptcy proceeding, to sell its customer lists in violation of its own privacy policy, suggests some of the ways that self-regulation can break down.[143] A cause of particular dismay for advocates of self-regulation was the failure of third party certification agency TRUSTe to stop one of its licensees from violating their agreement.[144]

Such breakdowns in self-control are important to electronic commerce participants who may suffer reputation harm by being associated with merchants who are perceived as lacking credibility with respect to their willingness to adhere to privacy or security policies.[145] The resulting loss of confidence creates an electronic commerce marketplace where efficient transactions are foregone, due to lack of certainty about privacy and security issues.[146] Adopting policies and procedures that raise the confidence of participants in electronic commerce may lead to the creation of markets that promote more transactions than they inhibit, creating greater wealth for all e-commerce participants.

142. *See* Children's Online Privacy Protection Act, Pub. L. No. 105–277, 112 Stat. 2681 (1998). S*ee* Associated Press, *Congress Mulls Internet Filtering,* CNET NEWS.COM, (Oct. 15, 2000), *available at* http://news.cnet.com/news/0-1005-200-3204667.html. *See* Steve Chapman, *It's Librarians to the Rescue on Net Speech,* THE BALTIMORE SUN, June 11, 2002, at A19.

143. *See* Federal Trade Commission (FTC), *FTC Announces Settlement With Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations, available at* http://www.ftc.gov/opa/2000/07/toysmart2.htm (July 21, 2000); Federal Trade Commission v. Toysmart.com, LLC, 2000 U.S. Dist. LEXIS 21963 (2000).

144. *Id.*

145. *See* AT&T Labs, *Beyond Concern: Understanding Net Users' Attitudes about Online Privacy,* Research Technical Report TR.99.4.3, April 14, 1999, *available at* http://www.research.att.com/resources/trs/TRs/99/99.4/99.4.3/report.htm; Better Business Bureau Online, *Benefits of Membership*, *at* http://www.bbbonline.org/reliability/benefits.asp (last visited Aug. 1, 2002).

146. United States Judiciary Committee, *Know The Rules Use the Tools: Privacy In The Digital Age: A Resource For Internet Users*, *available at* http://judiciary.senate.gov/oldsite/privacy.pdf (last visited Aug. 1, 2002); Reuters, *Poll Says Most Americans Have Cyber-Security Qualms,* INFOWORLD, (Oct. 16, 2000), *at* http://www.infoworldcom/articles/hn/xml/00/10/16/001016hnamericans.xml.

V. CRIMINAL LIABILITY

There are national economies great and small, and there are vastly different cultural views from country to country, all of which affect and compound problems associated with Internet content and electronic commerce activity. But two things found in common among every township and village the world over are the propensity of some people to commit crimes, and the inclination of local authorities to enact and enforce consumer protection laws. They come in a variety of shapes and colors, but they're all cut of essentially the same cloth.

No discussion of the problems facing ISPs and e-commerce companies is complete without assessing the risk of criminal liability for the acts of others and the possibility of running afoul of local consumer protection laws.

As a general matter, issues of criminal liability often turn on the fact that what may be perfectly legal in one place is criminal in another. As a related matter, who may be held responsible for criminal activity varies as well; in the courts of some countries, a disinclination to hold ISPs criminally liable for the acts of their customers is strongly emerging, while in other countries, the opposite is true. On the enforcement side, efforts are increasing to coordinate criminal investigative activities. Officials from the Group of Eight ("G-8") countries announced an effort to seek common law enforcement standards for the Internet.[147] The officials' proposal included a call for the establishment of a central office to coordinate the investigation of on-line criminal activity.[148] While the sensibilities of courts may vary widely, one thing is clear: law enforcement authorities are less ambivalent. Police and government investigators around the world speak in a common voice in calling for regulation of Internet activity, including increased access to ISP networks.[149]

The prospect of liability for "crimes" that constitute normal, even honorable (e.g., free speech) behavior in an ISP's or e-commerce company's home country may seem anathema. The

147. *See G-8 Officials Seek Common Standards against Internet Crime*, *at* http://www.it.fairfax.com.au/breaking/20001027/A10781-2000Oct27.html (last visited Nov.4, 2000); Ralph Atkins & Tobias Buck, *G-8 Seeks Tighter Internet Security*, FIN. TIMES, Oct. 27, 2000, at 16.

