UC Irvine
UC Irvine Previously Published Works

Title
Patents in Cyberspace: Territoriality and Infringement on Global Computer Networks

Permalink
https://escholarship.org/uc/item/9ph705tx

Author
Burk, DL

Publication Date
1993

Peer reviewed

eScholarship.org Powered by the California Digital Library
University of California

TULANE LAW REVIEW

VOL. 68 NOVEMBER 1993 NO. 1

PATENTS IN CYBERSPACE: TERRITORIALITY AND INFRINGEMENT ON GLOBAL COMPUTER NETWORKS*

DAN L. BURK**

* Copyright 1993 by Dan L. Burk. All rights reserved.

** Visiting Assistant Professor of Law, George Mason University. B.S., Brigham Young University, 1985; M.S., Northwestern University, 1987; J.D., Arizona State University, 1990; J.S.M., Stanford University, 1993. The author wishes to thank Professor John Barton, Stanford Law School, and the members of the seminar on Information Utilities for helpful discussion in the preparation of this Article.

I. INTRODUCTION

> Computers did it. Computers melted other machines, fusing them together. Television-telephone-telex. Tape recorder-VCR-laser disk. Broadcast tower linked to microwave dish linked to satellite. Phone line, cable TV, fiber optic cords hissing out words and pictures in torrents of pure light. All netted together in a web over the world, a global nervous system, an octopus of data.[1]

A quiet revolution has overtaken the societies of the world. As with every revolution, figurative or literal, it swirls around the control of information.[2] The key to past revolutions was said to be the printing press; the key to modern revolutions is said to be the broadcast media.[3] The key to cultural, political, and social revolutions of the near future may well be the computer network.[4]

---

1. BRUCE STERLING, ISLANDS IN THE NET 15 (1988).

2. Clifford A. Lynch, *Networked Information: A Revolution in Progress, in* NETWORKS, OPEN ACCESS, AND VIRTUAL LIBRARIES: IMPLICATIONS FOR THE RESEARCH LIBRARY 12, 13 (Brett Sutton & Charles H. Davis eds., 1992) [hereinafter NETWORKS, OPEN ACCESS, AND VIRTUAL LIBRARIES]. *See generally* WALTER B. WRISTON, THE TWILIGHT OF SOVEREIGNTY (1992) (discussing the political effect of modern global information technology).

3. Lynch, *supra* note 2, at 13.

4. The use of computers to disseminate news of the Tiananmen Square massacre is an early example of this phenomenon in the political arena. During the confrontation between protestors and Chinese government troops in Tiananmen Square, much of the news received

The mechanism of this revolution has quietly emerged from the convergence of telecommunications and computer systems.[5] Because of telecommunications, time and distance are no longer obstacles to accessing remote data processing facilities.[6] This development has created unprecedented possibilities in information exchange, and almost without realizing it, humankind has begun to reap the benefits and pay the price of existence in a wired world.[7] The strange character of this new existence is captured in the title that its mechanism bears, a name conceived in fiction but given substance by the reality of the "global digital highways"[8] spanning our planet: cyberspace.[9]

---

by the outside world was sent out of China via global computer networks. Concerning relevant computer networks, see JOHN S. QUARTERMAN, THE MATRIX: COMPUTER NETWORKS AND CONFERENCING SYSTEMS WORLDWIDE 23 (1990) (discussing computer conferencing systems and computer linked political communities).

5. *See* Karl P. Sauvant, *Transborder Data Flows and the Developing Countries*, 37 INT'L ORG. 359, 359 (1983); *see also* Patrick J. Leahy, *New Laws for New Technologies: Current Issues Facing the Subcommittee on Technology and the Law*, 5 HARV. J.L. & TECH. 1, 8 (1992) (quoting Mitch Kapor, President, Electronic Frontier Foundation).

6. *See* Sauvant, *supra* note 5, at 8.

7. *See* Enrique G. Manet, *Information Technologies: Strategic Changes*, TRANSNAT'L DATA & COMM. REP., June 1987, at 18, 18-19.

8. *See C&W Paves Global Digital Highway*, TRANSNAT'L DATA & COMM. REP., Feb. 1987, at 5, 5.

9. The word "cyberspace" was first coined by the science fiction writer, William Gibson. *See* Michael Benedikt, *Introduction* to CYBERSPACE: FIRST STEPS 1, 1 (Michael Benedikt ed., 1991). In Gibson's novels of society in the near future, "cyberspace is a postindustrial work environment predicated on a new hardwired communications interface that provides a direct and total sensorial *access* to a parallel world of potential work spaces." David Tomas, *Old Rituals for New Space: Rights de Passage and William Gibson's Cultural Model of Cyberspace*, *in* CYBERSPACE: FIRST STEPS, *supra*, at 31, 35. As employed by Gibson and subsequent science fiction writers,

> Cyberspace is a completely spatialized visualization of all information in global information processing systems, along pathways provided by present and future communications networks, enabling full copresence and interaction of multiple users, allowing input and output from and to the full human sensorium, permitting simulations of real and virtual realities, remote data collection and control through telepresence, and total integration and intercommunication with a full range of intelligent products and environments in real space.

Marcos Novak, *Liquid Architectures in Cyberspace*, *in* CYBERSPACE: FIRST STEPS, *supra*, at 225, 225.

The term "cyberspace," however, has been applied to the possible precursor of such an imaginative information environment: that is, to the burgeoning global, electronic-information infrastructure of the present. *See generally*, Special Issue, *Communications, Computers, and Networks: How to Live, Play, and Thrive in Cyberspace*, SCI. AM., Sept. 1991 (entire issue dedicated to discussing networks and their influence on global communication in the future).

Within this shadowy realm of cyberspace, time, distance, and physical barriers are meaningless.[10] Scientists may conduct research within virtual laboratories and interact with colleagues and equipment thousands of miles away;[11] students in virtual classrooms may learn from teachers and classmates that are not physically present;[12] even virtual corporations may coalesce to meet some financial or organizational need, then fade away when the goal of their creation is met.[13]

If, however, the transcendent quality of cyberspace creates new possibilities, it also creates new problems. Where political boundaries dissolve, political chaos may ensue; where information is unbounded, privacy and even identity may be lost.[14] Already, the transborder transfer of personal information has been identified as a challenge to the autonomy and sovereignty of the nation-state;[15] it is no less of a challenge to the autonomy and privacy of individuals.[16] Computer networks have blurred the limits of due process and constitutional rights against unreasonable searches and

10. Nicholas P. Negroponte, *Products and Services for Computer Networks*, SCI. AM., Sept. 1991, at 106, 108 ("Independence of space and time is the single most valuable service and product [networks] can provide humankind.").

11. *See* Michael Schrage, *Computer Tools for Thinking in Tandem*, 253 SCI. 505, 505 (1991).

