San Diego International Law Journal

Volume 5
Issue 1 *2004*

Article 12

5-1-2004

Using Architectural Constraints and Game Theory to Regulate International Cyberspace Behavior

Van N. Nguy

Using Architectural Constraints and Game Theory to Regulate International Cyberspace Behavior*

TABLE OF CONTENTS

* J.D. candidate 2004, University of San Diego School of Law; B.A. 1999, Pomona College.

The author would like to thank her family and friends for their love and support.

I. INTRODUCTION

The debate over whether cyberspace[1] can or should be regulated is essentially dead.[2] This is the conclusion being taught in law schools today.[3] The battle between Judge Frank Easterbrook[4] and Professor Lawrence Lessig[5] over "laws" and "horses," infamous among cyberspace legal scholars, became irrelevant when geographically-based governments began regulating Internet related activities.[6] However, debate over *how* the Internet should be regulated continues.

One way of framing this debate is in terms of deciding how to regulate *behavior* in cyberspace.[7] Professor Lessig postulated four kinds of constraints regulate behavior: (1) social norms, (2) markets, (3) law, and (4) architecture.[8] This comment first argues that lawmakers must focus

---

1. William Gibson coined the term "cyberspace" in his science fiction classic, NEUROMANCER, originally published in 1984. WILLIAM GIBSON, NEUROMANCER 51 (1984). *See also* THE ENCYCLOPEDIA OF SCIENCE FICTION 288 (John Clute & Peter Nicholls eds., 1993) (crediting Gibson with adding "cyberspace" to the English language); Susan Mallon Ross, *Frontiers and Legal Landscapes: As Safety Valves Open and Close, in* REAL LAW @ VIRTUAL SPACE: COMMUNICATION REGULATION IN CYBERSPACE 51, 53 (Susan J. Drucker & Gary Gumpert eds., 1999) (discussing Harvard Law Professor Laurence Tribe's definition of "cyberspace" in the keynote address of The First Conference on Computers, Freedom, and Privacy in 1991).

2. ROBERT S. R. KU ET AL., CYBERSPACE LAW: CASES AND MATERIALS 37 (2002) (stating "the debate over whether cyberspace could be regulated is largely a historical milestone"). During the debate over whether cyberspace can or should be regulated, freedom of expression advocates, like The Electronic Frontier Foundation declared a "cyberspace declaration of independence." John Perry Barlow, *A Declaration of the Independence of Cyberspace* (1996), *at* http://www.eff.org/~barlow/Declaration-Final.html (last visited Oct. 25, 2003).

3. Professor Jane Henning, Lecture at the University of San Diego School of Law on Cyberspace (Jan. 21, 2003).

4. *See* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 (1996).

5. *See* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999). Lawrence Lessig is a professor of law at Stanford Law School and founder of the Stanford Center for Internet and Society. In October 2002, Professor Lessig argued in front of the United States Supreme Court in Eldred v. Ashcroft, a case regarding the constitutionality of the Digital Millennium Copyright Act. *See* Stanford Law School: Lawrence Lessig, *A Short Biography*, *at* http://www.lessig.org/bio/short/ (last visited Oct. 31, 2003).

6. KU, *supra* note 2; *see also* Quill Corp. v. North Dakota, 504 U.S. 298 (1992); State of Washington v. Heckel, 143 Wash. 2d 824 (2001); CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1022 (S.D. Ohio 1997); Dow Jones & Co. v. Gutnick, 2002 AUST HIGHCT LEXIS 44 (2002).

7. *See* Lessig, *supra* note 5.

8. *Id.* at 507. *See generally* John de Monchaux & J. Mark Schuster, *Five Things*

on using the fourth constraint—architecture[9]—if an interconnected global, democratic society is truly an international goal. Second, this comment argues that, in focusing on architectural constraint, game theory is a uniquely appropriate tool for analyzing Internet issues and developing Internet laws.

II. FRAMING THE DEBATE

Even if effective regulation requires some mixture of the four constraints, groups will generally advocate for primary reliance on a single constraint.[10] Several of these groups are detailed below.

A. Social Norms and Freedom of Expression Advocates

Freedom of expression groups, like the Electronic Frontier Foundation (EFF) and 2600 Enterprises, Inc.,[11] focus on the first constraint, social norms. Social norms regulate behavior by threatening adverse consequences or punishments. In cyberspace, customs and etiquette (sometimes called "netiquette") impose these norms.[12] An example of such a custom is deleting a long list of recipient email addresses in a "forward" before one passes along a particularly interesting email message.[13] Another

---

to Do, in PRESERVING THE BUILT HERITAGE: TOOLS FOR IMPLEMENTATION 3, 3 (J. Mark Schuster et al. eds., 1997) (discussing the "tools approach to government action," but enumerating five, rather than four, modalities of constraint).

9. Lessig defines "architecture" as "the physical world as we find it, even if 'as we find it' is simply how it has already been made." *See* Lessig, *supra* note 5. For example, the fact that the Constitutional Court in Germany is in Karlsruhe, while the capital is in Berlin, limits the influence of one branch of the government over the other. Or, that a town has a square, easily accessible with a diversity of shops, increases the integration of residents in that town. *Id.* at 507.

10. *Id.* at 508 (stating, "These four modalities regulate together. The 'net regulation' of any particular policy is the sum of the regulatory effects of the four modalities together.").

11. Universal City Studios, Inc., sued Eric Corley and his company, 2600 Enterprises, Inc. over the publication of the DVD regional decryption code, DeCSS, on their website. *See* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001). "2600" has special significance as it was the frequency of a signal that some hackers formerly used to access the telephone system from "operator mode" by transmitting the 2600 hertz tone across a telephone line. *Id.* at 435 n.2.

12. Llewellyn Joseph Gibbons, *No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace*, 6 CORNELL J.L. & PUB. POL'Y 475, 493 (1997).

13. *See* http://email.about.com/cs/netiquettetips/tp/core_netiquette.htm (listing the "Top 10 Most Important Rules of Email Netiquette" by Heinz Tschabitscher) (last visited Apr. 7, 2003).

example is to exclude other people's email addresses from website email lists and forwards to protect them from spam.[14] Social norm punishment in cyberspace ranges from a polite message aimed at increasing awareness of the misconduct to social ostracism.[15] To freedom of expression advocates, social norms constraints are the best and most natural means of regulating the Internet.

1. Speech as Liberty and as a Means to Liberty

One simple reason for this perspective may be that the people who constitute these groups truly believe that thoughts should be freely expressed. United States Supreme Court Justice Brandeis touched upon this notion in 1927, when he wrote,

> Those who won our independence believed that the final end of the state was to make men free to develop their faculties, and that in its government the deliberative forces should prevail over the arbitrary. They valued liberty both as an end and as a means. They believed liberty to be the secret of happiness and courage to be the secret of liberty. They believed that freedom to think as you will and to speak as you think are means indispensable to the discovery and spread of political truth; that without free speech and assembly discussion would be futile; that with them, discussion affords ordinarily adequate protection against the dissemination of noxious doctrine; that the greatest menace to freedom is an inert people; that public discussion is a political duty; and that this should be a fundamental principle of the American government.[16]

This passage eloquently expresses an intuition held by many that the ability to express thoughts is a form of liberty as well as a means to liberty.

In addition to this intuition, philosophies such as individual liberty, pluralism, diversity, and community also drive many "freedom of expression" advocates.[17] As M. Kapor wrote, "[l]ife in cyberspace seems to be shaping up exactly like Thomas Jefferson would have wanted: founded on the primacy of individual liberty and a commitment to pluralism, diversity, and community."[18]

These ideals are supported internationally through the Universal Declaration of Human Rights, which states in Article 19 that "[e]veryone

---

14. *See* http://www.libertyaffiliate.com/netiquette.html (stating, "When you send an email to several people at one time, use the BCC feature (Blind Carbon Copy) on your email software. This will stop others from intentionally or accidentally providing your email address to bulk email spammers.") (last visited Apr. 7, 2003).

15. Gibbons, *supra* note 12, at 494.

16. Whitney v. California, 274 U.S. 357, 375 (1927) (J. Brandies, concurring).

17. M. Kapor, *Where is the Digital Highway Really Heading?*, WIRED 53–59 (July/Aug. 1993), *reprinted in* James E. Katz & Philip Aspden, *A Nation of Strangers?*, CYBERETHICS: SOCIAL & MORAL ISSUES IN THE COMPUTER AGE 296 (Robert M. Baird et. al., 2000).

18. Katz, *supra* note 17, at 296.

has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[19] The United Nations' recognition of these rights affirms the global commitment to the founding ideals of the Internet. Furthermore, international recognition of these rights specifically in the Universal Declaration of Human Rights, rather than any other resolution, suggests their fundamental nature and the role these principles will have in the future development of international cyberlaw and international law generally.[20]

2. *It Worked in the Past*

Another reason why social norms may be the best and most natural constraint on Internet behavior may be traced back to 1992.[21] That year, a major watershed in Internet governance took place when the National Science Foundation (NSF), having merged its network, NSFNet[22], with the Department of Defense's (DOD) network ARPANET[23], decided they could no longer run the backbone[24] of the newly created network

19. *Universal Declaration of Human Rights*, art. 19, G.A. Res. 217A, U.N. GAOR, 3rd Sess., U.N. Doc. A/811 (1948).

20. The United Nations' website states, "One of the great achievements of the United Nations is the creation of a comprehensive body of human rights law, which, for the first time in history, provides us with a universal and internationally protected code of human rights, one to which all nations can subscribe and to which all people can aspire. . . . The foundations of this body of law are the United Nations Charter and the Universal Declaration of Human Rights, adopted by the General Assembly in 1948." BASIC FACTS ABOUT THE UN. Sales No. E.00.I.21 (2000), *available at* http://www.un.org/rights/morerights.htm (last visited Oct. 29, 2003).

21. *See generally* Barry M. Leiner et al., *A Brief History of the Internet*, *at* http://www.isoc.org/internet/history/brief.shtml (last visited Oct. 31, 2003).

