2001

A Proposal for Removing Road Blocks from the Information Superhighway by Using an Integrated International Approach to Internet Jurisdiction

Catherine P. Heaven

Notes

A Proposal for Removing Road Blocks from the Information Superhighway By Using an Integrated International Approach to Internet Jurisdiction

*Catherine P. Heaven**

Imagine you are the driver of the typical American family. You cruise the Information Superhighway, driving the speed limit in your minivan, the two kids fighting in the back over whether the next website visited should be the WNBA[1] or the NFL[2]. Suddenly, a racecar displaying pornographic pictures in the windows streaks by, traveling at least twice the legal rate of speed. Ten minutes later, police cars follow as fast as their Ford Crown Victorias, Toyota Corollas, and Volkswagen Beetles will carry them. You just shake your head, knowing that the police cars will probably not catch the racecar. In the rare instances where the authorities do catch the racecar, the officers will fight over who has the authority to make the arrest. Their fighting will cause a slowing of the flow of traffic. Thus, in both directions of the highway cars will only move at a crawl.

Questions of jurisdiction and state control over the prosecution of its citizens are increasingly responsible for digital roadblocks. This Article begins by examining the development of the Internet. As cyberspace has evolved, issues of jurisdiction have arisen, as have proposed solutions. Next, this Article describes and analyzes the solutions proposed by the United

* A special thanks to Mary Rumsey for her tireless effort to find Internet sources for the European Union research. Heartfelt thanks to Beth DeCourcy for her support and careful edits, and to Ethan Glass for his uncanny ability to find the words to better express my thoughts in difficult passages.

1. *Women's National Basketball Association Website*, *at* http://www.wnba.com (last visited Oct. 2, 2000).

2. *National Football League Website*, *at* http://www.nfl.com (last visited Oct. 2, 2000).

States and the European Community. Finally, this Article concludes that, under the Outer Space Treaty, the World Wide Web (hereinafter "Web") should be deemed an international space.

I. THE INTERNET AND ITS DEVELOPMENT

A. THE BIRTH OF A GLOBAL PHENOMENON

Formally, the term "Internet" is defined as "the global information system that is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons."[3] In addition, included in this definition is a requirement that the Internet support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) and provide "high level services layered on the communications and related infrastructure."[4] Less technically, the Internet exists, "everywhere and nowhere. . .in the smallest bursts of matter and energy. . .called forth only by the presence of man through the intercession of an Internet provider."[5] Cyberspace is a global network of networks that allows an individual user to exchange information with any computer in the system.[6] This network of networks now entertains millions of users[7] and provides the medium for the transfer of billions of dollars of commerce.[8] Despite its current omnipotence, however, the Internet had a rather humble beginning.

J.C.R. Licklider of the Massachusetts Institute of Technology (MIT) first articulated the conception of social interactions through digital networking in August 1962.[9] He

3. Fed. Networking Comm'n, *Definition of the Internet* (Oct. 24, 1995), *at* http://www.fnc.gov/Internet_res.html.

4. *Id.*

5. Darrel C. Menthe, *Jurisdiction in Cyberspace: A Theory of International Spaces*, 4 MICH. TELECOMM. & TECH. L. REV. 69-70 (1998), *available at* http://www.mttlr.org/volfour/menthe.html.

6. *See* ACLU v. Reno, 929 F. Supp. 824, 830-31 (E.D. Pa. 1996), *aff'd*, Reno v. ACLU, 521 U.S. 844 (1997).

7. Commerce Net Research Center, *World Wide Internet Population*, *at* http://www.commerce.net/research/stats/wwstats.html (last visited Oct. 25, 2000).

8. *See generally* L. Margherio, *The Emerging Digital Economy* at http://www.ecommerce.gov/danintro.htm (last visited Oct. 25, (2000)).

9. *See* BARRY M. LEINER ET AL., A BRIEF HISTORY OF THE INTERNET (authored by the Director of the Research Institute for Advanced Computer Science, Senior

envisioned that computers across the world would be interconnected so users could quickly access any available data and programs from any location with a computer. His "Galactic Network" theory, incredibly, envisioned a system that closely resembles the Internet we use today. The first major step toward the Galactic Network occurred in 1965, when Larry Roberts and Thomas Merrill used the TX-2 computer in Massachusetts to call the Q-32 in California on a low-speed telephone line.[10] This creation of the first wide-area network proved that computers could work together, but it also demonstrated that the telephone system provided an inadequate backbone. Fortunately, Leonard Kleinrock of MIT (and others) remedied the problem by pioneering the use of packets rather than circuits in transferring information.[11]

At about the same time, the Defense Advanced Research Projects Agency (DARPA) hired Licklider to lead its computer research program.[12] Licklider in turn hired Roberts to develop the network concept, which resulted in the ARPANET proposal. In September 1969, after much research and funding requests, the first node on the ARPANET was installed at Kleinrock's Network Measurement Center at UCLA.[13] One month later, the Stanford Research Institute (SRI) connected to the ARPANET and the first host-to-host message was sent from UCLA to Stanford.[14] By the end of 1969, ARPANET had networked four computers. It took only three more years for the ARPANET to be developed to a point of wide use and for its first public demonstration at the International Computer Communication Conference (ICCC). The Internet was born.

As of January 2000, over 242 million people worldwide access the Internet, with a growth rate that projects 490 million users by the end of the year 2002.[15] North America leads the globe in number of users with 120 million, followed by Europe with 70 million.[16] The dominance of Europe and North America

---

Vice President of Internet Architecture and Technology at MCI WorldCom, Senior Research Scientist at the MIT Laboratory for Computer Science, President of the Corporation for National Research Initiatives, Professor of Computer Science at UCLA, among others), *at* http://www.isoc.org/internet/history/brief.html.

10. *See id.*
11. *See id.*
12. *See id.*
13. *See id.*
14. *See id.*
15. Commerce Net Research Center, *supra* note 7, at http://www.commerce.net/research/stats/wwstats.html.
16. *Id.*

can be reflected in the percentage of English speakers on the Internet (47.6%) and speakers of other European languages (29.2%) on the Net, compared with all other languages (23.2%).[17] However, this distribution of languages could change dramatically in the next few years. In general, any common Internet search is likely to pull many non-English language sites. Specifically, Asia and the Pacific Rim are expected to have a phenomenal growth rate of approximately 422% in the next five years, with an estimated number of users reaching 228 million by 2005.[18]

The growth of the Internet has already facilitated the globalization of financial markets and the rise of electronic commerce.[19] Individual companies such as Cisco, Dell and General Electric have collectively generated seventeen billion dollars in commerce over the past three years.[20] These companies represent a small proportion of e-commerce; that is, a 1999 survey predicted that e-commerce will generate 1.3 trillion dollars of revenue by 2003.[21] In additional to retail, nearly ninety percent of users surf the internet to gather news or information.[22]

For all of its potential to provide information and opportunities for commerce, the Internet also has a dark side. Businesses cite several problems as potential inhibitors of future growth, which include a lack of a predictable legal environment, the potential for taxation, and Internet security.[23] In addition, cybercrime against governments, businesses, and individuals is becoming more difficult to regulate.[24] A recent FBI study showed that between 1997 and 1999, Fortune 500

17. Global Reach, *Global Internet Statistics (by Language)*, *at* http://www.glreach.com/globstats/index/php3 (last visited Oct. 25, 2000).

18. Commerce Net Research Center, *supra* note 7, at http://www.commerce.net/research/stats/wwstats.html.

19. Joseph W. Dellapenna, *Law in a Shrinking World: The Interaction of Science and Technology with International Law*, 88 KY. L.J. 809, 837 (1999-2000).