12. Starr R. Hiltz, *Collaborative Learning: The Virtual Classroom Approach*, T.H.E. JOURNAL, June 1990, at 59; Michael A. Lev, *College by Computer Brings Classroom Home*, CHI. TRIB., July 13, 1992, at 1; Susan Watts, *Classrooms Without Walls*, INDEPENDENT, Jan. 20, 1992, at 15.

13. *See* John A. Byrne et al., *The Virtual Corporation*, BUS. WK., Feb. 8, 1993, at 98, 99; David C. Churbuck & Jeffrey S. Young, *The Virtual Workplace*, FORBES, Nov. 23, 1992, at 184, 186; Thomas W. Malone & John F. Rockart, *Computers, Networks and the Corporation*, SCI. AM., Sept. 1991, at 128, 134-36; *see also* Steve Pruitt & Tom Barrett, *Corporate Virtual Workplace*, *in* CYBERSPACE: FIRST STEPS, *supra* note 9, at 383, 383 ("The lumbering bureaucracies of this century will be replaced by fluid, interdependent groups of problem solvers.").

14. *See* Carol C. Gould, *Network Ethics: Access, Consent, and the Informed Community*, *in* THE INFORMATION WEB: ETHICAL AND SOCIAL IMPLICATIONS OF COMPUTER NETWORKING 1, 11 (Carol C. Gould ed., 1989) [hereinafter THE INFORMATION WEB].

15. Sol Glasner, *Multinational Corporations and National Sovereignty*, *in* TOWARD A LAW OF GLOBAL COMMUNICATIONS NETWORKS 335, 335 (Anne W. Branscomb ed., 1986); Michael Kirby, *Legal Aspects of Transborder Data Flows*, 11 COMPUTER/L.J. 233, 233 (1991). *See generally* WRISTON, *supra* note 2 (discussing the decline of sovereignty due to the transborder transfer of information).

16. *See* Gould, *supra* note 14, at 21-25; Deborah G. Johnson, *The Public-Private Status of Transactions in Computer Networks*, *in* THE INFORMATION WEB, *supra* note 14, at 37, 39; Jane H. Yurow, *Data Protection*, *in* TOWARD A LAW OF GLOBAL COMMUNICATIONS NETWORKS, *supra* note 15, at 239, 239.

seizures.[17] The parameters of free speech under the First Amendment are likewise unclear within the strange contours of cyberspace.[18]

Indeed, a major international organization monitoring the growth of the new global data net has expressed concern that "[t]he question of choice of law . . . is particularly difficult in the case of international computer networks where, because of dispersed location and rapid movement of data, and geographically dispersed data processing activities, several connecting factors could occur in a complex manner involving elements of legal novelty."[19]

This Article explores one narrow but vital area in which such a complex choice of law is certain to arise: intellectual property. Clearly, intellectual property rights will be among the issues intensely debated with regard to the burgeoning global data network. These issues have been addressed, to the extent they have been addressed at all, primarily in terms of copyright protection.[20] However, the role of patent law cannot be ignored, particularly with regard to protection of the computer software that is so integral to the operation of a data network.[21] United States patent law offers protection to software inventions that may be in use on a computer network; however, assessing patent liability for infringing software on an international data communications network may be problematic. The patent statutes are territorial in nature; the computer network is not. On-line databases and other information services are routinely accessed from abroad through transnational linkages. Such linkages are particularly common between the United States and Western Europe and are likely to grow in the

17. *See* Terri A. Cutrera, Note, *The Constitution in Cyberspace: The Fundamental Rights of Computer Users*, 60 UMKC L. REV. 139, 156-59 (1991); Mitchell Kapor, *Civil Liberties in Cyberspace*, SCI. AM., Sept. 1991, at 158, 158.

18. *See generally* Michael I. Meyerson, *Impending Legal Issues for Integrated Broadband Networks*, 3 U. FLA. J.L. & PUB. POL'Y 49 (1990) (discussing the application of the First Amendment to computer networks); Henry H. Perritt, Jr., *Tort Liability, The First Amendment, and Equal Access to Electronic Networks*, 5 HARV. J.L. & TECH. 65 (1992) (same); Edward J. Naughton, Comment, *Is Cyberspace A Public Forum? Computer Bulletin Boards, Free Speech, and State Action*, 81 GEO. L.J. 409 (1993) (same).

19. ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEV., *Explanatory Memorandum*, *in* GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA 13, 36 (1980).

20. *See, e.g.*, Nicholas P. Miller & Carol S. Blumenthal, *Intellectual Property Issues*, *in* TOWARD A LAW OF GLOBAL COMMUNICATIONS NETWORKS, *supra* note 15, at 227, 227; Ithiel De Sola Pool & Richard J. Solomon, *Intellectual Property and Transborder Data Flows*, 16 STAN. J. INT'L L. 113, 115-23 (1980).

21. *Cf.* Miller & Blumenthal, *supra* note 20, at 230 (discussing patent law and software).

future.[22] Where the users and providers of software-based services inhabit an electronic realm with virtual machines that transcend national boundaries, application of a territorial intellectual property scheme may be difficult and may lead to unintended results.

To examine this problem, Part I of this Article reviews the technology, structure, uses, and future of the global data communications network. Part II reviews the United States' patent system, emphasizing those provisions that may be implicated in the operation of computer software in a global data communications environment. Several of the current patent provisions could be applied in order to find liability for extraterritorial use of infringing software. However, Part III discusses the potential drawbacks of patent enforcement and tenders the proposal that until Congress takes the opportunity to weigh the competing interests in this area, courts enforcing software patents should be prepared to carve out certain exceptions to liability when international computer networking is involved.

II. GLOBAL COMPUTER NETWORKS

Data exchange is the lifeblood of our society, and the communications networks that carry data are now the vital circulatory system enabling that exchange.[23] Private data networks established by transnational corporations facilitate their financial, accounting, sales, purchase, and production operations.[24] Electronic cash registers effectively act as data entry terminals for inventory control. Consumers routinely use Automated Teller Machines (ATMs) for routine banking business or employ credit and debit cards in point-of-sale transactions.[25] Airline reservation systems, electronic mail systems, public telephone networks, international freight and inventory control systems, cable television distribution networks, and international manufacturing production systems are now such a common part of everyday life that little thought is given to their presence or use.[26]

---

22. *See* KARL P. SAUVANT, INTERNATIONAL TRANSACTIONS IN SERVICES: THE POLITICS OF TRANSBORDER DATA FLOWS 94 (1986).

23. Al Gore, *Infrastructure for the Global Village*, SCI. AM., Sept. 1991, at 150, 152.

24. Sauvant, *supra* note 5, at 361.

25. *See* SAUVANT, *supra* note 22, at 109; Lynch, *supra* note 2, at 26; *see also* MILTON R. WESSEL, FREEDOM'S EDGE: THE COMPUTER THREAT TO SOCIETY 69-81 (1974) (discussing societal implications of point-of-sale transactions).