22. In the early 1990s, organizations connecting to the Internet had to sign a usage agreement directly with NSFNet to gain access to large parts of the Public Internet, regardless of the Internet Service Provider from which they purchased Internet access. WIKIPEDIA: THE FREE ENCYCLOPEDIA, *at* http://en.wikipedia.org/wiki/NSFNet (providing a brief history of ARPANET) (last modified Dec. 8, 2003). NSFNet is related to neither NFSNet, a distributing computing effort to factor large numbers, nor Network File System (NFS), a TCP/IP filing sharing protocol. *Id.*

23. ARPANET, the Advanced Research Projects Agency Network, was the world's first operational packet switching network, and the progenitor of the global Internet. WIKIPEDIA: THE FREE ENCYCLOPEDIA, *at* http://en2.wikipedia.org/wiki/ARPANET (providing a brief history of ARPANET) (last modified Dec. 8, 2003).

24. In packet-switched networks, a backbone consists primarily of switches and interswitch trunks. WIKIPEDIA: THE FREE ENCYCLOPEDIA, *at* http://en.wikipedia.org/wiki/Backbone (defining "Backbone" in the context of the telecommunications field)

structure.[25] They distributed management of the network to public and private companies, effectively moving the system's technical administration out of the United States government's control entirely.[26] The Internet Society (ISOC), a private organization chartered by members of the Internet Engineering Task Force (IETF), gained formal oversight over the Internet Architecture Board (IAB)[27] and IETF.[28] ISOC committed itself to the following agenda:[29]

- assuring discrimination-free Internet access;
- halting censorship of online communication;
- limiting government control over essential elements of networking architecture;
- encouraging cooperation between interconnected networks; and
- guarding against misuse of personal information offered on the Internet.

This agenda comes as no surprise when one considers that the NSF created NSFnet not only to extend and improve on ARPANET by creating a much higher-speed backbone, but also to provide a means for universities and research institutions not funded by the DOD to gain access to Internet resources.[30] The notion that information should flow freely on this network was, and still is, considered essential to achieving many scientific objectives. The scientific community formally declared as much at the 1999 World Conference on Science in the *Declaration on Science and the Use of Scientific Knowledge*—"the importance for scientific research and education of full and open access to information and data belonging to the public domain."[31]

(last modified May 17, 2003). The term "Internet backbone" is now used loosely to describe the "core" of the current Internet, referring to the inter-provider links and peering points. WIKIPEDIA: THE FREE ENCYCLOPEDIA, *at* http://en.wikipedia.org/wiki/Internet_backbone (defining "Internet backbone") (last modified Nov. 18, 2003).

25. MARCUS FRANDA, GOVERNING THE INTERNET: THE EMERGENCE OF AN INTERNATIONAL REGIME 45–46 (2001).

26. *Id.* at 46.

27. *Id.* The Internet Architecture Board was formerly known as the Internet Activities Board and was chaired by David Clark from the Massachusetts Institute of Technology (MIT) for many years. *Id* at 45. The IAB, consisting of members from the Department of Defense (DOD) and MIT, replaced the Internet Configuration Control Board (ICCB) who coordinated the discussion of technical questions among government and private groups and oversaw the network's architectural evolution. The ICCB consisted of network experts. *Id.*

28. *Id.* at 46.

29. CHRISTOS J.P. MOSCHOVITIS ET AL., HISTORY OF THE INTERNET: A CHRONOLOGY, 1843 TO THE PRESENT 167 (1999).

30. FRANDA, *supra* note 25, at 45.

31. This idea that information must freely flow is a fundamental concept in the

This historical synopsis suggests that, before commercialization of the Internet, a large majority of Internet users, if not all users, held the same general vision of scientific advancement through information sharing. Using social norms to restrain undesirable behavior was practical and effective. First, there was no need to involve politicians to create laws regarding an area they cared little about and understood even less.[32] Second, there was little need for market constraints because the product was information. The social norm called for open transfer of information from all parties involved in the transactions. Finally, no reason existed for using architecture to constrain behavior on the network. The challenge, after all, was not to constrain behavior, but instead to create an architecture that would expand and increase activity on the Internet. The establishment of an international Internet regime evidences this focus on expansion. This regime moved "fairly quickly to the technical realm, largely because of:

1. the immediacy of the need to establish protocols and standards if the Internet was to function with a minimum degree of effectiveness and order;
2. the relatively small number of players with sufficient knowledge and interest to be involved in the determination of Internet protocols and standards; and
3. accelerating demand—particularly in the United States, Canada, Europe, and Japan—for access to what was widely viewed as a series of dramatic new inventions, particularly after the Internet was enhanced by the World Wide Web."[33]

Social norms regarding how to behave on the Internet and how to behave in "cyberspace,"[34] provided all the necessary regulation.

---

scientific community. *See* U.N. Educational, Scientific and Cultural Organization, Declaration on Science and the Use of Scientific Knowledge, World Conference on Science, Budapest, Hungary, July 1, 1999, *at* http://www.unesco.org/science/wcs/eng/declaration_e.htm.

32. FRANDA, *supra* note 25, at 44 (stating "most policymakers exhibited initial reluctance to put international Internet issues at the top of their political agendas, for a variety of reasons: (1) the Internet entailed subjects about which they knew little . . ."); *Id.* at 45–46 ("[T]he IAB set up a unique procedure for discussion and resolution of governance issues by opening its membership to anyone anywhere in the world with technical knowledge and related interests and with sufficient time to invest in the [IETF's] elaborate discussions.").

33. *Id.* at 44.

34. One legal scholar describes "cyberspace" most easily characterized by reference to

3. *The Past is not the Present*

The expansion and commercialization of the Internet dramatically changed the general profile of the user-base. No longer did everyone traversing the superhighway hold scientific or altruistic goals.[35]

During the 1980s and 1990s, business leaders became increasingly convinced of the significance of the Internet.[36] They were enthusiastic not about the ISOC's agenda, but rather about the potential for fundamental changes in business practices, such as through e-commerce, online banking, and business-to-business networks.[37] This potential was soon realized. In 1999, e-commerce generated an estimated $16.8 billion in revenues for the fifteen European Community (EC) nations and $71.4 billion for the United States.[38] In the United States alone, the overall online economy reportedly generated $507 billion in revenues and created 2.3 million jobs.[39]

The money-making potential of the Internet caused many groups, including politicians, to advocate using the second constraint—the market—to regulate behavior in cyberspace.

B. The Market and Corporations

The market constrains individuals and collective behavior on the

---

the Internet, being the virtual, non-physical, space between computer terminals, across which most communication now flows. Christopher T. Marsden, *Cyberlaw and International Political Economy: Towards Regulation of the Global Information Society*, 2001 L. REV. M.S.U. – D.C.L. 355, 368 (2001).

35. For example, in 1994, a British hacker accessed the information system of a Liverpool hospital "because he simply wanted to see 'what kind of chaos could be caused by penetrating the hospital computer.' Among other things, he changed the medical prescriptions for the patients: A nine-year-old patient who was 'prescribed' a highly toxic mixture survived only because a nurse re-checked his prescription." Legal Aspects of Computer-Related Crime in the Information Society, COM(98)1 58 (1998) [hereinafter COMCrime Study], *available at* http://europa.eu.int/ISPO/legal/en/comcrime/sieber.doc. Professor Dr. Ulrich Sieber of the University of Würzburg prepared the COMCrime Study for the European Commission. The study's aim was to provide the European Commission with up-to-date information on the legal issues of computer-related crime, especially with respect to substantive criminal law, procedural criminal law as well as the suggestion of alternative solutions. *Id.* at 3.

36. FRANDA, *supra* note 25, at 47. By the early 1990s both European and U.S. leaders had begun to realize the Internet's enormous potential for commercial, business, and economic development. *Id.* at 84.

37. *Id.* at 47.

38. *Id.* at 91 (estimation reported by the EC).

39. JAN H. SAMORISKI, ISSUES IN CYBERSPACE: COMMUNICATION, TECHNOLOGY, LAW AND SOCIETY ON THE INTERNET FRONTIER 110 (Molly Taylor et al. eds., Allyn & Bacon 2002) (*citing* Charles E. Ramirez, *Internet Produces Billions*, DETROIT NEWS Jan. 30, 2000, at C10).

Internet through methods such as price structures and congestion.[40] New Zealand is one country taking this approach.[41] According to Elizabeth Longworth, an advisor to the New Zealand Law Commission on electronic commerce,[42] "pricing structures such as access charges to certain information on the Web and to Internet services, as well as factors such as congestion, influence the choices that cyberspace consumers make and are all examples of cyberspace market regulation."[43]

In some ways, the market inherently regulates the Internet just as social norms do. The Internet, as a medium, allows easy movement and separation of people online who do not agree on basic ground rules.[44] This easy ability to exit is a form of control, a strategy used on Wall Street.[45] If shareholders are unhappy with a publicly traded company, they may sell their stocks.[46] Similarly, the Internet allows "exit", but the

40. Lessig, *supra* note 5, at 508–09 (stating, "Price structures often constrain access, and if they do not, then busy signals do. (America Online (AOL) learned this lesson when it shifted from an hourly to a flat-rate pricing plan.) Some sites on the web charge for access, as on-line services like AOL have for some time. Advertisers reward popular sites; on-line services drop unpopular forums. These behaviors are all a function of market constraints and market opportunity, and they all reflect the regulatory role of the market.").

41. Elizabeth Longworth, *The Possibilities for a Legal Framework for Cyberspace —including a New Zealand Perspective*, *in* THE INTERNATIONAL DIMENSIONS OF CYBERSPACE LAW 9, 23–24 (2000) (stating "[i]t is well recognized, especially in the New Zealand (deregulated) economy, that markets regulate: they constrain both individual and collective behavior.").

42. Elizabeth Longworth (LLM) has worked with or made presentations to the United Nations Educational, Scientific and Cultural Organization (UNESCO), the International Standards Organization (ISO), the European Union Telecommunications Data Protection Working Group, and the Organization for Economic Cooperation and Development (OECD). *Id.* at xi-xii.

43. *Id.* at 23–24. These same market constraints are already observable in the United States as well. For example, people in California pay about fifty dollars a month to receive broadband access in their homes. *See, e.g.*, Road Runner Residential Service, *at* http://www.roadrunner.com/rdrun/hso/pricing.html (last visited Oct. 20, 2003) (stating, "The price of the Road Runner Online Service varies from market to market. On average, a monthly subscription is $44.95 per month and includes a cable modem. This fee is in addition to the regular monthly cable subscription; however most cable providers offer money-saving packages. The monthly fee includes ALWAYS ON access to the online service and the Internet."). This allows these people to avoid congestion and access more information faster than using a regular dial up modem.