20. See L. Margherio, *supra* note 8, at http://www.ecommerce.gov/danintro.htm.

21. ActivMedia Research, *Global Ecommerce to Top USD95 Billion in '99* [NUA Internet Surveys], *at* //www.nua.ie/surveys/index.cgi? f=VS&art_id=905354987&rel=true (Jun. 28, 1999).

22. Kate Maddox, *Information Still Killer App on the Internet*, *in* ADVER. AGE (Oct. 6, 1997), *available at* http://adage.com/interactive/articles/19971006/article7.html.

23. *See* L. Margherio, *supra* note 8, at http://www.ecommerce.gov/danintro.htm.

24. *See International Chamber of Commerce Conference on Cybercrime, Alliance Against Commercial Cybercrime*, *at* http://www.infowar.com/conf/99conf_121799a_j.shtml (Dec. 7, 1999).

companies lost over $360 million due to computer crime.[25] The Internet was accurately summed up as providing "vast opportunities for socially beneficial endeavors, but also a potential way for individuals to commit unlawful acts anonymously and at low risk, such as unauthorized access to private communications, . . . financial fraud, the distribution of child pornography and the piracy of creative materials."[26]

B. NATION-BASED JURISDICTION AND AN INTERNATIONAL NETWORK

In the international community, a limit is placed on jurisdiction requiring States to refrain from actions that encroach on another State's sovereignty.[27] Jurisdiction has been primarily based on physical geography; the Internet, as a network of networks, destroys these classic notions by transcending geographic constraints.[28] A connection between a physical location and an Internet address is both unnecessary and unimportant, in some instances, such a connection is non-existent as many enterprises solely exist digitally.[29] The same technology that gives global consumers access to a virtual Nordstrom's shoe department also allows cybercriminals to commit offenses across international borders that are difficult to successfully prosecute.[30] Discrepancies in regulations and concepts of jurisdiction in the international community challenge law enforcement officials[31] as they try to appropriately assert their historical right to control crime within their borders stemming from extraterritorial acts.[32]

---

25. Christine Gregoire, *Law Enforcement Challenges in Cyberspace*, 34 PROSECUTOR 28, 29 (Sept. - Oct. 2000).

26. UNESCO Observatory on the Information Society, *G8 Paris Conference: Paris, 15th-17th May 2000*, *at* http://webworld.unesco.org/webworld/observatory/in_focus/120500.shtml (last visited Sept. 27, 2000).

27. *See* IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 301 (5th ed. 1998).

28. *See* Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 168-69 (S.D.N.Y. 1997).

29. Tapio Puurunen, *The Legislative Jurisdiction of States Over Transactions in International Electronic Commerce*, 18 J. MARSHALL J. COMPUTER & INFO. L. 689, 690 (2000) (citing D.R. Johnson & D. Post, *Law and Borders – The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1371 (1996)).

30. *See* ENLIST, *Computer Crime Commentary*, *at* http://195.40.43.15/enlist/subjects/is/resources/computer_crime.html (last visited Sept. 27, 2000).

31. *Id.*

32. Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOBAL LEGAL STUD. 475, 476 (1998).

Generally, if an activity takes place within a territory, that territory has the jurisdiction to create laws to regulate the activity.[33] This form of jurisdiction, by its very definition, excludes criminal and tortious acts that cross international borders. If the primary effect of an outside act is felt inside the territory, the injured party can claim objective territoriality.[34] Objective territoriality is also known as the effects doctrine, which grounds jurisdiction in the location of the injurious effect.[35] This form of jurisdiction is not effective in regulating the Internet, however, because placing information on the Internet that is broadcast internationally is generally recognized as insufficient for personal jurisdiction.[36]

Without a clear argument for following one of the classic types of international jurisdiction, territories have turned to regulating individual parties. International law does not prohibit concurrent jurisdiction over international criminal and civil matters, but in fact considers it the norm.[37] This unclear position on potential liability may encourage States to enact stringent Internet regulations to protect their consumers;[38] furthermore, this also makes it very difficult for a trader to predict how States will respond to legal actions that are filed.[39] For the wary consumer attempting to legally negotiate the Internet, caution must be used while both uploading and downloading information.

Nation-states attempting to control the proliferation of criminal activity on the Internet through territory-based regulations face two alternatives, i.e. they can regulate the uploader or the downloader. If governments choose to regulate the uploading of information on the Internet, they run into the problem of limiting freedom of expression by instituting limitations based on other countries' displeasure with website

33. Menthe, *supra* note 5, at 71-72.

34. *Id.* at 72.

35. PETER MALANCZUK, AKENHURST'S MODERN INTRODUCTION TO INTERNATIONAL LAW 110-11 (7th ed. 1997).

36. *See* Eric Schneiderman & Ronald Kornreich, *Personal Jurisdiction and Internet Commerce*, N.Y.L.J., June 4, 1997 at A4; Note, *World-Wide Volkswagen, Meet the World Wide Web: An Examination of Personal Jurisdiction Applied to a New World*, 71 ST. JOHN'S L. REV. 403 (1997).

37. *See* BROWNLIE, *supra* note 27, at 314.

38. *See e.g.* Statement of Minnesota Attorney General's Office on Internet Jurisdiction, *Warning to All Internet Users and Providers*, *at* http://www.ag.state.mn.us/home/consumer/consumernews/OnlineScams/memo.html (last visited Oct. 27, 2000).

39. Puurunen, *supra* note 29, at 733.

content.[40] Focusing on the downloader, or information receiver, also presents significant problems. Governments can penalize in-state users that participate in illegal transactions or download banned content,[41] but evasion will still be possible.[42] For example, censorship has been the policy choice of Singapore,[43] but the proliferation of cyberporn and other objectionable sites makes their attempts at regulation ineffective.[44] In addition, pressuring Internet sites to modify their content because of censorship has spillover effects in other countries by preventing citizens from downloading information that is legal in their countries.[45] Reducing this spillover effect is best achieved through inter-state harmonization of Internet regulations.[46]

C. IN SEARCH OF A SOLUTION TO THE JURISDICTIONAL PROBLEM

1. Approaches to Internet Regulation

Individual nations and groups of nations have been working to develop solutions to the questions posed by Internet jurisdiction. The current policy debate in the United States over who should have jurisdiction over cybercrime[47] exemplifies the current struggle between nation-states as they decide whether to create their own laws or join international attempts at regulation. The European Union is also developing an approach to Internet jurisdiction. In a number of initiatives, the European Community has created the beginnings of a global standard,[48] a

40. Menthe, *supra* note 5, at 82.

41. Goldsmith, *supra* note 32, at 481.

42. *Id.* at 482.

43. *See* Garry Rodan, *The Internet and Political Control in Singapore*, 113 POL. SCI. Q. 63, 77-78 (1998).

44. Joseph C. Rodriguez, *A Comparative Study of Internet Content Regulations in the United States and Singapore: The Invincibility of Cyberporn*, 1 ASIAN-PAC. L. & POL'Y J. 1, 24 (2000).

45. Goldsmith, *supra* note 32, at 488-89.

46. *Id.* at 490.

47. *See generally* Laura Ann Forbes, *A More Convenient Crime: Why States Must Regulate Internet-Related Criminal Activity Under the Dormant Commerce Clause*, 20 PACE L. REV. 189 (1999).