26. *See* Edward M. Roche, *The Landscape of International Computing: A Personal View*, TRANSNAT'L DATA & COMM. REP., Jan.-Feb. 1992, at 24, 24.

These various data communications systems are increasingly being directed by computers, in effect becoming computer networks.[27] True computer networks form a subset of this ubiquitous global communications network, a subset that until recently has been unfamiliar to society at large and has existed as a hidden, but active, web of global information conduits.[28] The computer network has been virtually invisible largely because it has remained the domain of its creators, the members of the scientific research community.[29] Typical of these research networks are USENET, an international message exchange network on a multitude of topics, and BITNET, an international network of mainframe computers linking scientists at many universities.[30] Such networks remain primarily in the hands of the technologically sophisticated, yet the information structure that is propelling computer networking beyond the confines of the research community has grown from one of these esoteric research networks: the Internet.

A. Network Structure

The Internet is the world's largest computer network and is also perhaps its most sophisticated and versatile. This network will define computer networking into the next century; the great data exchange systems planned for the future are described as having the virtues, or lacking the handicaps, of the Internet. Thus, a description of the contours of the Internet defines not only the shape of networks to come but also the profile of the legal questions that will attend them.

1. Information Highways

As their name implies, computer networks are formed by sets of computers linked together by means of communications media.[31] In order to communicate with one another, computers on a network share common communication protocols, which are conventions for sharing digital information.[32] Protocols, in fact, define the Internet. In the United States, computer networks following

27. *See* Brett Sutton, *Introduction* to NETWORKS, OPEN ACCESS, AND VIRTUAL LIBRARIES, *supra* note 2, at 1, 1.

28. *See id.*

29. *See id.*

30. QUARTERMAN, *supra* note 4, at 230; Sutton, *supra* note 27, at 3, 5.

31. *See* STEPHEN GOULD, LIBRARY OF CONGRESS, THE FEDERAL RESEARCH INTERNET AND THE NATIONAL RESEARCH AND EDUCATION NETWORK: PROSPECTS FOR THE 1990S 2 (1990) [hereinafter CRS ISSUE BRIEF].

32. *See* Vinton G. Cerf, *Networks*, SCI. AM., Sept. 1991, at 72, 73.

the Internet protocols are sponsored by a variety of federal agencies, including the Department of Energy (DOE), the National Aeronautics and Space Administration (NASA), the Department of Health and Human Services (HHS), and the National Science Foundation (NSF).[33] The most important of these other networks is probably NSFnet, funded by NSF.[34]

All the computers on these networks, as well as those on other national and international networks that have adopted the Internet protocols, have the capability of communicating together.[35] Consequently, the Internet is not a single integrated entity; rather, it is a loosely connected web of local, regional, and national computer networks that share certain procedures for addressing and routing computer data.[36] Indeed, two or more networks may be connected together by computers called gateways or bridges, which translate dissimilar messages.[37] The virtue of the Internet protocols, however, is that they obviate the need for such expensive bridges by allowing ready linkage of disparate networks.[38]

No centralized management or oversight exists for this assemblage of networks; each of the smaller entities comprising the Internet is operated and managed independently by its sponsor.[39] Additionally, each computer at a site connected to the Internet is generally controlled by its own operations center.[40] Funding for the Internet is provided by DOE, NSF, HHS, NASA, and the Department of Defense Advanced Research Projects Agency.[41] None of these agencies, however, directly oversees the network. Only a committee known as the Federal Research Internet Coordinating Committee (FRICC), consisting of representatives from the five funding agencies, has attempted to set standards and protocols for the Internet.[42]

---

33. U.S. GEN. ACCT'G OFFICE, REPORT TO THE CHAIRMAN, SUBCOMM. ON TELECOMMUNICATIONS AND FINANCE, COMM. ON ENERGY AND COMMERCE, HOUSE OF REPRESENTATIVES, COMPUTER SECURITY: VIRUS HIGHLIGHTS NEED FOR IMPROVED INTERNET MANAGEMENT 9 (1989) [hereinafter GAO REPORT].

34. *See id.*

35. *See* Sutton, *supra* note 27, at 3.

36. *See* Daniel P. Dern, *Applying the Internet*, BYTE, Feb. 1992, at 111, 111.

37. Cerf, *supra* note 32, at 79; *see also* Dern, *supra* note 36, at 111-13 (discussing "internetworking communities" and the interaction of geographically separated computer simulation researchers).

38. *See A Close-up of Transmission Control Protocol/Internet Protocol (TCP/IP)*, DATAMATION, Aug. 1, 1988, at 72.

39. *See* GAO REPORT, *supra* note 33, at 11.

40. *Id.*

41. *Id.* at 10.

42. *See id.* at 11.

The resulting structure resembles an electronic nervous system or circulatory system where information in tributaries flows into increasingly larger channels, eventually converging in the major conduit that ties the entire structure together.[43] Analogies have also been drawn to local roadways, maintained by municipalities, counties, and states but tied together by a national highway system.[44] The major conduit or superhighway for a computer network is referred to as a "backbone" network, which is a high capacity network linking other networks together.[45]

The national backbone of the Internet is NSFnet, which comprises a high capacity backbone network connecting six supercomputing centers as well as more than two-hundred and ninety local-area campus networks and thirteen regional networks.[46] Some networks, such as the Bay Area Regional Network in northern California, may cover a region; others, such as the New York State Education Research Network, may cover a state. Still other networks, such as the Southern Universities Research Association Network, may be multistate.[47] Local networks connect "host" computers within a university, business, or other entity that owns and operates the network.[48] These local networks are then interconnected via long distance telephone lines.[49]

As with a roadway or river basin, branches and tributaries are capable of accommodating different levels of traffic or flow. In networks, bandwidth, or the capacity to carry information, is measured in units of information, or bits, per second.[50] Regional networks now typically have a capacity somewhere between 1.5 and 45 megabits per second;[51] upgrades to fiber optic lines are

43. *See* Gould, *supra* note 14, at 1 ("Computer networks may be considered as the nervous system of the society of the future.").

44. *See* Gore, *supra* note 23, at 152-53; Bruce Schneier, *What is Happening to the Internet?*, MACWEEK, Apr. 27, 1992, at 24, 26 (quoting Bob Halloran, Networks Manager, AT&T Universal Card Services). *But see* Negroponte, *supra* note 10, at 113 (highway analogy is overused).

45. GAO REPORT, *supra* note 33, at 9 n.3.

46. *Id.* at 9.

47. *Id.* at 9 n.4.

48. The computers in the network that are used by human beings are referred to as "hosts." *See* QUARTERMAN, *supra* note 4, § 1.4.

49. *See The Fruitful, Tangled Trees of Knowledge*, ECONOMIST, June 20, 1992, at 85, 85 [hereinafter *The Tangled Trees*].