44. Longworth, *supra* note 41, at 34, *citing* David R. Johnson & David Post, *Law and Borders—the Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

45. Longworth, *supra* note 41, at 28.

46. However, this ability to exit cannot occur in a closely-held company, where no market exists in which to sell. LEWIS D. SOLOMON ET AL., CORPORATIONS LAW AND POLICY: MATERIALS AND PROBLEMS 421 (4th ed. 1998).

exit process is even easier. If a user does not like a particular site, chat room, or forum, he or she simply clicks to another page. Unlike selling stock, exercising "exit power" on the Internet is a zero-cost transaction. The user is not required to pay broker fees to leave, as a shareholder would pay on selling a stock. Economists tend to favor this "exit" strategy because it forces the organization whose site the user exits to eliminate inefficiency, or else the organization will be replaced by a more efficient competitor.[47]

1. Redrawing the Teams

Along these lines of market constraint, the United States released a document entitled *A Framework for Electronic Commerce* in 1997, in which President Bill Clinton and Vice-President Al Gore asserted:

> Governments can have a profound effect on the growth of electronic commerce. By their actions, they can facilitate electronic trade or inhibit it. Government officials should respect the unique nature of the medium and recognize the widespread competition and increased consumer choice should be the defining features of the new digital marketplace. *They should adopt a market-oriented approach to electronic commerce* that facilitates the emergence of a global, transparent, and predictable legal environment to support business and commerce.[48]

This framework report triggered widespread international discussion and controversy.[49] The European Union initiated a series of high-level meetings designed to formulate a European response to what was viewed as a rather extreme and potentially threatening U.S. stance on electronic commerce development.[50]

Additionally, the market approach proposed by the Clinton administration also alarmed the creators and seasoned users of the Internet. First, the science fiction authors, who coined the term "cyberspace" and filled their novels with the cyberspace vision,[51] often pitted individual hackers or freelance agents against mega-corporation villains, who had supplanted national governments.[52] The engineers and programmers who designed

---

47. *Id.* at 10–11.

48. Memorandum by Ira Magaziner, Chief Internet Policy Advisor to William J. Clinton, former President of the United States of America, *A Framework for Global Electronic Commerce* (Washington D.C. July 1, 1997), *at* http://www.ta.doc.gov/digeconomy/framewrk.htm (also known as the "Magaziner Report") (emphasis added).

49. FRANDA, *supra* note 25, at 83.

50. *Id.*

51. *See* THE ENCYCLOPEDIA OF SCIENCE FICTION, *supra* note 1.

52. Walter A. Effross, *High-Tech Heroes, Virtual Villains, and Jacked-In Justice: Visions of Law and Lawyers in Cyberpunk Science Fiction*, 45 BUFF. L. REV. 931, 941 (1997); JAK KOKE, DEAD AIR 11 (1996) (discussing a society "where megacorporations are more powerful than governments."). *See also* http://store.yahoo.com/2600hacker/coradtshir.html (last visited Oct. 27, 2003) (selling a t-shirt titled "Corporate America

and created protocols[53] and software for the Internet identified with these fictional hackers.[54] To these engineers, just as those science fiction writers had predicted, corporations were attempting to take governance of cyberspace away from those who had created and now lived an almost alter-ego life within it.[55] Despite the fact that "the market" is usually associated with free movement, the threat presented by corporations and their lobbying power made "the market" approach adversarial to freedom of information proponents.[56]

Commercialization of the Internet also made activists out of hackers, and made hackers allies with traditional activists.[57] Those who previously preferred to sit at home in front of monitors rather than be politically active suddenly found themselves, willing or unwilling, "virtually" standing side-by-side with grassroots activists. Even as they tried to

---

Tour Shirt" with the description "The front of the shirt is a graphical image of our continuing ride through the streets of Corporate America, constantly attracting the attention of enforcement agencies of all sorts. On the back you'll find a concert tour style listing of the various legal threats and lawsuits we've faced. Get yours soon before we have to add more threats and make the print smaller!").

53. The term "protocol" as used throughout this comment refers to the computing definition. *See generally,* WIKIPEDIA: THE FREE ENCYCLOPEDIA, *at* http://en.wikipedia.org/wiki/Protocol (defining "Protocol" in the context of the computing as "a convention or standard that controls or enables the connection, communication, and data transfer between two computing devices. Protocols may be implemented by hardware, software, or a combination of the two. At the lowest level, a protocol defines a hardware connection.") (last modified Dec. 9, 2003).

54. Union College's Science, Technology and Society Program offers a course called "Technology in Science Fiction," whose course description states: "A critical reading of various classical science fiction forms to investigate how well science fiction writers projected and predicted technological advances. To what extent is actual technological advancement driven by young future engineers and scientists reading and embracing science fiction literature?", *available at* http://www.union.edu/PUBLIC/ECODEPT/kleind/mellon/sts-proposal.htm (last modified May 12, 2000).

55. Effross, *supra* note 52, at 942 ("The hackers not only exist in the actual and virtual shadows of giant companies but attempt to adopt that grayness and anonymity as their own protective coloration. With rare exception, the corporations are portrayed as dramatically reducing the initiative and creativity of their employees, reducing them to figurative if not literal prostitutes.").

56. *See* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001); *see also* THE ISSUE: US CONSTITUTION, *at* http://anti-dmca.org/ (website protesting Digital Millennium Copyright Act). The site also campaigns visitors to place on the visitor's site a banner stating "Corporations, we've had enough. Take back the Net!", *see* THE ISSUE: US CONSTITUTION, *at* http://www.anti-dmca.org/intro.html.

57. *See* ELECTRONIC CIVIL DISOBEDIENCE, *at* http://www.thing.net/~rdom/ecd/ecd.html (describing Protest in Support of Labor and Indigenous Right's in Mexico by the Electronic Disturbance Theater on May 31st to June 1st, 2002, sponsored by the Berkman Center for Internet and Society at Harvard Law School).

cash in on the commercialization of the Internet during the dot-com era,[58] their "electronic civil disobedience" arose.[59]

"Hacktivists" continue to launch politically motivated attacks on e-mail servers or public web pages by overloading those servers and hacking into web sites to send a political message.[60] In addition, not only are citizens of certain countries expressing political views regarding issues in their own nations,[61] but people throughout the world are expressing views with regards to international issues, ranging from the Zapatista movement in Mexico[62] to NATO actions in Yugoslavia[63] and the war in Iraq.[64] Many journalists even attributed the organization of international protests against the United States regarding the 2003 war against Iraq to the Internet. These include a global protest on February 15, 2003 that consisted of between 8 and 11.5 million people, depending on the reporting source.[65] With this increased political use of the

58. *See* http://www.fuckedcompany.com (forum site for individuals to discuss company lay-offs, usually visited by technical employees who show frustration at "big brother" even as they attempted to get rich quick through dot-com stock options).

59. *See* http://www.thehacktivist.com/ (explaining "[t]he Hacktivist is dedicated to examining the theory and practice of hacktivism and electronic civil disobedience while contributing to the evolution of hacktivism by promoting constructive debate, effective direct action, and creative solutions to complex problems in order to facilitate positive change.").

60. Eric J. Sinrod & William P. Reilly, *Cyber-crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177, 183 (2000).

61. In 1999, the homepages for the White House, the U.S. Department of the Interior, White Pride, the United States Senate, Greenpeace, and the Ku Klux Klan were attacked by political activists protesting the sites' politics. *Id.* On February 7, 2000, the official web site of the Austrian Freedom Party was hacked to protest the inclusion of Jörg Haider and his party into a coalition Austrian government. *Id.* at 184. *See generally*, Christopher Hitchens, *Déjà vu all over again*, SALON.COM (Nov. 11, 1996), *at* http://archive.salon.com/news/news2961111.html (last visited Oct. 20, 2003) (stating, "The Freedom Party is led by Jorg Haider. His father was a leading member of the Austrian Nazi Party. Haider himself had to resign a few years ago as governor of the province of Carthinia after a speech in which he praised Adolf Hitler's policy of full employment. At 47, he also has every chance of becoming Chancellor of Austria in the not-too-distant future.").

62. The "Electronic Disturbance Theater" promotes civil disobedience on-line to raise awareness for its political agenda regarding the Zapatista movement in Mexico and other issues. Sinrod, *supra* note 60, at 184.

63. During the 1999 NATO conflict in Yugoslavia, hackers attacked web sites in NATO countries, including the United States, using virus-infected e-mail and other hacking techniques. *Id.*

64. *See 'Hacktivists' wage Iraq war online*, AGENCE FRANCE-PRESSE (AFP), Mar. 31, 2003, *available at* http://www.theage.com.au/articles/2003/03/29/1048653892300.html.

65. Vikram Khanna, *The anti-war phenomenon*, THE BUSINESS TIMES ONLINE EDITION (Feb. 17, 2003), *available at* http://business-times.asia1.com.sg/sub/views/story/0,4574,72838,00.html (last visited Feb. 21, 2003) (stating, "A total of 11.5 million people took part, according to the collective estimates of the organisers. More like eight million said police and official sources. The protests were staged in about 350 cities, said The New York Times. No, 603 cities (including 47 in Asia), said the United for

Internet, a unique and extremely valuable attribute of the Internet has come into fruition—it is now a potential means for actual global democracy.

2. *A Virtual World Makes Global Democracy a Reality*

Before the Internet, expressing one's voice in the international arena required traveling through several layers of representatives.[66] Beyond representatives, citizens possessed few practical means of voicing opinions or obtaining information regarding global issues. The significant effort required to become involved was unrealistic for the average individual busy with the demands of daily life.[67] As Brock Meeks wrote, "The twilight of the twentieth century is pock-marked by a citizenry more concerned about their daily health and well-being—about their day-to-day survival—than about where government leaders are taking

---

Justice and Peace (UJP), a coalition of non-governmental organisations which describes itself as 'a new national campaign' to bring together organisations opposed to a US-led war on Iraq. . . . [W]hat nobody disagrees with is that Saturday's protests were the largest in history—bigger, even, than at anytime during the Vietnam war. . . . No doubt about it, the power of the Internet has a lot to do with why the protests turned out to be so big."). *See generally,* Stephen D. O'Leary, *The Antiwar Movement on the Web*, USC ANNENBERG ONLINE JOURNALISM REVIEW (Oct. 23, 2002), *available at* http://www.ojr.org/ojr/oleary/ 1034893068.php (last visited Oct. 27, 2003) (stating, "The Web is proving to be increasingly important for both interested citizens seeking alternative perspectives, and antiwar activists seeking to mobilize the public."); David Emery, *Web as Political Force: Iraq war protest sites show power of Internet to mobilize people*, S.F. CHRON., Dec. 5, 2002, *available at* http://www.sfgate.com/cgi-bin/article.cgi?file=/gate/archive/2002/12/05/iraqprotweb.DTL (last visited Nov. 30, 2003) (quoting, "'The Oct. 26 demonstrations were organized entirely online,' says Pam Fielding, a D.C. political consultant and the author of 'The Net Effect: How Cyberadvocacy Is Changing the Political Landscape.'").