48. *See generally Resolution on the Communication from the Commission on Globalisation and the Information Society: The Need for Strengthened International Coordination*, 1999 O.J. (C 104) 128 [hereinafter International Coordination Resolution].

solution that some feel infringes upon individual rights.[49]

In addition to State action on the issue, prior treaties and current legal theories point to a global solution to regulating cyberspace through an international treaty that addresses illegal actions and censorship. Prior treaties that address Outer Space[50] and the Law of the Sea[51] set the foundation for the concept of international space as the "common heritage of mankind."[52] The "common heritage of mankind" (CHM) has been defined as a principle that extends management rights of an area to everyone, while giving ownership to no one.[53] The global community regulates the area using treaties and norms of international law.[54]

In addition to the framework established by the concept of CHM, a principle known as the "universality principle" provides a model for the type of treaty that could be established internationally to regulate the Internet. The universality principle allows any State to punish individuals for committing offenses of international concern even if the State has no jurisdictional links to the area the crime took place or the persons involved.[55] Currently, it has limited application to international wrongs such as crimes against peace, crimes against humanity, and war crimes.[56] Applying the universality principle to the Internet and agreeing on a global standard for a minimum level of consumer protection would give all States the ability to regulate international transactions.[57] Due to the varying approaches States have to consumer protection, a universal standard would be difficult to agree upon and

49. *See* The Global Internet Liberty Campaign, *Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime*, *at* http://www.gilc.org/provace/coe-letter-1000.html (Oct. 18, 2000).

50. *See* Treaty on Principles Governing the Activities of States in the Exploration and use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, art. 1, 18 U.S.T. 2410, 2412-13, 610 U.N.T.S. 205, 207-08 [hereinafter Outer Space Treaty].

51. *See* Convention on the Law of the Sea, Dec. 10, 1982, art. 136, 21 I.L.M. 1261, 1293.

52. Menthe, *supra* note 5, at 86.

53. Christopher C. Joyner, *Legal Implications of the Concept of the Common Heritage of Mankind*, 35 INT'L & COMP. L.Q. 190, 191 (1986).

54. *Id.*

55. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 404 (1986).

56. *See, e.g.*, G.A. Res. 95(I), U.N. GAOR., 1st Sess., pt. II, at 188 (1946); Treatment of Prisoners of War, Aug. 12, 1949, No. 972, 75 U.N.T.S. 135; Convention relative to the Treatment of Civilian Persons in Time of War, Aug. 12, 1949, No. 973, 75 U.N.T.S. 287.

57. Puurunen, *supra* note 29, at 730.

implement in the current international system.[58]

Although acknowledging that difficulty is a necessary and important step, it is highly unlikely that individual State action is capable of developing a logical approach to jurisdiction in cyberspace.[59] Territorial regulation of the Internet will succeed only in creating inconsistent regulations and difficult spillover effects.[60] Therefore, international harmonization or a new set of criteria for determining jurisdiction over claims may be necessary to resolve the current Internet regulation dilemma.[61]

2. On One Hand: The U.S Response to Internet Jurisdiction

Debates over who has jurisdiction to hale individuals into court for criminal charges relating to Internet behavior have been raging in the United States,[62] thus providing a concrete example of the types of jurisdictional questions that become more nebulous when they are applied to the International arena. The spectrum of policy choices for Internet jurisdiction can be exemplified by engaging in three legal examinations. First, this Part discusses the theoretical role of states' rights in the development of criminal sanctions.[63] Second, this Part turns to the actions of a state that broadly construe the concept of personal jurisdiction on the Internet.[64] Finally, this Part analyzes the former Attorney General's proposal for prevention of Internet crime and enforcement of current sanctions.[65]

a. Cybercrime Regulated through the Dormant Commerce Clause?

The area of criminal law is a startling example of the potential for jurisdictional complexity regarding the Internet because of its ability to pull individuals into jurisdictions without the minimum contact requirement for criminal prosecutions that is required in civil litigation.[66] The potential

58. *See* Matthew S. Yeo & Marco Berliri, *Conflict Looms Over Choice of Law in Internet Transactions*, 4 ELECTRONIC COM. & L. REP. 85, 89 (1998).

59. Puurunen, *supra* note 29, at 745.

60. Goldsmith, *supra* note 32, at 478.

61. Puurunen, *supra* note 29, at 745.

62. *See generally* Forbes, *supra* note 47.

63. *Id.*

64. State v. Granite Gate Resorts, Inc., 568 N.W. 2d 715, 718 (Minn. Ct. App. 1997), *aff'd*, 576 N.W.2d 747 (Minn. 1998).

65. *See generally* Janet Reno *Attorney General's Cyber Crime Plan*, 34 PROSECUTOR 21 (2000).

66. Terrence Berg, *State Criminal Jurisdiction in Cyberspace: Is There a*

for abusing the "long arm"[67] of criminal law is so great that even proponents for individual state regulation of intrastate Internet crime believe the "purposeful availment"[68] and "minimum contacts"[69] tests should be applied to criminal activities in any jurisdictional analysis.[70] Setting aside the problem of minimum contacts, the heart of the argument for retaining state autonomy in Internet crime regulation revolves around the notion that criminal law is one of the fundamental and classic domains of states' rights,[71] a right that should not be intruded on for fear of the creation of a general federal police power.[72] Proponents of the states' rights approach argue that the link between their regulation of Internet crime and interstate commerce is as attenuated as federal regulation of guns in schools,[73] and that as technology-based crime continues to increase, states will see a weakening of their constitutionally-given police power.[74]

Using this approach, each state would have jurisdiction over Internet crime that took place entirely within the state's borders.[75] While this theory may appear to preserve the classic notion of state-regulation of criminal activity[76] and Constitutional distinctions inherent in the U.S. system, it does not address the issues raised by interstate cybercrime, let alone international cybercrime. In addition to its limited focus, allowing the Dormant Commerce Clause to control Internet regulations leaves individual states with the power to create all-encompassing prohibitions that impinge on the sovereignty of other states.[77]

b. A State Attempt from the Land of Ten Thousand Lakes

If individual states are given discretion to create and enforce criminal statutes regulating Internet behavior, any

---

Sheriff on the Electronic Frontier? 79 MICH. B.J. 659, 662 (2000).

67. Forbes, *supra* note 47, at 190-91.

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

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

70. Forbes, *supra* note 47, at 190-91.

71. United States v. Lopez, 514 U.S. 549, 564 (1995).

72. *Id.* at 567.

73. *See id.*

74. Forbes, *supra* note 47, at 218.

75. *See generally* Berg, *supra* note 66 (desecribing state attemtps to prosecute cybercrime).

76. *See generally* United States v. Lopez, 514 U.S. 549 (1995).

77. *See e.g.* Statement of Minnesota Attorney General, *supra* note 38, at http://www.ag.state.mn.us/home/consumer/consumernews/OnlineScams/memo.html.

number of permutations of current penalties are possible; the most troubling are those states that claim jurisdiction over persons outside of their borders.[78] Minnesota represents the pinnacle of jurisdictional infringement on other states, issuing a statement on the Internet to all users who come into contact with Minnesotans.[79] The statement warns, "Persons outside of Minnesota who transmit information via the Internet knowing that information will be disseminated in Minnesota are subject to jurisdiction in Minnesota courts for violations of state criminal and civil laws."[80] The notice then reinforces the statement with the state's long-arm statute and Minnesota case law that permitted jurisdiction over cases the Attorney General equates with cybercrime.[81]

This sweeping interpretation of Minnesota's jurisdiction over the Internet has been reinforced in the court system. In 1997, the Minnesota Court of Appeals affirmed a district court's finding of personal jurisdiction over a n out-of –state website owner based on advertisements he placed on his website that was accessed by over 200 computers in Minnesota.[82] The Court considered the website a form of advertisement that indicated the defendant's intent to serve the area, and the intent to serve was illegal when applied to the gambling business of the defendant.[83] Minnesota demonstrates the danger that sweeping jurisdictional claims can have for persons operating websites and shows how creating statutes in an unregulated national system will infringe upon other state's jurisdictional rights.

c. A Federal Solution

Examining the reaction of the federal government to the increasing problems surrounding jurisdiction and the Internet is important not only because it shows the difficulty of superimposing multiple territorial statutes on a homeless network, but also because the United States has a dominant global Internet presence.[84] That is, Americans constitute a

78. Menthe, *supra* note 5.

79. *See* Statement of Minnesota Attorney General, *supra* note 38, at http://www.ag.state.mn.us/home/consumer/consumernews/OnlineScams/memo.html.