50. A bit, or binary integer, is the smallest unit of digital information that may be represented as a one or a zero. CHARLES J. SIPPL, MACMILLAN DICTIONARY OF DATA COMMUNICATIONS 32 (2d ed. 1985) (defining bandwidth); *see also id.* at 40 (defining bit and bit significance).

51. *See* Schneier, *supra* note 44, at 24, 26; Lynch, *supra* note 2, at 16.

expected to increase capacity to about 100 megabits per second.[52] Until recently, NSFnet carried information at the "T1" level, about 1.5 megabits per second.[53] The latest "T3" upgrade will increase the NSFnet backbone to 45 megabits per second; an additional upgrade now underway is expected to increase this capacity to 155 megabits per second or greater.[54] By comparison, if human beings are considered as information processors, we have a bandwidth of only about 50 bits per second.[55] For networks, if not for humans, continued increases in bandwidth are expected; fiber optic technology will support bandwidth in the gigabit range, that is, about one billion bits per second.[56]

In order to communicate, of course, the linked computers, or nodes, of a network must share more than a common language; they must share some medium for the conveyance of messages.[57] In a computer network, any combination of communications media may be used, including co-axial cable, fiber optic cable, twisted-pair copper wire, and microwave or satellite transmission.[58] The choice of medium will depend in part on the suitability of the particular medium to bridge physical distances in the most cost-efficient manner. Satellite or microwave transmission may be best suited to global or transcontinental distances; wireless cellular transmission is expected to become increasingly important for very short distance data communication.[59] Regional, national, and international networks are often carried over local and long distance high capacity lines that are usually leased from telephone carriers;[60] local-area networks are generally carried over wiring dedicated specifically to that function.[61] There has been a decided move by networks of all sizes toward use of fiber optic cable,

52. *See* Lynch, *supra* note 2, at 16.

53. *Id.* at 16.

54. *See id.* at 16; Johna T. Johnson, *NREN: Turning the Clock Ahead on Tomorrow's Networks*, DATA COMM., Sept. 1992, at 43, 44.

55. *See* Karen Wright, *The Road to the Global-Village*, SCI. AM., Mar. 1990, at 83, 84. As a consequence, "[h]uman beings excel at pattern recognition but are notoriously slow at sequential calculations." *Id.*

56. Michael L. Dertouzos, *Communications, Computers and Networks*, SCI. AM., Sept. 1991, at 62, 63.

57. *Id.* at 65-67.

58. *See id.*

59. *See id.* at 63, 66 (noting that cellular and other wireless networks reach people while they are driving or even walking).

60. *See The Tangled Trees*, *supra* note 49, at 85.

61. *Id.*

which is cheaper, requires less maintenance, and has a higher carrying capacity than copper wire.[62]

2. "Smart" Communications

All this data transmission ultimately rests on the functioning of computer software. The operation of the network is directed by its computers, but the operation of the computers is directed by their software.[63] The operation of modern data processing systems is a marriage of physical components, generally referred to as hardware, and programmed instructions entered into the system to direct the hardware, generally referred to as software.[64] Their interaction may be loosely analogized to the relationship between the body and the mind: the hardware of a computer system, like the body, is capable of performing a variety of tasks but only when it has been configured by the software that determines reactions to defined inputs.[65] Together, the software and hardware comprise a functional computer system.[66]

If computer networks are highways for information, a change from country roads to superhighways is not enough.[67] Rather, the intelligent and innovative use of capacity gives computer networks their true utility.[68] For example, digitized video consumes enormous bandwidth and would tie up considerable carrying capacity if transmitted over a computer network in real time.[69] A more efficient use of the network would be to download the video data as an information package to a data processing device at the viewer's terminal, a process requiring about five seconds.[70] At the receiving end, the video could be played for its actual duration without occupying network transmission lines for that period of time.[71]

Computer network technology is in fact based on this principle of routing information as packets, employing the intelligence at each node of the network to direct the use of the network

62. Negroponte, *supra* note 10, at 106.

63. *See* OFFICE OF SCIENCE AND TECHNOLOGY POLICY, U.S. EXECUTIVE OFFICE OF THE PRESIDENT, THE FEDERAL HIGH PERFORMANCE COMPUTING PROGRAM 23-24 (1989) (discussing the role of software in directing computer networks).

64. *See* Terrance A. Meador & Norman E. Brunell, *Software Patent Applications*, *in* HOW TO WRITE A PATENT APPLICATION 12-1, 12-4 to 12-5 (Jeffrey G. Sheldon ed., 1992).

65. *See id.*

66. *Id.*

67. *See* Negroponte, *supra* note 10, at 113.

68. *Id.* at 106, 113.

69. *Id.* at 106; Wright, *supra* note 55, at 83, 91-92.

70. Negroponte, *supra* note 10, at 106.

71. *Id.*

bandwidth in the most efficient manner possible.[72] In a communications network, communications information may be routed in one of two ways: circuit switching or packet switching.[73] The first of these methods, circuit switching, is poorly adapted to the speed of computer communications and data processing.[74] Circuit switching creates and breaks physical connections between communication lines in order to route information.[75] The time involved in setting up and tearing down such physical linkages is thousands of times greater than the time involved in computer communications; consequently, on a computer network, circuit switching tends to become inefficient, overloaded, and slow.[76]

In light of the inefficiencies of circuit switching, the preferred information routing method in computer networks is typically packet switching.[77] Under this method, digital information is transmitted in discrete units called packets.[78] Packet switching allows efficient and economical use of a single communication channel by breaking messages into packages that are transmitted among host computers on a network; the hosts then reassemble the packages received.[79] Host computers keep track of both their own connections with other hosts and traffic on the network; using this information, they route information packets.[80] Packets can be routed in whatever way the host computers determine is most efficient; the packets need not even arrive in the order sent.[81] This is because packets, like letters in the mail, include not only the information to be sent but also routing and ordering information.[82]

Packet switching entails other advantages related to the modulating function of the intermediate computer that does the routing. For example, the computers that route packets can slow or delay their transmission to allow computers with slower processing speeds to receive communications from computers with faster speeds.[83] This speed-matching feature allows many different types

72. *Id.*
73. *See* Cerf, *supra* note 32, at 74-75.
74. *Id.* at 74.
75. *Id.*
76. *Id.*.
77. *See id.*; *The Tangled Trees*, *supra* note 49, at 85.
78. *See The Tangled Trees*, *supra* note 49, at 85.
79. *See* GAO REPORT, *supra* note 33, at 8 n.2.
80. *See The Tangled Trees*, *supra* note 49, at 85.
81. *See* Cerf, *supra* note 32, at 74; *The Tangled Trees*, *supra* note 49, at 85.
82. *See The Tangled Trees*, *supra* note 49, at 85.
83. Cerf, *supra* note 32, at 75.

of computers to run on the same network concurrently.[84] Packet switches can also detect inoperable trunk lines and send information via a different route.[85] Finally, networks with different protocols may be linked by special packet switches, called gateway computers, that pass packets between networks while accommodating differences in network speed, packet length, and error correction.[86]

B. Network Use

Because computer networks are capable of communicating in an intelligent and efficient manner, they offer information exchange in an unprecedented fashion and enhance the value of information by freeing it from the constraints of time and space.[87] The Internet overcomes geography to create virtual communities: international gatherings of people with shared interests who may never meet physically but who communicate constantly and nearly instantaneously.[88] These communities do so in a variety of formats suited to their different purposes.