66. According to Udenrigsministeriet, the Royal Danish Ministry of Foreign Affairs, "The principle of 'one country one vote' embodied in the Charter of the United Nations for its General Assembly can be considered as fundamental and perfectly sound from the viewpoint of fair international relations and promotion of the concept of national sovereignty, but without bearing on 'democracy' as a form of political organisation in which citizens have equal rights to participate directly or indirectly in the exercise of power." *Political Culture and Institutions for a World Community, at* http://www.um.dk/udenrigspolitik/copenhagenseminars/um_eng_political_culture/obstacles_global.asp (last visited Nov. 30, 2003).

67. This is a problem not only in the political scene, but also the corporate one, where stockholders are rationally apathetic. *See* SOLOMON, *supra* note 46, at 545–46; ROBERT CHARLES CLARK, CORPORATE LAW 389–94 (1986). It is also a general problem when public goods are involved because individuals will have an incentive to ride on the coat-tails of others. *See* ROBERT P. MERGES ET AL., INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 12–15 (2d ed. 2000).

the country."[68] Of course, obtaining political participation is difficult even at a local or national level, let alone an international level.[69]

Little doubt exists that the Internet facilitates communication between groups who would otherwise never communicate. Because of this, it is an invaluable resource for a truly democratic world. The characteristics of cyberspace include its ability, as a medium, to communicate a diverse range of views and activities.[70] Users can move between environments, adopt different personas, and preempt attempts by nations or sovereign authorities to impose their own views as to which values, rights and policies should prevail in a global cyberspace community.[71] The Internet facilitates political ties across traditional socioeconomic boundaries and power differentials, increasing participation in civic life.[72]

This idea that the Internet provides a means towards an actual global democracy is receiving serious attention in academia. A course called "Problems of Democracy" taught at the University of Kent at Canterbury, Department of Politics and International Relations, states in its course description: "Problems of Democracy engages students in an exploration of the current debates about democracy .... New developments in democratic theory—as, for example, in visions of an emerging 'cyberdemocracy'—will also be examined on the basis of the theoretical insights gained in this module."[73] The democratizing attribute of the international Internet is, indeed, one of its unique attributes, separating it from media forms such as the telephone, which does not permit easy dispersal of information to mass numbers of people instantaneously for a flat fee.

Further, the Internet is readily distinguishable from media such as television. The Internet has a decentralized structure while television media has a centralized one. Before the mass expansion of the Internet,

68. Brock N. Meeks, *Better Democracy Through Technology*, 40 COMMUNICATIONS OF THE ACM 75 (Feb. 1997), *reprinted in* CYBERETHICS: SOCIAL & MORAL ISSUES IN THE COMPUTER AGE 288 (Robert M. Baird et al. eds., 2000). Of course, since the September 11th terrorist attacks, Meeks statement seems like an exaggeration unless one considers that political direction now looms in the back of Americans' minds as one factor in survival.

69. "The Czechs, for instance, are too busy making money, drinking absinthe and stumbling home on their cobblestone streets to read up on issues and candidates. ... Czechs no longer worry that their democratic experiment will end if they don't vote—and neither do people in the USA." Laura Vanderkam, *Hurrah for Right to Vote—or Not*, USA TODAY, Nov. 5, 2002, *available* at http://www.usatoday.com/news/opinion/ 2002-11-05-oped-vanderkam_x.htm.

70. Longworth, *supra* note 41, at 21.

71. *Id.* This all assumes, of course, either a common language or translation of information from one language to another.

72. Gibbons, *supra* note 12, at 479–80.

73. University of Kent at Canterbury, Course Description, PO833: Problems of Democracy, *available at* http://www.kent.ac.uk/politics/prospectivepg/ pgmodules/po833.html (last modified Sept. 23, 2003). This course was offered as early as Fall 2002.

television media controlled the visual and widespread presentation of social issues to multiple audiences at once. The "media" defines the terms of the debate, and which sources are authoritative.[74] Before the popularity of the Internet, if television did not present an issue, most individuals did not learn of it.[75] Cyberspace changed this. Unlike television, books, newspapers, or radio, cyberspace is not yet controlled by a few select corporations acting as gatekeepers to the mainstream world. The Internet provides a means to find information, fact or opinion, credible or ridiculous, on any type of topic at any time of day, with a simple click of the "Google™" search button.[76] The Internet's global and decentralized information network facilitates and enhances global democracy.[77]

This ability to facilitate and enhance global democracy is essential to achieving the goal of an integrated global community expressed by many international organizations. The Organisation for Economic Cooperation and Development (OECD), which consists of thirty member countries including the United States, Australia, Japan, and many European

74. Gibbons, *supra* note 12, at 479.

75. *See Bill White: American Media Uses Disinformation To Guide Policy: Corporations Have More Say Than Bush on Foreign Affairs*, PRAVADA, Oct. 11, 2001, *available at* http://english.pravda.ru/usa/2001/10/11/17799.html (Russian forum site with article heading "American Media Uses Disinformation to Guide Policy: Corporations have more say than Bush on foreign affairs."). Print media, radio and town hall meetings also present issues for the general public. However, factors such as convenience and low-time consumption make television an arguably more powerful form of mass persuasion. *See generally*, Shanto Iyengar, *'Media Effects' Paradigms for the Analysis of Local Television News* (1998) (research paper prepared for Center for Communications and Community, Annie E. Casey Foundation Planning Meeting, Sept. 17–18, 1998) ("Scholars from every discipline have weighed in at length on the meaning and significance of the shift from print media to television as the news medium of choice"), *available at* http://www.stanford.edu/~siyengar/research/papers/effects.html.

76. *See* ACLU v. Reno, 929 F. Supp. 824, 881 (E.D. Pa. 1996) ("The plaintiffs in these actions correctly describe the "democratizing" effects of Internet communication: individual citizens of limited means can speak to a worldwide audience on issues of concern to them. Federalists and Anti-Federalists may debate the structure of their government nightly, but these debates occur in newsgroups or chat rooms rather than in pamphlets. Modern-day Lutherns still post their theses, but to electronic bulletin boards rather than the door of the Wittenberg Schlosskirche. More mundane (but from a constitutional perspective, equally important) dialogue occurs between aspiring artists, or French cooks, or dog lovers, or fly fishermen.").

77. "The global information infrastructure . . . is often claimed to be a democratic technology. It is said to create electronic democracy, to facilitate or enhance democratic process." Deborah G. Johnson, *Is the Global Information Infrastructure a Democratic Technology*, COMPUTERS AND SOCIETY 27 (Sept. 1997), *reprinted in* CYBERETHICS: SOCIAL & MORAL ISSUES IN THE COMPUTER AGE 304 (Robert M. Baird et al. eds., 2000).

nations,[78] commits itself to democratic governments and the market economy.[79] The OECD produces internationally agreed instruments, decisions and recommendations to promote rules of the game in areas where multilateral agreement is necessary for individual countries to make progress in a globalized economy.[80] Additionally, the United Nations Educational, Scientific and Cultural Organization (UNESCO) is mandated under its Constitution to advance "the mutual knowledge and understanding of peoples, through all means of mass communication and to that end recommend such international agreements as may be necessary . . . [and to] give fresh impulse to popular education and to the spread of culture."[81]

An integrated global community should be a larger goal of the United States in furthering its national interests. President Clinton, one year after the September 11th terrorist attacks, explained his view on the larger reasons behind the unstable world situation:

> The interdependent world we live in is not yet an integrated community, that is, with shared values, shared benefits, shared institutions. So America's number one job now, is to change this interdependent world into an integrated community . . . . We can't put all the walls up again. So our real job is to bring the world closer together around shared values and shared interests.[82]

As many commentators assert, the Internet forwards this job of bringing the world closer together through its unique ability to cross borders and join people of shared values.[83]

Of course, this same ability to obtain information so readily and expansively on the Internet is also a threat. Neither social norms nor market constraints seem capable of controlling behavior criminal under traditional laws, including trafficking in child pornography,[84] attacks on life,[85] and organized crime.[86] Because of this, individuals such as law

---

78. *OECD Member Countries*, *available at* http://www.oecd.org/documentprint/0,2744,en_2649_201185_1889402_1_1_1_1,00.html (last visited Oct. 27, 2003).

79. About: OECD, *at* http://www.oecd.org/about/0,2337,en_2649_201185_1_1_1_1_1,00.html (last visited Nov. 30, 2003).

80. *Id.*

81. Teresa Fuentes-Camacho, *Introduction: UNESCO and the Law of Cyberspace*, 1 THE INTERNATIONAL DIMENSIONS OF CYBERSPACE LAW 1 (2000).

82. President Bill Clinton, *Late Show with David Letterman* (CBS television broadcast, Sept. 11, 2002), *available* at http://home.hiwaay.net/~ellisc/LateShow/LateShow2002-09-11-32k.mp3.

83. *See* CYBERETHICS: SOCIAL & MORAL ISSUES IN THE COMPUTER AGE 283–352 (Robert M. Baird et al. eds., 2000).

84. "In 1996, the Spanish public was stunned by a case of distribution of child pornography when two students with a collection of over 150 floppy disks with child pornography all collected over the Internet had to be released after 3 days in prison because of a legal gap in the new Spanish Criminal Code of 1996." COMCrime Study, *supra* note 35, at 56.