148. *Id.*

149. The U.S. Federal Bureau of Investigation has consistently sought and promoted policies and legislation expanding its access to communications and transactions on the Internet and other networks.

service provider's instinct may be to speak out against any potential imposition of liability, contemptuously ignoring the threat; or attempt to avoid the problem, to the extent possible, by not doing business in such a country. As we have seen with respect to civil liability for copyright infringement however, there may be administratively and economically palatable solutions to avoiding or complying with onerous laws that exploit markets, which would otherwise be lost.

The prospect of being subject to local consumer protection laws is a particularly vexing problem for e-commerce companies. Inexpensive access to the Internet and the decreasing cost of providing rich content and services has lowered barriers of entry to global markets. At the same time, buyers can now conduct business with sellers who cannot afford to defend themselves when disputes arise that subject them to the consumer protection laws—and the courts—of the buyer's locale. Traditionally, the disparity of resources in favor of sellers almost always justified subjecting sellers to the jurisdiction of buyers for purposes of resolving disputes or defending against claims brought by consumer protection authorities. The parties to an e-commerce transaction however, may be similarly situated; that is, the seller may have no resource advantage over the buyer.

As such, e-commerce companies that target—or at least do not attempt to exclude—buyers in foreign states must carefully weigh the risks of being subject to multiple jurisdictions. As a practical matter, this may entail absorbing losses associated with customer complaints and enduring default judgments on claims brought by consumer protection authorities.[150] While such judgments are undesirable from a business perspective (e.g., reputation damage),[151] it is important to remember that the same factors that inhibit an on-line seller from defending itself in the first place, limit the effect (i.e. enforcement) of a judgment as a practical matter; namely, no physical contacts with, or assets in, the jurisdiction.

150. The same interactive technology and innovative business methods that foster a comfortable and engaging forum for e-commerce transactions may provide opportunities to avoid the long arm of consumer protection authorities. To the extent that buyers, or consumers, have traditionally been viewed as un-empowered as compared to most sellers, e-commerce site operators may seek to dispel that notion by empowering consumers and customers with dynamic disclosures, user-friendly, easy to navigate terms and conditions and other methods.

151. Consumer-friendly e-commerce sites may also realize a competitive advantage by building a reputation that ia as sensitive to consumer protection issues (i.e. the best interests of its customers), just as some bricks-and-mortar businesses have established reputations for superior customer service.

Like criminal law enforcement, consumer protection officials have begun coordinating efforts with colleagues around the world. In late 2000, The U.S. Federal Trade Commission hosted a meeting of consumer protection authorities from nine countries, five U.S. administrative agencies, and twenty-three U.S. states.[152] It is reasonable to assume that the same rationale that led the guardians of intellectual property rights and criminal investigative authorities to ISPs, will lead to calls from consumer protection officials for help in reducing on-line fraud and other nefarious business practices. To the extent that ISPs may be subject to liability for the shady dealings of their customers, the need for predictability will require a harmonized approach to imposing—including limiting—such liability. In the context of consumer protection, there has been significant effort around the world to promote the use of on-line dispute resolution services to bring together remote parties to a dispute in a fast and economical manner. It may be possible to extend such efficiencies to consumer protection authorities and to the subjects of their claims, in some cases.