80. *Id.*

81. *Id.*

82. State v. Granite Gate Resorts, Inc., 568 N.W. 2d 715, 718 (Minn. Ct. App. 1997), *aff'd*, 576 N.W.2d 747 (Minn. 1998).

83. *Id.* at 719.

84. Rodriguez, *supra* note 44, at 46.

majority of Internet users,[85] and the United States will likely provide most of the content on the global network.[86]

Lawmakers at the federal level have vacillated in the last few years over the approach they want to take in regulating the Internet. In July 1997, the United States adopted a "hands off" policy toward the Internet to promote growth and diversity of ideas, arguing that users had the capability to shield themselves from content they deemed offensive.[87] A year later, Congress passed bills focused on policing the Internet, specifically in the areas of child pornography and obscenity.[88] While the federal government continues to try to strike a balance between protecting expression and the marketplace of ideas[89] and protecting citizens from illicit materials,[90] there has been a push to increase the federal government's influence over Web regulations.[91]

The arguments for increased federalization of Internet regulation are strengthened by cases such as those from Minnesota. The federal government argues that Internet communications are articles of interstate commerce,[92] and that the Internet, labeled the Information Superhighway, is the virtual equivalent of a paved highway, a classic example of a federally regulated commercial channel.[93] This premise has been reinforced in the court system, with a holding that inconsistent state regulations would have a chilling effect on commerce.[94]

While the debate on commerce continues to occupy space in the scholarly journals, former U.S. Attorney General Janet Reno forged ahead in the area of cybercrime. Her Cyber Crime Plan involved the development of a response network with federal, state, and local investigators equipped to keep pace with high-tech criminals and provide information to other jurisdictions

85. Commerce Net Research Center, *supra* note 8, at http://www.commerce.net/research/stats/wwstats.htm..

86. Rodriguez, *supra* note 44, at 46.

87. *See* William J. Clinton & Albert Gore, Jr., *A Framework for Global Electronic Commerce*, at http://www.iitf.nist.gov/eleccomm/ecomm.htm (last visited Mar. 26, 2001).

88. *See* ACLU v. Reno, 929 F. Supp.824, 844 (E.D. Pa. 1996), *aff'd*, Reno v. ACLU, 521 U.S. 844 (1997).

89. Rodriguez, *supra* note 44 at 3.

90. *Id.* at 34.

91. *See e.g., ACLU v. Reno*, 929 F. Supp. at 844.

92. Forbes, *supra* note 47, at 218.

93. *Id.*

94. *See* Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 174 (S.D.N.Y. 1997).

around the clock.[95] In creating her plan, she focused on fostering the emerging value placed on locating and prosecuting cybercriminals while also maintaining classic values such as freedom of speech, privacy, and growth of the free market.[96] The former Attorney General's approach to cybercrime regulation intertwines the federal and state governments[97], exemplifying the complex position of U.S. policymakers. In turn, the United States' position on the Internet, with a debate over how commerce should be regulated on the Internet combined with the beginning of a comprehensive solution to the problem of cybercrime, represents a microcosm of the debate taking place internationally on the growth and regulation of the Internet.

3. On the Other Hand: The European Community's Response to Regulating the Information Age

a. The European Union Data Protection Directive

Privacy law has developed concurrent with the growth of and dependence upon the electronic transmission of data.[98] Created as a response to the increase in cross-border transfer of information within the European Union,[99] the European Union Data Protection Directive (EUDPD) was adopted in 1995 and took effect in 1998.[100] Although the EUDPD was drafted in the early 1990s, before the Internet was viewed as a data collection tool,[101] the EUDPD applies generally to the processing of any personal data collected,[102] including websites that collect personal information. The protection principles of the EUDPD apply to the transfer of all data to countries or territories out of

95. Reno, *supra* note 65, at 25.

96. *Id.*

97. *Id.*

98. *See* John Mullen, E.U. Data Protection and the U.S. Safe Harbors 1 (Oct. 26, 2000) (unpublished conference materials, on file at Fredrikson & Byron, P.A.).

99. *Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Council Directive 95/46, 1995 O.J. (L281) 31, *available at*, http://europa.eu.int/eur-lex/en/lif/data/1995/en_395L0046.html (last visited Oct. 17, 2000), [hereinafter Council Directive 95/46/EC].

100. *Id.* at 49.

101. Peter P. Swire, *Of Elephants, Mice and Privacy: International Choice of Law and the Internet*, 32 INT'L. LAW. 991, 1008 (1998).

102. *Id. See generally* Kevin Bloss, Note, *Raising or Razing the E-Curtain?: the EU Directive on the Protection of Personal Data*, 9 MINN. J. GLOBAL TRADE 645 (2000).

the European Economic Areas.[103]

> In order to achieve a safe harbor from the regulations as a non-EU entity, the organization must satisfy seven principles: 1) provide notice to the individual of: a) of the purposes for collection, b) how to contact the organization, c) what other parties will receive the information, and d) choices for limiting disclosure; 2) have either opt-out or opt-in provisions available for all data collection, with opt-in as the mandate for sensitive information; 3) apply all notice principles to the use of information by 3rd parties; 4) maintain access and ability to correct information; 5) take reasonable precautions to secure the information against lost or misuse; 6) take reasonable steps to ensure the information is accurate and current; and 7) provide mechanisms for the investigation and resolution of individual's claims.[104]

Enactment of the EUDPD does not actually take place through the European Union, but is effectuated by having all member countries pass laws in their home states and making those subject to their jurisdiction operate under the State law.[105] The laws will differ from one another in both large and small ways, with potential problem areas surrounding sensitive data and data transfer outside of the European Union.[106] Individual states are allowed to modify the proposal when enacting the legislation in their governments for: 1) national security; 2) defense; 3) public security; 4) crime enforcement; 5) an important economic interest of a Member State; 6) monitoring or inspection in cases of official authority; and 7) the protection of data subject to the right of freedom to others.[107]

Problems arise when examining choice of law and jurisdiction issues. First, there is a question of which country's law applies when an institution is headquartered in one country and operates businesses in another.[108] That difficulty is only compounded when an entity is located in multiple EU countries, a situation where most likely the strictest privacy protocol will apply in all countries where the entity is located.[109] The complexity increases further when the entity offending the privacy laws is located outside of a EUDPD country. Finally, there is a possibility that U.S. websites that collect information from citizens of EU countries are subject to the EU courts for

103. Mullen, *supra* note 98.
104. *Id.*
105. *See generally* http://www.privacyexchange.org (containing information on data protection laws and decisions of agencies on the subject matter).
106. Swire, *supra* note 101, at 1002.
107. *See Council Directive 95/46/EC, supra* note 99.
108. Swire, *supra* note 101, at 1007.
109. *Id.*

violations of their privacy directives.[110] The EUDPD, while it has taken great strides toward instituting measures to protect information about individuals, will still face many difficult choice of law and jurisdictional questions as long as States enact their own, discrepant laws.

b. European Committee on Crime Problems Committee of Experts on Crime in Cyber-Space

The Council of Europe made progress in the field of international cybercrime regulation when it released the first draft of an international convention in April 2000.[111] In a resolution predating the proposal, the European Parliament asserted its desire to create a legislative approach that is both timely and flexible to accommodate developing technology,[112] and allow for open access to the Internet without U.S. jurisdiction over the Internet as a whole.[113]

The Crime in Cyberspace[114] draft that followed is a significant step toward the first international treaty to regulate computer systems and criminal offenses.[115] Once completed, it will require future Parties to provide each other with assistance in the collection of evidence, location of offenders, and extradition, as well as establish national contact points continuously available for handling such requests.[116] The treaty will also include a section on content-related offenses, including child pornography and copyright law.[117]

Jurisdiction will be founded on whether the offense is committed in the territory or by a national, and disputes are to be settled through consultation.[118] Extradition will be handled by including cybercrime as an extraditable offense under existing treaties.[119] It is important to note that the current draft

110. *Id.* at 1008.