85. *See* COMCrime Study, *supra* note 35.

professors advocate using law, the third constraint, to control such behaviors on the Internet.[87]

C. The Law Constraint and Law Professors

The law constraint penalizes or sanctions behavior that violates a directive under that law.[88] Numerous law review articles argue for the application of real world laws to the Internet realm, contending that analogies between behavior in the physical world and cyberspace are adequate.[89] To these scholars, cyberspace is simply another new technology that must be integrated into the current legal framework like the steam engine.[90] Recently, these scholars began announcing that an international regime was emerging.[91]

1. Stages in the Formation of an International Regime

Generally, international regimes form through three stages: (1) agenda setting, (2) negotiation, and (3) operationalization.[92] The first stage, agenda setting, includes the debate over whether cyberspace could be regulated. It also includes studies by different international bodies defining cyberspace, categorizing cyberspace behavior, and surveying issues specific to the Internet.[93] During this first stage, the European Commission sanctioned a report received in 1998 which divided computer crimes into four main categories: (1) infringement of privacy, (2) economic offenses, (3)

86. In 1994, a Russian group attacked one of the best known U.S. banks in New York via data networks, transferring over $10 million to foreign accounts from their operating base in St. Petersburg. COMCrime Study, *supra* note 35, at 58.

87. *See* Lee Gomes, *Hot Field of Cyberlaw Is So Much Hokum, Some Skeptics Argue*, WALL ST. J., July 1, 2002, at B1.

88. Longworth, *supra* note 41, at 23.

89. *See generally* Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998); *but cf.* David R. Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996) (criticizing this view).

90. Joseph H. Sommer, *Against Cyberlaw*, 15 BERKELEY TECH. L.J. 1145, 1147 (2000) ("The steam engine and the Industrial Revolution probably transformed American law, but the "law of the steam engine" never existed).

91. *See* FRANDA, *supra* note 25, at 44; MARC D. GOODMAN, *The Emerging Consensus on Criminal Conduct in Cyberspace*, 2002 UCLA J. L. TEC. 3, 5 (2002).

92. FRANDA, *supra* note 25, at 2. (Franda credits Oran Young as identifying these steps.) ORAN R. YOUNG, CREATING REGIMES: ARTIC ACCORDS AND INTERNATIONAL GOVERNANCE 1–28 (1998)); *see also* Eva T. Bloom, Book Review, 95 A.J.I.L. 481 (2001) (reviewing ORAN R. YOUNG, CREATING REGIMES: ARTIC ACCORDS AND INTERNATIONAL GOVERNANCE (1998)).

93. *See* COMCrime Study, *supra* note 31.

illegal and harmful contents, and (4) other offenses, including attacks on life, organized crime, and electronic warfare.[94]

The second stage in the formation of an international regime, negotiation, includes the 1997 Clinton administration proposal, which set forth the previously noted *Framework for Global Electronic Commerce*.[95] This stage also includes negotiations between major international organizations, including the Organization for Economic Cooperation and Development (OECD),[96] the Group of Eight (G8),[97] the Council of Europe,[98] the European Union,[99] and Interpol.[100]

The final stage of international regime formation, operationalization, has largely taken place in advanced information technology (IT) societies, such as the United States.[101] Formidable challenges continue to exist in emerging and less developed countries, however, including the People's Republic of China, perhaps the most advanced computer society among less developed countries.[102]

2. *The Great Firewall of China*

China is one of several nations attempting to firewall the entire nation from the rest of the world's Internet infrastructure by using a separate, government authorized protocol, X.25, rather than the decentralized and

94. *Id.* at 39–61.
95. *See* Magaziner, *supra* note 48.
96. *See supra* at 445.
97. The G-8 (Group of Eight) began to call for international cooperation to prevent cybercrime in 2000. *See* Yomiuri Shimbun, *G-8 to Address Cybercrime for 1st Time, at* http://www.globalpolicy.org/globaliz/law/g8cyber.htm (last visited Jan. 30, 2003). The G-8 consists of the United States, the United Kingdom, Canada, France, Italy, Germany, Japan, and Russia. Luke Johnson, *G-8 Nations Highlight Need for Universal Internet Access* (Aug. 7, 2000), *available at* http://usembassy.state.gov/tokyo/wwwhg084.html.
98. The Council of Europe consists of forty-five member countries and considers policy in every area except defense. *See generally* http://www.coe.int/T/e/Com/about_coe. *See also* http://www.mfa.gov.tr/grupa/al/04.htm (stating that the Council of Europe does not cover defense issues).
99. The European Union (EU) was established after World War II. Today, the EU has fifteen member nations and is preparing for the accession of thirteen eastern and southern European countries. *See The Europorean Union at a Glance, at* http://www.europa.eu.int/abc/index_en.htm (last visited Jan. 30, 2003).
100. "Interpol," once the telegraphic address, was officially incorporated into the Organization's new name adopted in 1956: International Criminal Police Organization-Interpol (abbreviated to ICPO-Interpol). Interpol was set up in 1923 to the purpose of globally enhancing and facilitating cross-border criminal police co-operation. Today, it is the biggest international police organization with 181 member countries spread over five continents. *Interpol—an overview, at* http://www.interpol.int/Public/Icpo/FactSheets/FS200101.asp (last visited Oct. 17, 2003).
101. FRANDA, *supra* note 25, at 2.
102. *Id.*

de facto world standard, TCP/IP.[103] The media has sometimes termed this "the Great Firewall of China."[104] Computer networking within China's national borders is similar to secure and restricted intranets of large private corporations.[105]

China sits at one end of the spectrum for less developed countries. At the other end are the poorer least developed countries, whose main operability challenge arises with simply providing meaningful connectivity between their citizens and the digital world.[106] This has been termed the "digital divide," defined as the gap between those able to benefit by digital technologies and those who are not.[107] The G8 mandated the elimination of the digital divide in the July 2000 Okinawa Charter on the Global Information Society, and created a task force called the Digital Opportunity Task Force (DOT Force) to oversee this mission.[108]

D. Preservation through Architecture

Even as an international regime for governing the Internet emerges, lawmakers must remain vigilant in protecting the unique opportunities the Internet provides the global community in its evolution towards a truly global society. As Professor Raymond Ku argues, "Cyberspace, like the Western frontier, reopens 'the debate over values that always precede the formation of principles and always infuses the effort to implement and interpret law and legal principles.'"[109] The opportunities

---

103. *See infra* at 453.

104. *See* Hamish McDonald, *Struggle of Ideas Heads into Space*, SYDNEY MORNING HERALD, Oct. 5, 2002, at 15 (stating "Try typing 'Falun Gong' into your Internet search engine in China and you will not get far. What is now known as the 'Great Firewall of China' comes into action and you get a notice saying: 'This page cannot be displayed'"); Bruce Einhorn, *The Great Firewall of China*, BUSINESS WEEK, Sept. 23, 2002, at 58 (stating "For now, at least, the Great Firewall appears to be successfully guarding the Middle Kingdom.").

105. FRANDA, *supra* note 25, at 2–3.

106. *Id.* at 3.

107. *Welcome to DigitalDivide.org, at* http://www.digitaldivide.org/over.html (last visited Oct. 17, 2003). *See generally* the Public Broadcasting System's series on the digital divide, *available at* http://www.pbs.org/digitaldivide/ (discussing the role computers play in widening social gaps).

108. *About the DOT Force, at* http://www.dotforce.org/about/ (last visited Oct. 17, 2003). *See also Canada Helps Build New Partnerships with Africa* (June 27, 2002), *at* http://www.pm.gc.ca/default.asp?Language=E&Page=newsroom&Sub=newsreleases&Doc=africa.20020627_e.htm (announcing "Canada Helps Build New Partnerships with Africa: $35 million for three initiatives to help bridge the digital divide.").

109. Ira Glasser, *The Struggle for a New Free Speech Paradigm: Protecting Free Speech and Privacy in the Virtual World of* Cyberspace, 23 NOVA L. REV. 627 (1999), *as*

the Internet provides go beyond this debate over interpretation of legal principles and reaches to all of the democratizing and globalizing features of the Internet. To achieve these international goals of democratization and globalization, the fourth constraint—architecture—sits in a unique position to effectively regulate the Internet.

The common real world example of how architecture constrains behavior is the highway.[110] A highway dividing two neighborhoods limits the extent to which the neighborhoods integrate.[111] Analogously, the infrastructure of the Internet may be used to constrain behavior in cyberspace. This infrastructure includes transfer protocols and physical routes from the home computer to the Internet backbones.[112]

1. Architecture as the Primary Constraint

Architecture should be the primary constraining method on the Internet for three main reasons. First, developers are less likely to resist this type of regulation because it allows them to remain directly involved in the evolution of the Internet, their brain child.[113] Consider the Free Network Project, which created Freenet, a large-scale peer-to-peer network designed by professors, professionals, and other leaders in the network communications field.[114] Using the inherent properties of cyberspace, this program is designed to completely decentralize peer-to-peer file sharing.[115] All communications are encrypted and anonymous.[116] Basically, the program evades the legal problems of Napster.[117] Developers specifically

---

cited in Raymond Ku, *Forward: A Brave New Cyberworld?*, 22 T. JEFFERSON L. REV. 125, 129 (2000).

110. Lessig, *supra* note 5, at 507.

111. *Id.*

112. *Id.* at 509 (stating "[t]he code, or the software and hardware that make cyberspace the way it is, constitutes a set of constraints on how one can behave.").

113. Scholars commonly use the metaphor of a "brain child" in discussing intellectual property protection. *See, e.g.*, Mark D. Janis, *Patent System Reform: Patent Abolitionism*, 17 BERKELEY TECH. L.J. 899, 912 (2002) ("...a greedy corporation has kidnapped his brain child and its inheritance").

114. *See* Ian Clarke et al., *Freenet: A Distributed Anonymous Information Storage and Retrieval System*, In Proc. of the International Computer Science Institute Workshop on Design Issues in Anonymity and Unobservability, Berkeley, CA, 2000, *available at* http://citeseer.nj.nec.com/clarke00freenet.html. *See generally*, The Free Network Project, *at* http://freenetproject.org (last visited Oct. 19, 2003).

115. *Id. See also*, Ian Clarke et al., *Protecting Free Expression Online with Freenet*, IEEE INTERNET COMPUTING 40 (Jan. & Feb. 2002), *available at* http://www.freenet project.org/papers/freenet-ieee.pdf ("Freenet employs a completely decentralized architecture").

116. *Id.* at http://freenetproject.org/index.php?page=faq (stating "Freenet is free software designed to ensure true freedom of communication over the Internet. It allows anybody to publish and read information with complete anonymity.").