VI. A CLOSER LOOK AT THE BALANCED APPROACH OF NOTICE AND TAKEDOWN

While no one regulatory policy model will effectively allow governments to control every type of content or activity on the Internet, there is at least one model that shows great promise and should be considered as the foundation for a harmonized approach to global content/activity regulation. This model, called "Notice and Take Down," has two major components: (1) limited immunization from damages, when certain conditions have been met, wherever an involved party lacks control over the content/activity involved; and (2) limited damages (e.g., only injunctive relief), when certain conditions are met, wherever a party has the right and ability to control content/activity but is not the originator of such content/activity, and complies within a reasonable period of time to an adequate notice (or in response to an appropriate knowledge standard) to block or remove such contact/activity.[153] If content/activity is removed by mistake, a process exists for having it returned. Removing third parties from the dispute is only a process for dealing with illegal control/activity once it has been appropriately

152. *Law Enforcers Target "Top 10" Online Scams*, *at* http://www.ftc.gov/opa/2000/10/topten.htm (last visited Aug. 1, 2002).

153. *See* CASEY, *supra* note 50, at 103–104; 17 U.S.C. § 512 (2000).

identified, and is completely unaffected by the nature of content/activity being so regulated.

The Conference Report on the DMCA cites two purposes of Title II.[154] The first is preserving "strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment."[155] Simultaneously, the law is designed to provide "greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities."[156] This law adds a new section (§ 512) to the Copyright Act,[157] limiting the liability of service providers arising from four activities: transitory digital network communications, system caching, information residing on systems or networks at direction of users, and information location tools (e.g., hyperlinks, on-line directories and search engines).[158] The provisions entitle qualified service providers to a complete bar on monetary damages.[159] In addition, Title II restricts the availability of injunctive or other equitable relief.[160] In order to be entitled to these "safe harbor" protections, a party must qualify as a "service provider" under §§ 512(k)(1)(A) and (B), and meet several conditions.[161] A service provider must designate with the Copyright Office an agent that will receive DMCA notifications.[162] The service provider must develop a procedure for processing DMCA notifications and for filing that information on its website.[163] With regard to information residing on systems or networks at the direction of users and information location tools, the service provider cannot have actual knowledge of the infringing content, or be aware of facts or circumstances from which infringement is apparent.[164] If the

154. *See* 144 CONG. REC. 10,048, 10,067 (daily ed. Oct. 8, 1998).

155. *See id*. at 10,067.

156. *See id.*

157. Codified at 17 U.S.C. § 512.

158. *See* 17 U.S.C. §§ 512 (a)–(d) (2000); United States Library of Congress, Copyright Office, *Digital Millennium Copyright Act: U.S. Copyright Office Summary*, 8 & 12, Dec. 1998, *available at* http://www.loc.gov/copyright/legislation/dmca.pdf [hereinafter "Copyright Office Summary"].

159. *See* 17 U.S.C. §§ 512 (a)–(d),(j); *See Copyright Office Summary, supra* note 158, at 9.

160. *See Copyright Office Summary, supra* note 158, at 9.

161. *See* 17 U.S.C. §§ 512 (k)(1)(A),(B); CASEY, *supra* note 50, at 158–159.

162. *See* 17 U.S.C. § 512 (c)(2); CASEY, *supra* note 50, at 158.

163. *See* 17 U.S.C. §§ 512 (c)(2), 512 (i); CASEY, *supra* note 50, at 158.

164. *See* 17 U.S.C. §§ 512 (c)(1)(A)(i)–(ii), (d)(1)(A)–(B); CASEY, *supra* note 50, at 158–159.

service provider obtains knowledge or awareness, it must act expeditiously to remove or disable access to such material.[165] In addition, the service provider cannot receive any financial benefit directly attributable to the infringing activity in a situation where the service provider has the right and ability to control such activity.[166]

Title II also creates a procedure by which a copyright owner may request a federal court to issue a subpoena to a service provider in order to identify an alleged infringer.[167] However, the statute specifically states that it does not condition the availability of the safe harbor provisions on the service provider monitoring its services or affirmatively searching for infringing activity.[168] The protections also cannot be conditioned on the service provider gaining access to, removing, or disabling access to material in cases in which such conduct is prohibited by law.[169]