111. *See generally* Council of Europe, *Draft Convention on Cyber-crime, No. 19, available at* http://cybercrimes.net/CouncilEurope/maindraft.html (last visited Mar. 14, 2001).

112. International Coordination Resolution, *supra* note 48.

113. *See generally Draft Convention on Cyber-Crime No. 19,* http://cybercrimes.net/CouncilEurope/maindraft.html, *supra* note 111.

114. *See generally id.*

115. Resolution on the Communication from the Commission on Globalisation and the Information Society: The Need for Strengthened International Coordination, 1999, O.J. (C 104) 128.

116. *Draft Convention on Cyber-crime No. 19, supra* note 111.

117. *See id.* at 4-5.

118. *Id.* at 8.

119. *Id.* at 9.

of the treaty requires participating Parties to pass their own legislative measures concerning these topics, desiring but not requiring that the criminal statutes passed are uniform.[120] The treaty aims to be legally binding, finalized by December 2000, and open for signature autumn 2001.[121]

On October 2, 2000, the Council of Europe released a second draft of its proposal for a comprehensive solution to the problem of international cybercrime.[122] The proposal has a sweeping scope, purporting to include "any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and any other entity that processes or stores computer data on behalf of such communication service or users of such service."[123] The Draft on Cyber-Crime (Draft) requests that each participating Party pass legislative and other measures that establish criminal and other penalties for offenses relating to: 1) illegal access and interception of data; 2) data interference; 3) system interference; 4) the production, sale, import, and distribution of illegal devices; 5) computer-related forgery; 6) computer-related fraud; 7) child pornography; 8) copyright infringement; 9) accomplice liability; and 10) corporate liability.[124] In order to enforce the proposed criminal statutes, procedural methods for cooperation are detailed in the proposal,[125] including a designated point of contact available twenty-four hours a day, seven days a week, to ensure immediate assistance in the investigation of computer-related offenses.[126]

The Council has invited all member States, as well as non-member states that have participated in the process, to ratify the Draft, either with or without reservations.[127] Once the Draft is ratified, the Parties may establish jurisdiction over offenses committed: 1) in its territory; 2) on-board a ship flying the flag of the Party; 3) on-board an aircraft registered with the Party; 4) on board a satellite; or 5) by one of its nationals, if: a) the offense has criminal penalties in the home State; or b) the offense is

120. *Id.* at 6.
121. *Id.* at 1.
122. Council of Europe, *Draft Convention on Cyber-crime No. 22, Rev. 2, available at* http://conventions.coe.int/treaty/en/projects/cybercrime22.htm (last visited Mar. 14, 2001).
123. *Id.* at 3.
124. *Id.* at 3-6.
125. *Id.* at 7-16.
126. *Id.* at 16.
127. *Id.* at 17.

committed outside the State's territorial jurisdiction.[128] Each Party has the power to sign the Draft with reservations in regard to jurisdiction, and in cases of overlapping jurisdiction, the Parties will consult to determine where the trial will be located.[129]

The Draft has met with strong criticism from groups in the international community such as the ACLU, Canadian journalists for Free Expression, Digital Freedom Network, and many others.[130] In a letter addressed to the Council of Europe, these groups raise numerous concerns about the breadth and scope of the regulations.[131] For example, Internet Service Providers raised an objection to the provisions that require the retaining of records of the activities of consumers; provisions (Articles 17, 18, 24, 25) that the organizations believe contradict the basic principles of the Data Protection Directive.[132] These groups believe that the Draft gives law enforcement agencies the power to seize information from individuals and organizations without the appropriate due process limitations and investigative procedures necessary to safeguard rights.[133]

Others have pointed out the expansion of the extradition portions of the Draft and the requirement that those indicted process their own data to withdraw the "relevant" portions as encroach on the rights of the accused.[134] In addition, the Draft is no longer limited to the Council of Europe and drafting countries, but will be opened to all countries once it becomes effective.[135] This sweeping jurisdiction without participation in the process, along with an overly aggressive stance on prosecution for cyber-crime, calls into question the validity of a region-based solution to a global phenomenon.

128. *Id.* at 10.

129. *Id.*

130. *See* Global Internet Liberty Campaign, *Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime*, 4-7, *at* http://www.gilc.org/privacy/coe-letter-1000.html (last visited Mar. 14, 2001).

131. *See generally id.*

132. *Id.* at 1.

133. *Id.* at 2.

134. David Banisar, *Commentary; Cybercrime Treaty: Take Two*, SECURITYFOCUS NEWS, Oct. 8, 2000, at 1, *at* http://www.securityfocus.com/commentary/98 (last visited Oct. 25, 2000).

135. *Id.* at 2.

II. HOW HAS GLOBAL SPACE BEEN REGULATED?

A. INTERNATIONAL SPACE THEORY

The concept of regulating technology that is rapidly changing global communication through international law is in a sense ironic because many scholars consider international law primitive.[136] International law has not been dominant in the field of science and technology, with participating countries only drafting a few treaties on the subject.[137] However, through treaties regulating the sea and outer space, a theory of "international spaces" has developed.[138] According to the theory of international spaces, nationality, not territory, is the basis for jurisdiction.[139] Thus, the person who created or controls the website or links to websites attaches his or her nationality to the site and creates virtual islands,[140] much like how flags created an island of jurisdiction for ships at the beginning of the development of the Law of the Sea.[141] The nationality of individuals surfing the Web can be viewed as an anchor of jurisdiction in cyberspace, a nonphysical,[142] non-territorial virtual community.[143] The Web itself has the potential to be classified using more global terminology.

B. THE COMMON HERITAGE OF MANKIND

Global commons are areas outside of the jurisdiction of nations, whether singularly or in associations.[144] The theory behind global commons and Common Heritage Mankind (CHM) is *res communes*: all nations should benefit from the resources that are recovered from areas in which all nations have an interest.[145] According to CHM principles, no one nation owns

136. Dellapenna, *supra* note 19, at 859.
137. *Id.* at 831.
138. Menthe, *supra* note 5, at 70.
139. *Id.* at 83.
140. *Id.* at 93.
141. *Id.*
142. *Id.* at 85.
143. *Id.* at 96.
144. Phillip E. Wilson, Jr., *Barking Up the Right Tree: Proposals for Enhancing the Effectiveness of the International Tropical Timber Agreement*, 10 TEMP. INT'L & COMP. L.J. 229, 232 (1996).
145. Joan Eltman, *A Peace Zone on the High Seas: Managing the Commons for Equitable Use*, 5 INT'L LEGAL PERSP. 47, 64 (1993).

areas that have the CHM distinction.[146] Instead, the international community, through treaties, norms, and agreements, collectively regulate the area for the benefit of all parties.[147] Under CHM, "mankind" takes on a set of priorities distinct from the summation of individual nation-state interests.[148] Examples of global commons, or CHM spaces, include outer space,[149] Antarctica,[150] and the high seas.[151] Most authorities agree that there are five elements of CHM: 1) the CHM cannot be appropriated; 2) all states manage the resources in the CHM; 3) benefits from exploitation of the resources in the CHM area are shared; 4) the CHM area is used for peaceful purposes only; and 5) the CHM should be preserved for future generations.[152]

Developing nations favor a broad CHM application, arguing that it is crucial to a reformulation of the existing geopolitical order.[153] For that same reason, developed states believe that CHM should not diminish or alter in a nation's freedom to explore and exploit both the sea and outer space in any way.[154] This inherent difference in interpretation is analogous to the "tragedy of the commons,"[155] a theory which states that any communal resources will be subject to overuse by those able to exploit them.[156] In this communal situation, the argument is that wealthy and powerful members of the collective will push through rules that favor them, often at the expense of the

146. Christopher C. Joyner, *Legal Implications of the Concept of the Common Heritage of Mankind*, 35 INT'L & COMP. L.Q. 190, 191 (1986).