117. Professor Lawrence B. Solum, Lecture at the University of San Diego School of Law on Introduction to Intellectual Property (Oct. 31, 2002) (powerpoints for lecture

designed this program to resist attempts by "outsiders" to regulate "their network."[118] The architecture constraint takes advantage of this mentality, reinforcing its effectiveness. Involving engineers discourages certain hacking behaviors.[119] In other words, social norms act as a secondary constraint.

Secondly, the architecture constraint, when modeled using game theory, takes into account market forces and constraints such as "exit."[120] Market constraints are arguably inherent in the Internet and must be taken into account.[121] Some consider the emerging Global Information Society to be a child of international economic law.[122] Although "legal constraints" may take into account market forces, the architecture constraint modeled using game theory couples more naturally with market theory. Both game theory and market theory fall within traditionally mathematical economic fields. Additionally, game theory traditionally models market behaviors, such as pricing controls.

Finally, focusing on the architecture constraint minimizes the amount of new Internet specific laws requiring global adoption. The United States may pass laws related to cyberspace, but encouraging adoption of internationally binding obligations is obviously more difficult. Reliance on a behavioral constraint which minimizes the need for such an arduous process is preferable.

Code[123] in cyberspace more easily substitutes for law or norms, subtly controlling and disciplining socially undesirable behavior.[124] Different architectures express different values (e.g., code that permits filtering promotes parental control). Software that encourages chat rooms, irrespective of identity or profiles, reflects values of openness and freedom of speech.[125] If regulation through code dominates cyberspace's legal framework, then the issue becomes whether the code projects the "right"

---

available on file with Professor Solum).

118. The term "their" refers to the creators of the Internet, including original and current software and network architects, programmers, and developers. *See, e.g.*, The Freenet Network Project, *supra* note 116 (stating "Nobody controls Freenet, not even its creators, meaning that the system is not vulnerable to manipulation or shutdown.").

119. *See supra* at 433.

120. *See supra* at 439.

121. *See* discussion, *supra* at 439.

122. Perry Keller, *China's Impact on the Global Information Society*, *in* REGULATING THE GLOBAL INFORMATION SOCIETY 265, 266 (Christopher T. Marsden ed., 2000).

123. "Code" refers to software code throughout this Comment.

124. Longworth, *supra* note 41, at 25.

125. *Id.*

values. According to Lessig:

> Law . . . is vulnerable to the competing sovereignty of code. Code writers can write code that displaces the values that law has embraced. . . . As the Net grows, as its regulatory power increases, as its power as a source of values becomes established, the values of real-space sovereigns will at first lose out. In many cases, no doubt, that is a very good thing. But there is no reason to believe that it will be a good thing generally or indefinitely. . . . Indeed, to the extent that code writers respond to the wishes of commerce, a power to control may well be the tilt that this code begins to take.[126]

This competing sovereignty is indeed the cyberspace that many people perceive, an alternative sovereign authority that needs its own law, its own cyberlaw.

Naturally, this seems to threaten the current sovereignty of all States in existence. However, it nevertheless is consistent with the international model of governance—that is, governance by customary law. An example of this model of customary law is reflected in the merchant law of the Middle Ages.[127] The growth of trade required resolution other than by reference to local law. Merchants needed a common recognition of certain rules independent of any particular sovereignty.[128] The twentieth century saw the rise of "positivism," which drove jurists to seek the source of law in a sovereign before that law could be recognized as authoritative.[129] However, analysis of current international law shows that this customary law model is still applicable.

International law recognizes a number of sources, including international custom.[130] Customary international law has two elements: (1) uniform and constant usage practiced by countries, and (2) a sense of obligation to follow these rules (*opinio juris*).[131] This customary law is decentralized and not grounded in the actions of any particular sovereign.[132] Similarly, the Internet's inherently decentralized characteristic naturally falls into this model of governance.

2. *Technological Feasibility of Reliance on the Architectural Constraint*

Architectural constraint is not impossible given the existing global Internet infrastructure. China, for example, bases some of its internal computer networks on X.25 protocols.

---

126. Lessig, *supra* note 5, at 543, 548.
127. Longworth, *supra* note 41, at 29.
128. *Id.* at 29–30.
129. *Id.* at 30.
130. Statute of the International Court of Justice, June 26, 1945, art. 38, 59 Stat. 1055, 1060.
131. ROSALYN HIGGINS, PROBLEMS AND PROCESS: INTERNATIONAL LAW AND HOW WE USE IT 19 (1994).
132. Longworth, *supra* note 41, at 30.

Leading government monopoly telephone carriers in Europe, Canada, and Japan (also known as Post, Telegraph and Telephone (PTT) companies) developed the X.25 protocols.[133] These protocols were based on the assumption that each country would have a single public data computer network that interconnects with adjoining networks at national borders, just like telephone companies.[134]

The public phone network started as one system whose lines and cables were controlled by government-run companies of sovereign states. One monopolistic entity owned the entire infrastructure from end to end.[135] This led interoperating local, regional, national, and global networks to charge each other access fees.[136] The monopolistic entity ultimately charges these access fees back to the originating caller.[137]

Following this model, X.25 was designed as a public utility that could guarantee quality of service over a single network in return for access charges. In adopting X.25 as its Internet standard, China provides for a larger government role in network administration and more possibilities for government Internet control than otherwise possible if either TCP/IP or other proprietary protocols were adopted as the national standard.[138] However, any move to transition from TCP/IP to X.25 protocols in nations currently running TCP/IP will meet resistance.

Several reasons lay behind this. First, TCP/IP (Transmission Control Protocol/Internetwork Protocol) is now used almost universally throughout the world. It has become the de facto network standard.[139] The cost of

133. FRANDA, *supra* note 25, at 26. X.25 is considered multipoint technology, along the lines of frame relay or ATM. WILLIAM R. CHESWICK & STEVEN M. BELLOVIN, FIREWALLS AND INTERNET SECURITY: REPELLING THE WILY HACKER 69 (1994).

134. FRANDA, *supra* note 25, at 26–27.

135. Howard M. Cohen, *Economics and the Internet: No Free Rides on the InfoBahn The Information Superhighway Becomes a Toll Road, in* REAL LAW @ VIRTUAL SPACE: COMMUNICATION REGULATION IN CYBERSPACE 95, 96 (Susan J. Drucker & Gary Gumpert eds., 1999).

136. *Id.*

137. *Id.*

138. FRANDA, *supra* note 25, at 208.

139. FRANDA, *supra* note 25, at 22, 29. TCP/IP was accepted as a worldwide standard in the 1990s. *Id.* at 23. The acceptance of TCP/IP was by no means certain. Many companies not initially involved with the development of the Internet developed rival networking protocols to compete with TCP/IP as the potential significance of a worldwide computer network began to come into focus in the 1970s. *Id.* at 23–24. These companies included IBM, Xerox, and Honeywell. *Id.* at 24. However, because proprietary protocols were machine and manufacturer specific and subject to intellectual property protections which required licensing fees, the market naturally chose TCP/IP, which was free and cross-platform. *Id.*

switching away from TCP/IP is a formidable obstacle.

Furthermore, the Internet started as a network of networks, designed and developed to provide common communications between various platforms.[140] TCP/IP literally privatized and completely decentralized responsibility for the establishment, control, accountability, maintenance, and costs of building and maintaining computer networks.[141] This privatization suggests that, between TCP/IP and X.25, the former would be the cheaper means of expanding the Internet into third world countries, eliminating the "digital divide" and increasing global democracy.

Finally, unlike X.25, network specialists designed TCP/IP to further the universality and decentralized nature of worldwide computer networking.[142] The Internet's decentralized infrastructure is harder to control, but makes the system very robust. A highly organized, systematic, and centralized global computer network designed like those of the airline route model may potentially be more efficient and capacious,[143] but lacks this robustness. A snowstorm or downed city will congest airline traffic in many, and potentially all, other cities. Network specialists consider such centralized models threatening. The decentralized design of the Internet makes it very difficult to attack.[144] Rather than centralize and control the network, these specialists have learned to live with and highly value what Quentin Hardy has called "the chaotic nature of the beast, with the guiding philosophy being—'hey, nobody owns this thing.'"[145]

This does not mean the world must chose between a centralized and decentralized system, however. TCP/IP and X.25 protocols are not mutually exclusive. Systems running TCP/IP and X.25 can be combined into a single global network.[146] Furthermore, one can still model the resulting mixed networking system using the analytical tool of game theory.

---

140. *Id.*

141. FRANDA, *supra* note 25, at 27.

142. *Id.* at 23. TCP/IP was originally developed under the U.S. Defense Advanced Research Projects Agency (DARPA) and was deployed on the old ARPANET in 1983. CHESWICK, *supra* note 133, at 19.

143. FRANDA, *supra* note 25, at 213.

144. *See* Mathias Strasser, *Beyond Napster: How the Law Might Respond to a Changing Internet Architecture*, 28 N. KY. L. REV. 660, 664 (2001) (stating "one of the foremost concerns was to provide it with as robust an infrastructure as possible so as to enable it to resist attacks and catastrophic events.").

145. FRANDA, *supra* note 25, at 213. (quoting Quentin Hardy, *Weaving the Perfect Net*, FORBES 141 (July 3, 2000)).

146. FRANDA, *supra* note 25, at 27. This is not to suggest, however, that X.25 does not have its own problems. Public X.25 data networks tend to be an "infested soup of corruption for which the hackers have a separate set of laundering tricks." CHESWICK, *supra* note 133, at 142.

II. GAME THEORY AND CYBERSPACE

Increasingly, scholars are using game theory to analyze and develop legal theories. The range of fields analyzed is broad, spanning constitutional law,[147] bankruptcy law, pre-trial behavior, civil procedure, family law, contract law, corporate law, tort law, and conflicts in law.[148] In addition to these fields, scholars also use game theory to analyze emerging international legal issues. These include environmental problems like global warming,[149] international treaty issues,[150] global economics,[151] and superpower conflicts.[152] However, despite its increasing use, game theory remains a mathematical model, relying on assumptions that do not necessarily mirror the real world.[153]

A. Basics of Game Theory

Game theory is a formal mathematical field that studies strategic behavior.[154] Strategic behavior arises when two or more individuals interact and each individual's decision is influenced by actions of the other people.[155] Game theory allows its users to describe and to predict strategic behavior,[156] logically analyzing situations of conflict and cooperation.[157]

147. Meyerson provides an enlightening application of game theory to constitutional battles, including the infamous case of *Marbury v. Madison* and the "creation" of the Dormant Commerce Clause. *See generally* MICHAEL I. MEYERSON, POLITICAL NUMERACY: MATHEMATICAL PERSPECTIVES ON OUR CHAOTIC CONSTITUTION 110–24 (2002).