1. Network Services

Computer networks facilitate communication and resource sharing by offering capabilities such as electronic mail service, computer conferencing or bulletin boards, file sharing, and remote log-on or device access.[89] Most networks offer only some subset of these capabilities. For example, BITNET primarily supports electronic mail and file transfer, and USENET supports only message distribution.[90] The Internet supports virtually the full range of services including electronic mail, electronic bulletin boards on various topics, access to many on-line libraries, file transfer capability, and remote terminal capability that allows access to other computer systems and other devices.[91]

---

84. *Id.* at 75.

85. *Id.*

86. *Id.* at 79.

87. *See* Negroponte, *supra* note 10, at 108.

88. Lynch, *supra* note 2, at 18.

89. *See* CHARLES R. MCCLURE ET AL., THE NATIONAL RESEARCH AND EDUCATIONAL NETWORK (NREN): RESEARCH AND POLICY PERSPECTIVES 2, 3 (1991); QUARTERMAN, *supra* note 4, §§ 2.1, 2.2.

90. *See* QUARTERMAN, *supra* note 4, §§ 10.2.1, 10.2.2.

91. *See* Schneier, *supra* note 44, at 24.

Electronic mail activity predominates over the Internet information flow.[92] Electronic mail resembles postal mail, because both involve written messages sent to specific destinations, often with some delay before receipt.[93] Unlike postal mail, however, electronic mail tends to be faster, less expensive, and because of its electronic form, the message can be readily reused.[94] Electronic mail messages are reusable in both time and space: the message may be forwarded sequentially, or via the addressing feature of the network protocols, messages may be broadcast to all users, multicast to a select group, or targeted to a single recipient.[95] Internet subscribers trade software as well as news and data;[96] even commercial firms may use the system's file transfer capability to distribute software updates.[97]

Internet also allows resource sharing through remote log-on or remote device access.[98] For example, the network can be used to link complex weather and ecological computer models running on different computers, thereby allowing more detailed modeling than computers could accomplish alone.[99] Scientists can also use the network to conduct experiments at remote sites, using specialized equipment such as electron microscopes, supercomputers, or synchrotron radiation sources without the scientists' physical presence:[100] the experiments controlled, and resultant data gathered, from a distance, creating a "virtual laboratory." Indeed, at various times, equipment as unusual and diverse as elevators, soft drink vending machines, and even toasters have been connected to and made accessible via the Internet.[101]

The Internet is also expected to become an important tool in electronic publishing—the paperless dissemination of documents.[102] An important milestone was recently reached in elec-

92. Lynch, *supra* note 2, at 20; Paul E. Peters, *Networked Information Resources and Services: Next Steps on the Road to the Distributed Digital Libraries of the Twenty-first Century*, *in* NETWORKS, OPEN ACCESS, AND VIRTUAL LIBRARIES, *supra* note 2, at 40, 50.

93. *See* QUARTERMAN, *supra* note 4, § 2.1.1.1.

94. *Id.*

95. *See generally* Cerf, *supra* note 32, at 73 (discussing computer communications protocols).

96. *See* Schneier, *supra* note 44, at 26.

97. *See id.*

98. *See* QUARTERMAN, *supra* note 4, §§ 2.2.1.1, 2.2.1.6.

99. *See* Dern, *supra* note 36, at 112.

100. *See id.* at 112-13; *The Tangled Trees*, *supra* note 49, at 87; Johnson, *supra* note 54, at 57 (discussing remote supercomputer use).

101. *See* Lynch, *supra* note 2, at 20.

102. Sutton, *supra* note 27, at 7. *But see* Lynch, *supra* note 2, at 28-30 (discussing the practical limits on electronic publishing).

tronic publishing with the advent of the *Online Journal of Current Clinical Trials*. This source, available over the Internet and other networks, is a paperless peer-review scientific journal, sponsored by the American Association for the Advancement of Science and the Online Computer Library Center.[103] It is expected that this first foray into scientific electronic publishing will be followed by other on-line publications.[104]

The Internet also provides access to enormous databases, including repositories of government data, over one hundred on-line library catalogs, archives of software, the digitized text of books, weather information, train schedules, and song lyrics.[105] Access to commercial fee-based information utilities, such as LEXIS and DIALOG, is expected soon.[106] Linkages to commercial computer services, such as CompuServe and AppleLink, are already available.[107] Access to such commercial services, however, is problematic. The use of the NSFnet backbone is largely restricted to government, educational, and research uses.[108] Because its sponsor, the National Science Foundation, uses public money to fund the network for research purposes, NSFnet has an "acceptable use" policy that prohibits transmission of commercial data.[109] Commercial institutions that support certain types of research may use government-funded portions of the network but only to send noncommercial research and development data.[110] To circumvent these use restrictions, private organizations have created subnetworks for commercial traffic that bypass the restricted NSFnet.[111] Additionally, some commercial traffic is now transmitted using spare capacity on the NSFnet backbone; because the commercial traffic is segregated from the noncommercial traffic, the acceptable use policy is satisfied.[112]

---

103. *See* Joseph Palca, *New Journal Will Publish Without Paper*, 253 SCI. 1480, 1480 (1991); Sutton, *supra* note 27, at 7.

104. Palca, *supra* note 103, at 1480; Sutton, *supra* note 27, at 7.

105. *See* MCCLURE ET AL., *supra* note 89, at 1; Lynch, *supra* note 2, at 21.

106. *See* Lynch, *supra* note 2, at 21-22.

107. *See* Schneier, *supra* note 44, at 26.

108. *See id.*

109. *See* Peter Heywood, *Is Commercial Traffic In the Stars?*, DATA COMM., Aug. 1992, at 104, 104, *available in* LEXIS, Nexis Library, Data File.

110. *See id.*; Schneier, *supra* note 44, at 26.