147. *Id.*

148. Harminderpal Singh Rana, *The "Common Heritage of Mankind" & The Final Frontier: A Revaluation of Values Constituting the International Legal Regime for Outer Space Activities*, 26 RUTGERS L.J. 225, 229 (1994).

149. *See generally* Outer Space Treaty, *supra* note 50.

150. *See generally* Antarctic Treaty, Dec. 1, 1959, art. VIII § 1, 12 U.S.T. 794, 402 U.N.T.S. 71.

151. *See generally* Convention on the Law of the Sea, *supra* note 51, at 1293.

152. Barbara Ellen Heim, Note, *Exploring the Last Frontiers for Mineral Resources: A Comparison of International Law Regarding the Deep Seabed, Outer Space, and Antarctica*, 23 VAND. J. TRANSNAT'L L. 819, 827 (1990).

153. Gennady M. Danilenko, *The Concept of the "Common Heritage of Mankind" in International Law*, 13 ANNALS AIR & SPACE L. 247, 249 (1988).

154. Grier C. Raclin, *From Ice to Ether: The Adoption of a Regime to Govern Resource Exploitation in Outer Space*, 7 NW. J. INT'L L. & BUS. 727, 738 (1986).

155. *See generally* Garrett Hardin, *The Tragedy of the Commons*, 162 SCIENCE 1243 (1968) (arguing that the population problem, among others, has no technical solution because participants perceive marginal individual rewards of exploiting the commons, while the costs are less salient to the participants because they are distributed among the group of participants).

156. *See id.* at 1244-45.

group.[157] This effect can be lessened by relatively equal access among all users of the particular resource.[158] Even with these potential problems, the CHM principle has been applied to outer space treaties.

C. OUTER SPACE TREATIES

The United Nation's Committee on the Peaceful Uses of Outer Space (COUPOS) drafted the first Outer Space Treaty in 1967.[159] This treaty has formed the basis for other agreements concerning the exploration of space.[160] The treaty makes explicit its overarching goal to leave outer space a free zone for exploration and use by everyone without discrimination and according to international law.[161] Viewing the Outer Space treaty as a whole, a few basic principles appear: 1) Activities must be conducted in the interest and benefit of all countries, with a general prohibition on appropriation and militarization;[162] 2) States are responsible for, and should be in reasonable control of, objects launched under their authority;[163] and 3) international mutual assistance and cooperation are obligatory in outer space activities.[164]

The Moon Treaty, an outgrowth from the first Outer Space Treaty, is the first theory to give force to the CHM principle.[165] Article 11 of the Moon Treaty states that, "the moon and its natural resources are the common heritage of mankind. . .not to be subject to national appropriation."[166] In addition, the treaty mandates that the surface and subsurface of the moon cannot become the property of any party.[167] This sweeping language classifies the moon as the collective possession of the people of Earth.[168]

---

157. *See* Eric A. Posner, *Law, Economics and Inefficient Norms*, 144 U. PA. L. REV. 1697, 1741-42 (1996).

158. *See id.*

159. *See generally* Outer Space Treaty, *supra* note 50.

160. *See* Joseph A. Bosco, *International Law Regarding Outer Space—An Overview*, 55 J. AIR L. & COM. 609, 614 (1990).

161. Outer Space Treaty, *supra* note 50, at 2410.

162. Rana, *supra* note 148, at 245.

163. *Id.*

164. *Id.*

165. Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, *opened for signature* Dec. 18, 1979, arts. 1(1), 3, 4, 6, 11, 14, 1363 U.N.T.S. 22, 22-26 [hereinafter Moon Treaty] (declaring moon to be CHM).

166. *Id.* at 25.

167. *Id.*

168. Heidi Keefe, Essay, *Making the Final Frontier Feasible: A Critical Look at*

This evolution of international treaties toward CHM has not been met without criticism. The Moon Treaty itself has been subject to the criticisms that it is "insufficient in scope, ineffective for control, and unavailing for implementation and enforcement for the purposes of regulation."[169] To reinforce the argument that it is insufficient in scope, some literalists have read the treaty's text and concluded that since its sweeping language does not include individual exploitation of the moon's resources, it effectively prohibits governments from taking possession of celestial resources, but allows private individuals free reign.[170] A final structural criticism of the Moon Treaty is that it does not establish an international regime to enforce its directives, but instead requests that the States-Parties do so.[171]

On a theoretical level, additional criticisms have been leveled against the CHM provisions of the Moon Treaty. One such criticism is that a lack of sovereignty or ownership by Parties over territory in outer space prevents the formation of a stable environment that would allow individuals with the resources to explore the area.[172] Perhaps more importantly, if Parties decide to risk exploration in an area of universal ownership, there is ample opportunity for exploitation that other Parties might ignore in the name of international cooperation.[173] Thus, the CHM principle, while attractive and arguably necessary for newly defined international spaces, requires a stable structure and detailed statutes to balance its highly conceptual vision of what a global community can aspire and grow to be.

---

the Current Body of Outer Space Law, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 345, 366-67 (1995).

169. Harry H. Almond, Jr., *New Law for Outer Space: The Adoption of Standard Terms and Conditions by Treaty*, *in* PROC. THIRTY-FOURTH COLLOQUIUM L. OUTER SPACE 3 (1991).

170. Stephen Gorove, *Interpreting Article II of the Outer Space Treaty*, 37 FORDHAM L. REV. 349, 351-52 (1969).

171. *See* Nandasiri Jasentuliyana, *Space Law and the United Nations*, 17 ANNALS OF AIR & SPACE L. 137, 147 (1992).

172. *See* Charles Chukwuma Okolie, *International Law Principle of Jurisdiction in Regard to Settlements of Humankind on the Moon and Mars*, *in* PROC. THIRTY-FOURTH COLLOQUIUM L. OUTER SPACE 64-65 (1991).

173. Keefe, *supra* note 168, at 361.

III. REGULATING THE INTERNET LIKE OTHER GLOBAL SPACES

The Internet has become a global force, generating billions of dollars in revenue and accommodating millions of users worldwide.[174] As a network of networks, the connections established between parties are fleeting and ever-shifting, transferring from country to country in a matter of seconds.[175] Finding an anchor for jurisdiction can be difficult in this virtual community that requires no territory.[176] For that reason, it is a logical extension of the theory of international spaces to put the Internet in a category with other areas that cannot be acquired through territorial claims.[177]

A. THE INEFFECTIVENESS OF CURRENT ATTEMPTS TO REGULATE THE INTERNET

Minnesota's approach to Internet regulation represents what every jurisdiction should strive not to do.[178] The notice that the Office of the Attorney General of Minnesota displays on the Internet attempts to subject the producer of any web page accessed by Minnesotans to jurisdiction in the state.[179] Concurrent jurisdiction is allowed on criminal matters,[180] so this declaration has the potential to hale in defendants from countries around the globe. A policy this stringent is not likely to prevent the owners of current gambling sites from operating websites,[181] but it is dangerous when taken to a general level. That is, if every state in the United States, let alone every nation in the world, decided to create similar policies, every claim brought for Internet-related crimes or torts would have the potential to be decided in any number of states. Creating a system with choice of law questions that eclipse the attempts at regulation will not succeed in bringing international order to the Internet.