148. DOUGLAS G. BAIRD ET AL., GAME THEORY AND THE LAW 5 (1994).

149. *See generally* MICHAEL FINUS, GAME THEORY AND INTERNATIONAL ENVIRONMENTAL COOPERATION (2001); *See also* CONTROLLING GLOBAL WARMING: PERSPECTIVES FROM ECONOMICS, GAME THEORY, AND PUBLIC CHOICE (Christoph Böhringer et al. eds., 2002).

150. *See generally* JON HOVI, GAMES, THREATS, AND TREATIES: UNDERSTANDING COMMITMENTS IN INTERNATIONAL RELATIONS (1998).

151. *See generally* JOHN MCMILLAN, GAME THEORY IN INTERNATIONAL ECONOMICS (1986).

152. *See generally* STEVEN J. BRAMS, SUPERPOWER GAMES: APPLYING GAME THEORY TO SUPERPOWER CONFLICT (1985).

153. MEYERSON, *supra* note 147, at 110.

154. MEYERSON, *supra* note 147, at 109. Modern game theory was developed by mathematician John von Neumann around 1928, and extended by economist Oskar Morgenstern in 1944. *See* JOHN VON NEUMANN & OSKAR MORGENSTERN, THEORY OF GAMES AND ECONOMIC BEHAVIOR (Princeton University Press, 1972). Some describe game theory as the "logical analysis of situations of conflict and cooperation." PHILIP D. STRAFFIN, GAME THEORY AND STRATEGY 3 (1993).

155. BAIRD, *supra* note 148, at 1. *See also* MEYERSON *supra* note 147, at 109.

156. Randal C. Picker, *An Introduction to Game Theory and the Law, in* CHICAGO LECTURES IN LAW AND ECONOMICS 29, 30 (Eric A. Posner ed., 2000).

All "games" have at least three basic elements: (1) players; (2) strategies; and (3) payoffs.[158] Each strategic actor, or "player," can chose from among several courses of action.[159] The plan or rule used to determine which course of action to take at any given instant is the player's "strategy."[160] A player's returns, or "payoffs," represent the value of the outcome to the player and are often measured in levels of utility obtained by each player.[161] Monetary amounts, such as profit in a corporation, rather than general utility, are sometimes used to define payoffs in the analysis for the sake of simplicity.[162] Simply stated, a player's payoff is the amount that using a particular strategy winds up being worth to the player.[163] Other variables that may be modeled in games include the level and symmetry of information available to each player, the number of times the game is played, and the number of players in the game.[164] Collectively, all of these variables set forth the "rules" of the game. These rules define the conditions under which the players operate in the game, that is, who can do what and when they can do it. [165]

A typical game relies on several basic assumptions in order to simplify the game. For instance, many games assume that every possible combination of plays available to the players lead to a well-defined end state (win, loss, or draw) that terminates the game. One fundamental assumption is that all players are rational; that is, each player has complete and

157. STRAFFIN, *supra* note 154.

158. WALTER NICHOLSON, MICROECONOMIC THEORY: BASIC PRINCIPLES AND EXTENSIONS 672 (6th ed. 1995); ERIC RASMUSEN, GAMES AND INFORMATION: AN INTRODUCTION TO GAME THEORY 22 (1989) ("At a minimum, the game's description must include the players, strategies, and payoffs, for which the actions and information are building blocks."); *see also* J.D. WILLIAMS, THE COMPLEAT STRATEGYST 11–17 (1966) (enumerating three elements of players, strategies and payoffs). Varying sources describe game theory as having usually between three to six elements. *See* STRAFFIN, *supra* note 154 (enumerating four elements: players, strategies, outcomes, and payoffs); HOVI, *supra* note 150, at 3–4 (enumerating five elements: players, strategies, outcomes, payoffs, and other rules of the game); RASMUSEN, *supra* note 158 (enumerating six general elements: players, actions, information, strategies, payoffs, outcomes, and equilibria).

159. NICHOLSON, *supra* note 158; RASMUSEN, *supra* note 158 ("An action or move by a player . . . is a choice he can make").

160. RASMUSEN, *supra* note 158 at 24. *See also* HOVI, *supra* note *.

161. STRAFFIN, *supra* note 154; RASMUSEN, *supra* note 158, at 24. In the classic "Prisoner's Dilemma" game, the utility is no prison sentence versus a heavy prison sentence. *See* STRAFFIN, *supra* note 154, at 73.

162. *See* RASMUSEN, *supra* note 158, at 294–300 (applying game theory to patent races, with monetary payoff).

163. ALAN C. STOCKMAN, INTRODUCTION TO ECONOMICS 418 (1996). *See also* NICHOLSON, *supra* note 158, at 673.

164. *See generally* RASMUSEN, *supra* note 158, at 51, 88; STRAFFIN, *supra* note 154, at 128.

165. STOCKMAN, *supra* note 163.

transitive preferences.[166] In other words, given two alternatives, a player will select the one that yields him the most utility, the greater payoff. No special abilities or shortcomings cause the player to deviate from the course of action yielding the most favorable return.[167] In other words, given his belief about the environment, the rational player maximizes his objective function.[168] This assumption is often criticized for reducing the ability of a game theory model to accurately predict real-world situations, despite the simplicity it lends to the modeling process.[169]

Those who use game theory to analyze and develop legal theories realize the limitations, yet contend that game theory provides "valuable insight, even if it does not result in a complete explanation of situations where peoples' fates are intertwined."[170] This belief is especially justified when game theory is applied to an entity like the Internet.

B. Setting up the Internet Game Theory Model

Any useful game theoretic model of cyberspace must ensure that the actors cannot ignore the reaction of others. This is because rational actors by definition cannot exist in situations where the reaction of others may be ignored.[171] To illustrate, consider an electric company deciding whether to order a new power plant given its estimate of demand for electricity in ten years.[172] The company faces a complicated decision, but it does not face another rational agent, so its situation is not appropriate for game theory modeling.[173] In cyberspace, passive web site publishers are not appropriate actors for a game theory model because they have no stake in whether or not others visit their site. The game theory model of cyberspace proposed here defines the "players" to be the networked computers and the "rules" to be the architecture and infrastructure of the entire network, including industry standards which control communications traveling on that network.

166. *See* ROBERT GIBBONS, GAME THEORY FOR APPLIED ECONOMISTS 7 (1992) (stating "we need to assume not only that all the players are rational, but also that all the players knows that all the players are rational, and that all the players know that all the players know that all the players are rationale, and so on, *ad infinitum*.).
167. NICHOLSON, *supra* note 158, at 672.
168. JÜRGEN EICHBERGER, GAME THEORY FOR ECONOMISTS 1 (1993).
169. *Id.*
170. *Id.*
171. *See* RASMUSEN, *supra* note 158, at 9 (stating "the game theory model is not useful when decisions are made that ignore the reactions of others or treat them as impersonal market forces.").
172. *Id.*
173. *Id.* at 10.

1. Players player1 = 192.168.0.1;

Traditionally, game theory model "players" are human, and inherently irrational. Computers, by their very nature, must respond rationally according to their architecture and programming, despite the irrational user giving commands.[174] Therefore, a game theory model that predicts effects of regulations on computer actors is potentially more accurate than typical games which try to predict effects on human actors.[175] The limiting assumption that the "players" must be rational no longer becomes a limitation if the "players" truly are rational entities. One property of the "player" would be connection speed. By designating this constraint as a property of the "player" (the connected computer), this game design incorporates a market constraint that leads Internet users to buy broadband access. This model also confines the analyzed activities to interactions between computers in cyberspace. Every time a human user uses a computer connected to the Internet, the user logs on and a certain profile is activated. This description is not unrealistic as it accurately portrays how employees interact with their company's intranet.[176] In fact, recent operating systems, such as Windows 2000 and Windows XP, require home users to create a login into their own home desktops for security protection.[177] However, confining the game boundaries to interactions between computers requires us to acknowledge implicitly the existence of a separate cyberspace, an idea many engineers embrace and many legal scholars are reluctant to accept. Some law professors view the notion of a separate cyberspace jurisdiction as neither necessary nor helpful, and in fact, even dangerous.[178] Nevertheless, accepting this separate existence helps us model behavior in cyberspace.

---

174. The very essence of being a computer is possessing rationality. *See* Rosalind W. Picard, *Does Hal Cry Digital Tears? Emotions and Computers*, *in* HAL'S LEGACY: 2001'S COMPUTER AS DREAM AND REALITY 279, 280 (David G. Stork ed., 1997) ("After all, isn't possessing the highest form of rationality one of the hallmarks of computers?").

175. *See* HUGH H. SCHWARTZ, RATIONALITY GONE AWRY?: DECISION MAKING INCONSISTENT WITH ECONOMIC AND FINANCIAL THEORY 31–32 (1998) (asserting that "[s]ome prominent mainstream economists concede that their models have not described what successful producers, investors and consumers actually do, to nearly the degree they had expected" and that "[p]erhaps the inclination of many economists and financial analysts to continue to use models that presume high degrees of rationality reflects what has been termed a conservative status quo bias, rather than an exercise in rational behavior on the part of the model builders.").

176. Amy Rogers, *You Got Mail But Your Employer Does Too: Electronic Communication and Privacy in the 21st Century Workplace*, 5 J. TECH. L. & POL'Y 1, 19 (2000) (stating "Many employees log onto their computers immediately upon arriving to work, which usually enters them into a company Intranet system.").

177. The integration of .Net into all aspects of Windows will also facilitate this type of computer interaction. *See generally, Defining the Basic Elements of .NET, at* http://www.microsoft.com/net/basics/whatis.asp.