A notice and takedown procedure is also applied in Section 4 of the EU E-Commerce Directive.[170] Service providers are provided with limited liability in the conduct of caching and hosting activities and when acting as a "mere conduit."[171] The preamble to the E-Commerce Directive states that the liability limitations are necessary to eliminate disparities between member states regarding the liability of service providers and to develop "rapid and reliable procedures for removing and disabling access to illegal information."[172] The preamble suggests that this arrangement "strikes a balance between the different interests at stake and establishes principles upon which industry standards can be based."[173] As in the DMCA, service providers that obtain actual knowledge or awareness of illegal activities have to act expeditiously to remove or disable access to the information.[174] The E-Commerce Directive does not preclude the imposition of injunctions by courts and administrative authorities to remove or disable information deemed to be illegal.[175] Although the E-Commerce Directive seeks greater uniformity in the imposition of liability to service providers and precludes general monitoring

165. *See* 17 U.S.C. §§ 512(c)(1)(A)(iii), (d)(1)(C); CASEY, *supra* note 50, at 159.
166. *See* 17 U.S.C. §§ 512(c)(1)(A)(iii), (d)(2); CASEY, *supra* note 50, at 159.
167. *See* 17 U.S.C. § 512(h); *Copyright Office Summary, supra* note 158, at 9.
168. *See* 17 U.S.C. § 512(m); *Copyright Office Summary, supra* note 158, at 9.
169. *See* 17 U.S.C. § 512(m); *Copyright Office Summary, supra* note 158, at 9.
170. *See* Council Directive 2000/31/EC, 2000 O.J. (L 178) 12–13.
171. *See id.*
172. *Id.*
173. *Id.*
174. *Id.*
175. *Id.*

requirements, it gives EU member states the authority to require monitoring in specific cases and when ordered by national authorities in accordance with national legislation.[176] Additionally, the E-Commerce Directive does not prevent member states from applying, under national law, duties of care to service providers who host information provided by recipients of their service, in order to detect and prevent certain illegal activities.[177]

Jurisdiction remains the biggest obstacle to the effective functioning of an international notice and takedown regime. The barriers to enforcement and adjudication created by jurisdictional difficulties could allow parties to ignore notice and take down orders ("NTO"), or they could promote the development of multilateral treaties that would cause NTO orders to be respected internationally. One form of multilateral treaty arrangement that may be effective is to allow countries to pass and enforce domestic controls within their own countries, but to limit extraterritorial enforcement until a specified percentage of countries had agreed to that control.

Ultimately, the country with the lowest controls could become the economic power of the 21st century, as users and companies servicing such users flock to the most reasonable and economically satisfying system of regulation.

VII. CONCLUSION

Internet service providers facilitating global electronic commerce by bringing together buyers and sellers typically have no knowledge of or control over the activities of their customers. Nonetheless, in an era of 1) rock-bottom barriers to market entry, 2) virtually no relationship between the cost of reaching a customer and the physical distance from buyer to seller, and 3) potential anonymity of Internet users, ISPs are in a unique position to assist law enforcement officials in safeguarding the public welfare and rights holders in protecting their valuable interests. Irrespective of the equity of holding ISPs responsible for the actions of their customers, they have been and will continue to be called upon to aid in controlling content and activity on the Internet. As a practical matter, this has resulted in the imposition of liability for the acts of third party customers or, in the case of the Digital Millennium Copyright Act,

176. *See* Council Directive 2000/31/EC, 2000 O.J. (L 178) 12–13.

177. *Id.*

limitations on liability in exchange for assisting rights holders in their efforts to preserve their economic interests.

In order to foster the business certainty that service providers—from ISPs to e-commerce companies—require, in order to continue investing in infrastructure and services, a harmonized or uniform approach must be taken to the imposition of liability, including setting out qualified limitations on liability. Setting the ground rules, while relying on service providers to design, implement and manage the processes to comply with those rules, will lay a solid foundation on which to build a globally-networked economy fueled by electronic commerce activity.