---

174. *See supra* notes 3-5, 15-22 and accompanying text.
175. *See supra* notes 9-18.
176. *See supra* notes 137-139 and accompanying text.
177. *See supra* Part II.
178. *See supra* notes 38, 66, and 76 and accompanying text.
179. *See* Statement of Minnesota Attorney General, *supra* note 38, at http://www.ag.state.mn.us/home/consumer/consumernews/OnlineScams/memo.html.
180. BROWNLIE, *supra* note 27 and accompanying text.
181. *See supra* note 38 and accompanying text; *see also* State v. Granite Gate Resorts, Inc., 568 N.W. 2d 715, 718 (Minn. Ct. App. 1997), *aff'd*, 576 N.W.2d 747 (Minn. 1998).

Individual states in the United States jealously guard their ability to regulate criminal law, education, and other areas of civic importance that have traditionally fallen within the states' domain.[182] Therefore, the nationalization of Internet regulation, especially in the area of cybercrime, does not register well with some.[183] Unfortunately, the argument that "local" Internet crime exists is unrealistic. E-commerce fits a classic definition of interstate commerce.[184]

Extending this definition to the international community, it makes no more sense to create individual state regulations in the United States than it does to create individual nation-state laws that overlap and contradict in their application to the Internet. Individuals "surfing" the web in Alabama are just as likely to be on a New York website as they are a London one, and will most likely travel the globe at the speed of their modem. By creating different laws from nation to nation for downloaders and uploaders,[185] especially as applied to criminal sanctions, the international community is building roadblocks along the Information Superhighway.

In determining its policy approach for regulating the Web, the United States government vacillates between increasing protection of its citizens from the dangers of fraud and cyberporn and protecting classic rights to privacy and freedom of expression.[186] The burden of creating these regulations and balancing individual interests is being shifted increasingly to the federal government, this shift serves as an acknowledgment that individual state regulations can make the Web a complicated array of penalties that have a chilling effect on commerce.[187] The benefits of the U.S. Attorney General's plan to fight cybercrime, primarily a unified network that will provide assistance to all jurisdictions and set a universal standard for what constitutes a cybercrime, demonstrate on a national level that the global community can reap from creating a uniform policy for Internet regulation.[188]

182. *See, e.g.*, United States v. Lopez, 514 U.S. 549, 564 (1995).
183. *See supra* notes 47, 66.
184. *See supra* notes 92-96 and accompanying text.
185. *See supra* notes 40-45 and accompanying text
186. *See supra* notes 87-90 and accompanying text.
187. *See supra* notes 87-97 and accompanying text.
188. *See* supra notes 95-97 and accompanying text.

B. A STEP TOWARD GLOBAL HARMONIZATION

The European Union created a highly detailed response to the problem of unauthorized information transfer when it enacted the EUDPD.[189] The safeguards that are established to control the flow of data from state to state in the European Union would be stringent enough to ensure that privacy is protected for sensitive data transferred on the Web,[190] even though the EUDPD was drafted before the Internet was the monolith that it is today.[191] These progressive protections of personal information are minimized, however, by the decision of the European Union not to create a seamless network for all countries to join.[192]

The EUDPD was drafted to give individual countries the power to modify the data privacy principles in order to pass the directive through the various European legislatures.[193] While this policy has increased the ease in which the EUDPD was ratified, it has also led to problems with choice of law and jurisdiction.[194] Now, international companies have to balance all of the modifications of the EUDPD in various Member countries, creating difficulties similarly present when each state has different data protection laws.[195] This privacy law is a conceptual leap forward that recognizes the importance of maintaining privacy in an increasingly information-dominant society. Nevertheless, the EUDPD's failure to require a uniform standard for all participating countries has provided an unfortunate complication to an otherwise progressive policy.

The Crime in Cyberspace Draft (Draft) purports to cover any entity that communicates through a computer system, making it a far-reaching proposal that extends into the homes and offices of millions in the European Union and beyond.[196] Compared to the EUDPD, the Draft features a more detailed description of how jurisdiction is established, but like the EUDPD, the Draft requires each country to pass similar legislation.[197] In an attempt to increase cooperation, the Draft

189. *See supra* I.C.2.a.
190. Swire, *supra* note 101.
191. Id.
192. *See supra* note 105.
193. *Council Directive 95/46/EC*, *supra* note 99, at 31-30.
194. Swire, *supra* note 101, at 1007-08.
195. *Id.*
196. *Draft Convention on Cyber-crime No. 22, Rev. 2*, *supra* note 122, at 4.
197. *Id.* at 10

has additional provisions that require future Parties to collect evidence for other Parties, create national contact points, and assist in the extradition of accused individuals within their territories.[198]

The strength of these measures has created international concern by various rights activist groups.[199] They feel that the extradition measures and the ability for law enforcement to investigate data files violate due process rights as well as the EUDPD.[200] Essentially the opponents argue is that in trying to protect citizens from the dangers of cyberspace, the Draft committee has created legislation that strips individuals of traditional protections against unjust prosecution.[201] Somewhere between the fragmented protection of the EUDPD and the aggressive international prosecution of the Draft, there should be a medium for a comprehensive, global approach to Internet jurisdiction.

C. THE NECESSITY OF A GLOBAL SOLUTION

Traditional notions of jurisdiction based on territory in the international system are and will continue to be ineffective to regulate the growing World Wide Web.[202] Even application of personal jurisdiction, through the effects an action has in a different territory, is insufficient to base personal jurisdiction on the growing numbers of Internet claims.[203] A lack of a coherent international system has forced countries to enact inconsistent regulatory schemes that focus on different parties in Internet transactions,[204] thus creating a potentially hazardous business environment[205] and spillover effects that aversely affect freedom of expression.[206]

The Internet fits into the concept of a global commons[207]

198. *See Draft Convention on Cyber-crime, No. 19*, *supra* note 111.
199. *See* Global Internet Library Campaign, *supra* note 130, at 4-7.
200. *Id.* at 1-2.
201. *Id.*
202. *See* Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 168-69 (S.D.N.Y. 1997).
203. *See* Schneiderman & Kornreich, *supra* note 36, at 1; *see also id.*, supra note 36 and accompanying text.
204. *See* Brownlie, *supra* note 27 at 314.
205. *See* Gregoire, *supra* note 25, at 29; *see also* Gregoire, *supra* note 25 and accompanying text.
206. *See* Goldsmith, *supra* note 32, at 488-89, *see also* Goldsmith, *supra* note 32 and accompanying text.
207. *See* Menthe, *supra* note 5, at 83.

more naturally than any attempt to superimpose territoriality on the nebulous network.[208] The principle that CHM areas belong to no one but are regulated by everyone through global treaties and norms[209] is the only way to contain a network that has not been successfully regulated using traditional notions of jurisdiction.[210] While acknowledging that creating universal norms[211] and regulations for Internet usage will be difficult,[212] a future of inconsistent national policies and spillover effects limiting free expression[213] will not maximize the potential the Web has as a communication device and economic tool.

The five elements of CHM[214] are actually more easily applied to the Internet than any physical territory because the majority of the arguments against the CHM principle focus on the limited nature of resources and the ability of the powerful to exploit them through the use of their current economic leverage.[215] Although there is an inherent requirement for a computer with the capability to attach itself to the Web, overall usage does not depend on the ability to be able to extract natural resources. Rather than being an exploitable resource with limited capacity, the Internet's ability to grow is limited only by the power of technological advances.