178. Gomes, *supra* note 87.

2. *Rules = protocols*

This game theory model also proposes that protocols, rather than individuals, define and enforce the rules of the game. In this way, the architecture constraint operates, rather than the social norm constraint. Although many engineers may prefer the social norm constraint,[179] they will more readily support this architecture constraint because it does not facially challenge their control of cyberspace. It also continues to allow them to participate in the development of what is essentially their creation.[180] Support from engineers is vital in the growth of a productive and democratizing Internet because, again, social norms, as a secondary constraint, will prevent hacking driven by subculture calls to "fight the machine."[181]

Using protocols to define and enforce the rules is also more cost effective for the government than using individuals, such as FBI agents, to roam the Internet, searching endlessly for illegal activity.[182] The networked nature of cyberspace permits this kind of self-policing. To illustrate, if the ISOC adopts a new standard, the hold-outs may find that they are unable to communicate with networks outside the hold-out community.[183] Consider an historical example: As Microsoft's Internet Explorer (IE) stole the consumer browser market from Netscape, web developers had to develop code that ran more efficiently on IE than on Netscape, although they preferred Netscape themselves.[184] Those that

179. *See supra* at 433.
180. *See* discussion *supra* at 450.
181. *Id.*
182. *See* Paul Taylor, *Issues Raised by the Application of the Pen Register Statutes to Authorize Government Collection of Information on Packet-Switched Networks*, 6 VA. J.L. & TECH. 4, at para. 8 (2001) ("The program is reported to be named Carnivore because it rapidly finds the meat, in vast amounts of data. It was developed at FBI computer labs in Quantico, Virginia, and has been reported to have been used in fewer than 25 investigations over the past 18 months. However, Marcus Thomas, chief of the FBI's cyber-technology section at Quantico, has indicated that the FBI has already has seen 'growth in the rate of requests', for use of the Carnivore program. The new program operates on commonly available personal computers and takes advantage of the 'packet'-based nature of Internet communications in which computers on the Internet break up e-mail messages, World Wide Web site traffic, and other information into pieces and route the packets across the global network, where they are reassembled at the other end. FBI programmers are reported to have devised a 'packet sniffer' system that can analyze data flowing through computer networks to determine whether it is part of an e-mail message or some other piece of Web traffic. The Carnivore program is operated under the exclusive control of government agents.").
183. Gibbons, *supra* note 12, at 492–93.
184. *See* Jesse Berst, *Why the Browser War is Over*, ZDNET ANCHOR DESK (Nov. 10, 1999), *available at* http://www5.zdnet.com/anchordesk/story/story_4076.html.

developed code for Netscape eventually were unable to ensure their code functioned in IE, and were left to choose between remaining with the most basic of web page features (operable on both browsers), communicating with only those inside their "hold-out" community, or switching to IE-friendly code despite their own personal preferences. The networked architecture of the Internet constrained the developers' behaviors.

This "protocols as rules" approach is more scalable than current policing solutions such as FBI agent roaming. As the network expands, the latter approach requires the addition of more individuals proportionately. Contrast this with the protocol approach, in which the benefits of following the rules/standards—and the costs of deviating from them—increase as the network grows. Economists sometimes describe this as "network externalities."[185] Users benefit from the fact that others use the network, so with each new person that follows a protocol, all current users of the protocol benefit.[186] For example, the more people using Napster, the more beneficial Napster became because the selection of downloadable music increased as the number of people on the network increased.[187] In a similar way, developers are encouraged to follow a new standard as use of that standard increases.

This game theory model of cyberspace is superior for two final reasons. First, data to perform an empirical analysis of the game theoretic model can be gathered quickly and is, in fact, currently being gathered by several sources.[188] Second, the number of players in the game and the potential number of strategies available to the players make statistical analysis more accurate. Generally, the larger

185. MERGES, *supra* note 67, at 734; *see also* Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1007 (2001) (stating that the economic theory of "network effects" instructs us that, the Internet, like the telephone system before it, increases in economic and social value as more people are connected to it. As many of the positive benefits of the Internet are linked to this dynamic, in assessing the impact of regulatory efforts that seek to alter the underlying architecture, "interconnectivity is an important goal that should not be sacrificed lightly.").

186. MERGES, *supra* note 67, at 734.

187. *See* Alfred C. Yen, *A Preliminary Economic Analysis of Napster: Internet Technology, Copyright Liability, and the Possibility of Coasean Bargaining*, 26 U. DAYTON L. REV. 247, 270 (2001) ("[A]s each new user joins Napster, the amount and variety of music available over the Napster network increases.").

188. *See generally* Terrorism Research Center: Information Research Center, *at* http://www.terrorism.com (last visited Oct. 21, 2003) (maintaining a database in cooperation with Georgetown University on information warfare incidents); Australasian Institute of Network and Information Warfare, *at* http://www.infowarzone.com/ (last visited Oct. 21, 2003) (containing information warfare research in Australia); The Berkman Center for Internet & Society at Harvard Law School, *at* http://cyber.law.harvard.edu/ (last visited Oct. 21, 2003) (a research program to explore cyberspace); COMCrime Study, *supra* note 35, at 21–23.

the sample the more accurately a model will reflect the characteristics of a population or sub-group of that population.[189]

C. Structuring the Game

With the basics of this proposed game theory model of cyberspace in place, the next step in developing a useful model requires determining the form and variables that must be introduced into the game to produce useful predictions.

1. Form

Generally, there are three ways to structure a game: (1) extensive form; (2) normal form; and (3) coalitional form.[190] The extensive form game describes the game most explicitly. It includes the sequence of moves, all possible states of information, and the choices at different stages for all players of the game.[191] The normal form, or strategic form, omits many of the details in the extensive form, and instead concentrates on the strategic aspects of the game and the outcomes represented by their associated payoffs, neglecting the game's dynamic structure.[192]

Finally, the coalitional form, or characteristic function form, is a description of social interactions where binding agreements can be made and enforced.[193] This model allows groups of players to form coalitions, and is often useful in analyzing distributional problems and situations in which multiple players may have rationally coinciding strategies.[194]

Due to the massive amount of data available in modeling cyberspace, a computer program could be developed to determine which of the above forms most accurately reflects the nature of the interactions taking

189. RUSSELL LANGLEY, PRACTICAL STATISTICS SIMPLY EXPLAINED 45 (Dover Publ'n, 1971). Statistical mechanics does not concern itself with detailed consideration of the actions of particular actors, but rather takes advantage of the fact that the actors are numerous and average properties of a larger number of actors can be calculated even in the absence of any information about specific actors. "Thus, an actuary for an insurance company can predict with high precision the average life expectancy of all persons born in the United States in a given year, without knowing the state of health of any one of them." FRANCIS W. SEARS & GERHARD L. SALINGER, THERMODYNAMICS, KINETIC THEORY, AND STATISTICAL THERMODYNAMICS 302 (3d ed. 1975).

190. EICHBERGER, *supra* note 168, at 1–2.

191. *Id.* at 2.

192. *Id.*

193. *Id.* at 34.

194. *Id.* at 2.

place between networked computers. Any cursory conclusion as to the best form for the model without a detailed mathematical analysis adds little to the discussion.

2. *The Role of Reputation and Repetition*

Beyond form, other factors play a role in structuring a game theory model. Often, when interaction between players is repeated, a player is willing to forego all gains in one game in order to receive higher gains in subsequent games, if the overall gain is greater.[195] For example, suppose Player X wins in round 1 by lying, and the penalties for lying are insufficient. If the relationship is repeated, then Player X may choose to be honest in round 1 if total gains from round 1 and 2 together are greater if Player X benefits from the reputation of being honest than from lying in round 1.[196] Game theory models that account for repetition are called repetition form games. Reputation makes threats to punish credible.

At first glance, a game theory model of cyberspace interactions may seem like a repetition form game. However, reputation may not be reliable in cyberspace if people can take on different personas and can remain mostly anonymous.[197] In other words, since different users use different computers, and may be identified as different players in cyberspace, the player's past actions cannot accurately predict the player's future action. Different users may be controlling the player (the networked computer) at different times. Therefore, the game should not be modeled as a repetition game unless anonymity on the Internet effectively disappears.[198] Instead, a one-shot game like the model described above accurately represents reality: many users, using many computers, potentially never using the same computer twice, but using computers over and over again—many distinct, separate games are played, rather than many repetitions taking place of the same single game.

---

195. *See id.* at 205–30; RASMUSEN, *supra* note 158, at 121–40.

196. RASMUSEN, *supra* note 158, at 129.

197. *See* Rob Kling et al., *Anonymous Communication Policies for the Internet: Results and Recommendations of the AAAS Conference*, INFORMATION SOCIETY 15 (1999), *reprinted in* CYBERETHICS: SOCIAL & MORAL ISSUES IN THE COMPUTER AGE 97–98 (Robert M. Baird et al. eds., 2000) ("[w]hile many people believe that anonymous communication on the Internet is not only acceptable but has positive value, others see risk in it because anonymous users are not accountable for their behavior.").

198. Many parties have interest in protecting or preventing anonymity on the Internet. *See* KU, *supra* note 2, at 38.

IV. CONCLUSION

A game theory model of cyberspace has the potential to guide international law makers in developing a regulatory framework which not only maintains the ideals upon which the Internet was founded, but also actualizes the international community's vision of an interconnected, global democracy. Throughout history, humans have always struggled with the threat of massive destruction caused by ideological differences between peoples. In one century, humanity faced two world wars and a nuclear arms race which threatened to destroy the entire world. Humanity now sits at the cusp of a new era. The foundation for this era has already been laid, with covenants, treaties, and declarations committed to the sanctity of individuals and cultures.[199] But the reality is still far from the vision.

In the past, distance and access to information played a significant role in differentiating peoples. With the expansion of the Internet, these factors will play a smaller role in the future. Even as the world increasingly specializes, separate disciplines must come together to integrate the solutions. Lawmakers, business leaders, scholars, scientists and engineers must all work together to find a solution for regulating this realm, keeping in mind the vision of an interconnected and integrated global community.

This solution must start first with a foundation. As the saying goes, every solid house is built on a solid foundation. This is true even in cyberspace. The architecture of the global Internet must provide the fundamental framework for further international regulation. Game theory tools developed in the field of mathematics and microeconomics should be used to model this framework. The other constraints—law, social norms, and market—should sit atop of this architecture foundation so that together, all four constraints may interact in a manner that will maintain the uniquely positive aspects of the Internet of information dissemination while minimizing its less desirable effect of information abuse.

VAN N. NGUY

199. *See* Universal Declaration of Human Rights, *supra* note 19.