111. Heywood, *supra* note 109, at 104.

112. *Id.*

2. Network Growth

The structure and decentralized management environment of the Internet is the product of its history of explosive and somewhat haphazard growth. In 1969, the United States Department of Defense Advanced Research Projects Agency (DARPA) founded an experimental prototype network, the Advanced Research Projects Agency Network (ARPANET), which became the basis for the Internet.[113] ARPANET was created to facilitate real-time access to remote research resources such as supercomputers, radio telescopes, and specialized databases.[114] During the 1970s, DARPA promulgated the set of computer communication standards known as the "Internet protocols," which were quickly adopted by independent networks attached to the ARPANET backbone. By the early 1980s, ARPANET became so heavily used that the Department of Defense moved operational military traffic onto a separate network known as Milnet.[115] By the late 1980s, ARPANET traffic had entirely outstripped its technology; ARPANET users were moved to a new Defense Research Internet (DRI) and ARPANET was "honorably retired."[116]

The Internet protocols that characterized ARPANET allowed it to unite with other networks and eventually assimilated it into the conglomerate Internet. Consequently, the networks' growth has been phenomenal; the Internet comprised about fifty networks in 1983 and over five hundred by 1988.[117] During 1991, the number of networks connected to the Internet backbone tripled, quintupling backbone traffic to over forty gigabytes per day.[118] No one actually knows how many hosts are linked on the Internet, but the number appears to grow by twenty to thirty percent each year.[119] A recent estimate of Internet affiliation suggests that the net includes more than five thousand networks and seven hundred and fifty thousand hosts linking an estimated twenty-five million users in thirty-three countries.[120]

113. *See* Schneier, *supra* note 44, at 24; Brad Schultz, *The Evolution of ARPANET*, DATAMATION, Aug. 1, 1988, at 71, 71.

114. *See* Dern, *supra* note 36, at 111.

115. *See* CRS ISSUE BRIEF, *supra* note 31, at 4; GAO REPORT, *supra* note 33, at 8-9.

116. *See* QUARTERMAN, *supra* note 4, § 7.3.2.1; Schultz, *supra* note 113, at 71, 73.

117. GAO REPORT, *supra* note 33, at 10; *see also* Peters, *supra* note 92, at 42 (diagramming growth and traffic on NSFnet).

118. Schneier, *supra* note 44, at 24.

119. *See The Tangled Trees*, *supra* note 49, at 86.

120. *See* Dern, *supra* note 36, at 114; Schneier, *supra* note 44, at 24.

Protocols may facilitate network connectivity, but the demand for network access is driven by network benefits.[121] Young networks tend to grow exponentially, in part because of an effect known appropriately to economists as network externalities.[122] The more people who join a network, the more valuable it is to the next person who joins, because there are more people with whom to communicate. In addition, the cost of joining the network decreases with each new member because of the efficiencies gained with increased membership. Computer networks enjoy distributional economies of scale similar to those of radio and television broadcasting; broadcasters incur no additional cost when additional people tune in.[123] Similarly, the incremental cost for computer networks over fiber optic cable is very low.[124] Indeed, computer networks lower the cost of message transmission close to the cost of mass media and still allow the message to be directed to particular receivers.[125] These effects are eventually capped when the network saturates its user market or demand outstrips the ability of technology to connect new members. BITNET, for example, stopped growing at a relatively modest size, but Internet membership continues to skyrocket.[126]

3. Foreign Growth

Neither the benefits available from computer networking nor its phenomenal growth has been limited to the United States. Japan and Europe, in particular, have followed the early U.S. lead of investment in network technology and infrastructure.[127] Consequently, major research networks are available in most industrialized nations. These include the Joint Academic Network (JANET), Starlink, and UKnet in the United Kingdom; DFN and

---

121. *See* Peters, *supra* note 92, at 41-47 (listing simplification, connectivity, and performance as network benefits).

122. *See The Tangled Trees*, *supra* note 49, at 86 (discussing computer network growth). *See generally* Michael L. Katz & Carl Shapiro, *Network Externalities, Competition, & Compatibility*, 75 AM. ECON. REV. 424 (1985) (discussing network externalities).

123. OFFICE OF TECHNOLOGY ASSESSMENT, U.S. CONGRESS, OTA-CIT-302, INTELLECTUAL PROPERTY RIGHTS IN AN AGE OF ELECTRONICS AND INFORMATION 159 (1986) [hereinafter OTA INTELLECTUAL PROPERTY REPORT].

124. *Id.* at 161.

125. ITHIEL DE SOLA POOL ET AL., COMMUNICATIONS FLOWS: A CENSUS IN THE UNITED STATES AND JAPAN 30 (1984).

126. *See The Tangled Trees*, *supra* note 49, at 86.

127. EXECUTIVE OFFICE OF THE PRESIDENT, OFFICE OF SCIENCE AND TECHNOLOGY POLICY, A RESEARCH AND DEVELOPMENT STRATEGY FOR HIGH PERFORMANCE COMPUTING 18, 20 (1987).

Dnet in Germany; FNET, ARISTOTE, and REUNIR in France; CDNnet in Canada; Japanese University Network (JUNET) in Japan; and SDN in Korea.[128]

On the international level, worldwide networks span the continents. USENET connects more than two hundred and sixty-five thousand users on ninety-seven hundred hosts on five continents.[129] BITNET connects more than twenty-three hundred hosts in thirty-two countries.[130] Regional research networks have also developed, including the Nordid Universities Network (NORDUnet) in Scandinavia, AUSEAnet in Australia and Southeast Asia, SPEARNET in the South Pacific, and PACNET in the Pacific Basin.[131] A network dubbed "GlasNet" has recently connected nodes throughout the Commonwealth of Independent States.[132]

Considerable regional networking activity has accompanied the formation of the European Community (EC). The European region enjoys several regional networks, the largest of which, Eunet, connects twenty-five hundred sites in twenty-five countries.[133] However, in contrast to the development of U.S. networking capability, little governmental sponsorship has taken place in Europe.[134] Rather, the construction of European networks, such as Eunet, has been accomplished by private entities.[135] These sponsoring entities include universities, telephone carriers, and corporations.[136] As a consequence, few of these networks have acceptable use policies prohibiting commercial traffic. However, the cost of commercial use varies greatly between network operators and is usually higher than the cost of noncommercial use.[137]

Access between North America and Europe has also become increasingly important as the Internet has seen more and more European users.[138] Operators of European Internet protocol networks have begun construction of a backbone network comparable to NSFnet.[139] The European backbone, known as Ebone, connects

128. *See* QUARTERMAN, *supra* note 4, § 6.5.6.
129. *See id.* § 10.2.2.
130. *See id.* § 10.2.1.
131. *See id.* § 6.5.7.
132. *See* Schneier, *supra* note 44, at 26.
133. Heywood, *supra* note 109, at 105.
134. *See id.* at 104.
135. *See id.* at 105.
136. *See id.* at 105-06.
137. *See id.* at 105.
138. *See id.* at 104.
139. *See id.*

computer network nodes in Amsterdam, Geneva, London, Stockholm, and Montpelier. Additionally, there is a German node in development.[140] The Geneva, Stockholm, and London nodes are also directly linked to NSFnet.[141] At present, Ebone traffic, like that of NSFnet, is limited to noncommercial transmissions.[142] Eunet, however, offers alternative routing for European commercial traffic and is directly linked to U.S. mid-level networks in order to avoid the NSFnet commercial-use restrictions.[143]