The basic principles of the Outer Space Treaty,[216] precursor to the Moon Treaty, provide an excellent theoretical foundation for current Internet regulations. First, activities should be conducted in a manner that benefits all countries without attempts at militarization.[217] This principle sets the appropriate tone for creating restrictions on use and protecting consumers from fraudulent and criminal harms without attempts to gain political or military advantages over another country.

Second, the Outer Space Treaty makes nations responsible for the reasonable control over objects launched under their authority.[218] Adopting a principle similar to this, each individual nation would take responsibility for the misbehavior of their

208. *See* Puurunen, *supra* note 29, at 745.
209. *See* Joyner, *supra* note 146 at 191.
210. *See* discussion *infra* Part I.B.
211. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW, *supra* note 55, at 254.
212. *See* Yeo & Berliri, *supra* note 58, at 89.
213. Goldsmith, *supra* note 32, at 488-89.
214. Heim, *supra* note 152, at 827.
215. *See* Posner, *supra* note 157, at 1741.
216. Rana, *supra* note 148, at 245.
217. *Id.*
218. *Id.*

citizens on the Web while enforcing the universal provisions created as norms of international law. If a universal set of regulations could be created in this manner, all Web participants could be made aware of the restrictions on the Internet and also face penalties for their actions in their home territory.

The third general principle set forth in the Outer Space Treaty makes international mutual assistance and cooperation obligatory.[219] Mutual assistance is also required in the Cybercrime Draft,[220] so the concept should not be surprising to international diplomats. The Draft also demonstrates that any policy instituted to assist with international investigations should include clear due process limitations to preserve the rights of individuals accused of international cybercrimes.[221]

The moon, as the collective possession of the people of Earth,[222] represents the first application of the CHM theory to an international treaty.[223] Although the treaty is written for the collective good, individuals are not explicitly mentioned in the treaty, leading some to argue that while governments are prevented from exploiting the moon as a resource, individual investors are not.[224] This concern about the omission of individuals in the Moon Treaty is compounded in the case of Internet regulation because while few individual investors currently have the resources to send mining equipment to the moon, millions of individuals have the capability to log on and exploit the Internet, often in a location as convenient as their homes. To eliminate the risk of such strict literalist interpretations, any treaty drafted must be careful to include individuals, organizations, and governments in its regulations.

A significant additional criticism of the Moon Treaty is that a lack of ownership prevents the formation of a stable environment for investors to explore and develop resources.[225] The size of e-commerce and its potential for growth make this a very salient argument for potential Internet regulation.[226] Any regulations of the Internet should be enacted universally for the purpose of creating a sense of stability that will allow investors

219. *Id.*
220. *Draft Convention on Cyber-crime, No. 19, supra* note 111, at 1.
221. *See supra* notes 133-136 and accompanying text.
222. *See* Keefe, *supra* note 168, at 366-67.
223. *See* Moon Treaty, *supra* note 165, at 1434.
224. Gorove, *supra* note 170, at 351.
225. Okolie, *supra* note 172, at 64-65.
226. *See supra* notes 19-22 and accompanying text.

to comfortably expand their markets and rest assured that any wrongs committed against them will be remedied regardless of the location of the offender.

IV. A MODEST PROPOSAL

No object can effectively contain an item larger than itself. Just as a pint glass will not hold a gallon of water, individual territory-based regulations cannot effectively control an international, fluid network of computers. If nations want to protect their citizens from cyber-based harm, they must link with the rest of the global community, creating an international structure large enough to contain the Web. I propose the creation of an international committee with the sole purpose of implementing universal standards created by treaty and ratified by participating Parties designed to bring order to and create jurisdictional rules for the Internet.

The treaty should begin by declaring the Internet a new global space, defined by the theory of CHM. Arguably, there is nothing more entitled to a claim for collective ownership than a network that has been built by individuals across the globe. Once the Internet as CHM has been established, representatives from all regions should participate in the process of drafting regulations for civil and criminal Internet actions, as well as the laws covering jurisdiction for legal action between parties domiciled in different nations.

The regulations that are created should be reviewed and ratified by all participating Parties. As a prerequisite for ratification, the Parties must agree to insert the regulations directly into their legal code, without room for reservations or modifications of the policies. If Parties are allowed to modify the regulations that are agreed upon, the problems seen in the Data Privacy Act will only be compounded, depriving Internet users of clear notice when they have stumbled into an illegal action.

The requirement that Parties adopt the provisions virtually verbatim in order to participate in the treaty will be met with reservations throughout the international community. For that reason, it would be very difficult to create a first draft of a treaty that incorporated sensitive areas of the law where countries are in sharp disagreement. Instead, the committee creating the regulations should focus on problems that currently approach universal harms, such as child pornography, and then subsequently build the regulations from there. This incremental

approach, while slow and tedious, will allow for a gradual adjustment to direct implementation of the provisions of treaties and will also serve to introduce Parties to the novelty of international Internet regulation at a pace that most will be able to handle.

Questions of jurisdiction will need to be addressed often by the committee and the Parties. Once uniform, universal regulations are enacted to battle cybercrime, the jurisdiction for hearing the claim will be the jurisdiction of the individual or entity charged with violating the law. Therefore, a person who ships illegal pornography to Singapore from the United States will be prosecuted in the United States under U.S. law. The debate over civil jurisdiction is still a looming one, one that should be addressed after the criminal sanctions and jurisdiction provisions are in place.

The committee should have representatives from each region of the globe, as well as representatives from the countries with the highest concentration of Internet activity, with the actual number to be determined by the United Nations. The representatives will be responsible for creating the initial drafts of regulations that will be sent to Parties participating in the Internet treaty. Those regulations will be modified through an interactive process with the Parties, leading to the ratification of amendments to the original treaty establishing an international commitment to uniform Internet regulation.

In addition to creating draft regulations, the Committee will be in charge of collecting and distributing data on Internet usage, commerce, and crime. The reports will be used to further modify Internet regulations and alert the global community to potential problems with the existing provisions. Finally, the Committee will be the coordinating body for international efforts to increase access to technology in countries that currently have disproportionately low Internet usage. By increasing access to the Internet internationally, the Committee will be fulfilling the principles of universal access that are the foundation for the 'common heritage of mankind' philosophy used to create this regulatory body.

V. CONCLUSION

The Internet has had a tremendous impact on the development of a global society, generating billions of dollars in commerce, allowing instantaneous communication, and

providing a new medium for information transfer. Along with this incredible surge in economic and political growth has come increased responsibility for the dark side of the technology: cybercrime, copyright infringement, and a potentially unstable business environment. The only way to successfully regulate this new technology is to create a system that is as global and integrated as the Web, using as its foundation the CHM principles that advocate the global, open society that the Internet has propagated.

Creating a regulatory body focused on implementing laws for the globe rather than individual nation-states is a daunting task. As the Outer Space and Moon Treaties illustrate, coaxing sovereign nations into giving up potential territorial rights to future resources is extremely difficult, and has thus far been effectuated primarily in cases of resources too difficult to obtain to be considered lucrative. The Internet, as a huge market that impacts a range of consumers from powerful corporations to individual home-users, mostly likely presents itself to nations as a cyber gold rush with endless possibility. Creating the inertia for a large group of countries to view international Internet regulation as a necessity is a daunting task and one that governments may therefore be unwilling to undertake until international Internet crime and torts are viewed as a global crisis.

Current difficulties aside, the future may contain an integrated approach to Internet jurisdiction as the number of users grows and the geographic areas with readily available Internet access increases. The growth of the Internet will demonstrate that traditional notions of jurisdiction will become increasingly ineffective in regulating its development. As long as nations hold on to antiquated views of territorial sovereignty as supreme for jurisdiction over legal matters, the Internet will continue to be a complicated array of inconsistent regulations and criminal safe havens.