C. *Future Networks*

The phenomenal growth of computer network use bears testimony to the benefits of networking; however, the networks in their present state entail serious drawbacks. For the technologically sophisticated, the Internet is unsatisfactory, because its various constituents are technically uneven and mismatched, thereby hampering many advanced applications.[144] For the technologically unsophisticated, the Internet is equally unsatisfactory, because it lacks ease of use: the network is by no means "user-friendly."[145] This situation is beginning to change. Both the benefits and the liabilities of the Internet have captured the attention of the White House and of Congress, and the network is now slated for replacement by a "data superhighway" envisioned as accommodating both the research community and the general public.[146]

1. National Research and Education Network (NREN)

The initial steps toward construction of a national "data superhighway" were taken with the introduction into Congress of the High-Performance Computing Act of 1991 (High-Performance Computing Act).[147] Sponsored by Vice-President Gore during his tenure in the Senate, the Act authorizes expenditures of $2.9 billion over five years to finance research into high-speed networked computing and to upgrade the present government research net-

140. *See id.* at 105.
141. *See id.*
142. *See id.* at 104, 106.
143. *See id.* at 106.
144. *See* McCLURE ET AL., *supra* note 89, at 9-10.
145. *See id.*
146. *See* John Markoff, *Building the Electronic Superhighway*, N.Y. TIMES, Jan. 24, 1993, § 3, at 1.
147. *See* S. 343, 102d Cong., 1st Sess. (1991); S. REP. No. 57, 102d Cong., 1st Sess. (1991), *reprinted in* 1991 U.S.C.C.A.N. 1228-55.

works.[148] Ultimately, the U.S. government High Performance Computing and Communications (HPCC) program will develop a National Research and Education Network (NREN), whose capabilities will dwarf those of the present Internet backbones.[149]

The shape of the proposed NREN is uncertain, but it will likely track the three-tiered structure of the Internet, which consists of backbone, regional, and local networks.[150] NREN is expected to boost the productivity of the research community by increasing access to distant colleagues through mail and databases.[151] Increased formal and informal scientific contact will occur, in part, through enhanced versions of present Internet services: electronic mail, bulletin boards, electronic publishing, and teleconferencing.[152]

Despite these increased capabilities, the true value of the new high capacity network will lie in new applications. As one computer scientist has observed, "[W]ho needs a gigabit of electronic mail?"[153] Future applications for the enhanced research network may include interactive videoconferencing,[154] construction of virtual libraries for interactive research,[155] information retrieval via programmable "knowbots" that will comb the network for requested materials,[156] and linkage of network nodes for distributed data processing that would effectively knit the entire network into one great computer.[157]

For such applications to become practical, however, more than increased bandwidth is required. Executing such information transfer at gigabit speeds would overwhelm present protocols; even supercomputers would become swamped. Present routing and addressing schemes would also be inadequate. Consequently, under the auspices of the High-Performance Computing Act, five gigabit testbed sites scattered across the United States are develop-

148. *See* High-Performance Computing Act of 1991, Pub. L. No. 102-194, 105 Stat. 1594 (1991); *see also* Markoff, *supra* note 146, at 6.

149. *See* Johnson, *supra* note 54, at 44.

150. *See* McCLURE ET AL., *supra* note 89, at 10-11.

151. *See id.* at 59.

152. *See id.*

153. Johnson, *supra* note 54, at 57 (quoting David Farber, University of Pennsylvania).

154. *Id.* at 60.

155. Charles E. Catlett & Jeffrey A. Terstriep, *The Use and Effect of Multimedia Digital Libraries in a National Network*, *in* NETWORKS, OPEN ACCESS, AND VIRTUAL LIBRARIES, *supra* note 2, at 84, 87-93; Johnson, *supra* note 54, at 59-60.

156. Cerf, *supra* note 32, at 74; Johnson, *supra* note 54, at 58.

157. *See* Johnson, *supra* note 54, at 57; Schultz, *supra* note 113, at 73.

ing new software and protocols for the NREN as well as imaginative applications for the network.[158]

At present, the testbeds are all that exist of the NREN, and application of their research lies in the future.[159] A prototype NREN is not expected to be running until at least 1996, when the testbeds will be linked with an Internet enhanced to a capacity of six hundred and twenty-two megabits per second.[160] In the meantime, a makeshift "Interagency Interim NREN" is being cobbled together: it will comprise the upgraded present Internet with a new name.[161] Ongoing upgrades through 1994 will give the present system a capacity of 155 megabits per second; it has already acquired its new name and new oversight entities.[162] Thus, a new national network is expected to rise triumphant, like the Phoenix, from the chaos of the Internet.

2. Consumer Networks

Improved research networks may well generate new discoveries that will impact the commercial sector,[163] but networks are not truly expected to come into their own until they are more widely available to consumers. Such a network would make all the services of the research networks available to homes, libraries, and schools, and would offer consumer services on a commodity basis, rather than through government procurement.[164] One of the first services could be movies on demand,[165] followed by commercial services that will allow consumers to order personalized news text or news reports;[166] browse through databases on summer rental housing, restaurants, or other goods and services;[167] or order customized automobiles direct from the factory.[168]

The current administration has already begun peddling this concept; during his presidential campaign, then-Arkansas Governor Bill Clinton called for a door-to-door fiber optic system by the

158. *See* Johnson, *supra* note 54, at 44-46.
159. *See id.*
160. *See id.*
161. *See id.* at 44.
162. *See id.* at 44-46 (noting that the Internet is now the "Interagency Interim NREN"); *A NREN Alphabet*, DATA COMM., Sept. 1992, at 48, 48-49 (listing NREN oversight bodies).
163. U.S. CONGRESS OFFICE OF TECHNOLOGY ASSESSMENT, OTA-BP-CIT-59, HIGH PERFORMANCE COMPUTING & NETWORKING FOR SCIENCE: BACKGROUND PAPER 3-6 (1989).
164. Lynch, *supra* note 2, at 17.
165. Markoff, *supra* note 146, at 6; Negroponte, *supra* note 10, at 108-09.
166. Negroponte, *supra* note 10, at 110-11.
167. *Id.* at 110.
168. Dertouzos, *supra* note 56, at 67-68.

year 2015.[169] Vice-President Gore has touted this vision as one of the selling points for continued investment in high performance computing needed to develop the infrastructure, software, and expertise capable of handling a flood of information services directed at twenty-first century consumers.[170]

It might therefore seem that the question is no longer "whether digital networks will become as commonplace as the telephone but when."[171] Observers caution, however, that previous attempts in the private sector to promote consumer information services have not resulted in rousing successes. Bell Laboratories' Picture Phone project of the 1960s was an expensive flop,[172] as was Knight-Ridder's videotext Viewtron project.[173] Prodigy, the joint Sears-IBM information service, has relatively few subscribers.[174] Although the general public has taken to the use of ATMs,[175] relatively few people in the United States take the opportunity to bank by computer.[176]

This dismal history of private attempts to create an information market has prompted calls for governmental procurement to launch an everyman's network. Powerful advocates within the Clinton Administration, particularly Vice-President Gore, support government-sponsored. construction of the domestic network which, it is hoped, would then attract private service providers.[177] This proposal has support from a variety of constituencies, including librarians, educators, computer manufacturers, and information-service providers, all of whom assert that government intervention will insure quicker consumer access.[178]

However, other interests in the private sector—particularly long distance carriers with established networks—oppose such government intervention.[179] Instead, they champion the use of

169. *See* Johna T. Johnson, *Whose NREN?*, DATA COMM., Sept. 1992, at 56, 57.

170. *See* Gore, *supra* note 23, at 152-53; Markoff, *supra* note 146, at 1, 6.

171. Sutton, *supra* note 27, at 1.

172. *See* Markoff, *supra* note 146, at 6.

173. *See* Wright, *supra* note 55, at 85.

174. Fred Guterl, *Vive le terminal*, SCI. AM., Mar. 1990, at 88, 88; Wright, *supra* note 55, at 85.

175. *See* SAUVANT, *supra* note 22, at 109-110.

176. *See* Wright, *supra* note 55, at 85. ATMs are now routinely used for deposits, cash withdrawals, payments, transfers and similar simple transactions; however, mortgage lending, bond trading, brokering, and other more complex transactions could also be conducted on-line. *See* Karl P. Sauvant, *The Tradability of Services*, *in* THE URUGUAY ROUND: SERVICES IN THE WORLD ECONOMY 114, 115 (Patrick A. Messerlin & Karl P. Sauvant eds., 1990).

177. *See* Markoff, *supra* note 146, at 1.

178. *Id.*

179. *Id.*

Integrated Digital Services Network (ISDN) technology, which would use existing copper wire connections to offer consumers two 64-kilobit-per-second voice channels and one 16-kilobit-per-second data channel, reaching the upper limit of bandwidth for standard copper cable.[180] This would provide immediate access and, when the information-services market has grown sufficiently, could be upgraded to Broadband ISDN (BISDN), delivering multi-megabit data services over fiber optic cable.[181] Advocates of the Clinton Administration's approach, however, suggest that the slender data-carrying capacity of ISDN would not provide enough incentive to lead to upgrades or would do so too slowly, thus making a large initial governmental presence necessary.[182]

This later argument gains credence from the experience of other nations. Elsewhere in the world, government-owned telecommunications monopolies have begun to make consumer network access a reality. Both Japan and Europe are pursuing the ISDN option;[183] Japan is also investing heavily in BISDN.[184] The Nippon Telegraph and Telephone Corporation has announced plans to lay fiber optic cable to virtually every home, office, and factory in Japan.[185] A highly successful consumer network is already operating in France in the form of Minitel, the French telecommunications services' electronic information exchange.[186] Originally intended to replace printed telephone books with terminals for a computerized directory, the service also carries enough capacity to accommodate information-service providers.[187] The system provides access to about eighteen percent of French households, offering not only electronic phone and service directories but also electronic mail, travel services, electronic banking, and electronic catalog shopping.[188]

---

180. *See* Lynch, *supra* note 2, at 17; Wright, *supra* note 55, at 93; *see also* Anthony M. Rutkowski, *Integrated Services Digital Network*, *in* TOWARD A LAW OF GLOBAL COMMUNICATIONS NETWORKS, *supra* note 15, at 121 (describing ISDN technology).

181. *See* Markoff, *supra* note 146, at 5. *See generally* Michael Botein, *Regulation of Fiberoptic Integrated Broadband Networks: Common Carriage, Ownership and Rates*, 3 U. FLA. J.L. & PUB. POL'Y 65 (1990) (describing legal issues likely to be raised by BISDN implementation).

182. *See* Markoff, *supra* note 146, at 6; Wright, *supra* note 55, at 93.

183. *See* Wright, *supra* note 55, at 93.

184. *See* Lynch, *supra* note 2, at 17.

185. *See* S. REP. No. 64, 102d Cong., 1st Sess. 7 (1991).

186. *See* Guterl, *supra* note 174, at 88.

187. *Id.*

188. *Id.*

In some form, then, it appears that consumers in the United States and elsewhere are likely to gain a significant measure of access to the growing global data network. This in itself will swell the size and activity of the network and seems likely to generate new services and technology that will promote even further growth and activity. If recent experience with networks is an indicator of future trends, this increased network access and activity appears to be the type of technological development that requires a rethinking of societal laws and norms.[189] Among the legal standards that may require rethinking are those governing patent protection.

III. NETWORKS AND INFRINGEMENT

Computer networks offer access to valuable commodities—information and information-based products; however, the precise value of these commodities is often difficult to ascertain.[190] This is due in part to the ephemeral nature of information, which defies the conventional barriers and regulations applied to physical property.[191] This characteristic of information is complemented, and even enhanced, by the collapsing of geographical and physical barriers by computer networks. Furthermore, the decentralized management of networks, such as the Internet, ensures that information exchange will garner little or no oversight. Thus, given the technology employed by computer networks, regulation or interdiction of proscribed information exchange is likely to be difficult or impossible.[192] The best and most logical legal construct through which regulation, valuation, and control over computer network interchange could be attempted is that governing intellectual property. The mercurial nature of present information and communication technologies, however, may defy even the ability of the current intellectual property regime to regulate commerce in intangible goods.[193]

---

189. *See* James W. Nickel, *Computer Networks and Normative Change*, *in* THE INFORMATION WEB, *supra* note 14, at 161, 161-62.

190. *See* Anne W. Branscomb, *Overview: Global Governance of Global Networks*, *in* TOWARD A LAW OF GLOBAL COMMUNICATIONS NETWORKS, *supra* note 15, at 1, 17; Wright, *supra* note 55, at 94.

191. *See* Branscomb, *supra* note 190, at 17; Anne W. Branscomb, *Common Law for the Electronic Frontier*, SCI. AM., Sept. 1991, at 154, 156.

192. *See* Lynch, *supra* note 2, at 19.

193. *See* OTA INTELLECTUAL PROPERTY REPORT, *supra* note 123, at 19; Branscomb, *supra* note 190, at 17.

A. *Patents and Software*

Global computer networks are by no means the first situation in which the absence of physical barriers has presented quandaries of ownership and control.[194] Concerns for the protection of American "artistic and intellectual creativity" and innovation, research, and development form the basis for the entire field of intellectual property law.[195] Knowledge or ideas associated with technological advances may be created as pure intellectual goods or embodied to some degree in a physical form, such as an invention.[196] Like physical goods, intellectual goods may have great industrial value, and generating such knowledge may entail significant production costs of time and effort.[197] However, unlike physical goods, intellectual goods do not encompass the natural physical barriers that would exclude potential consumers.[198] Ideas, after all, may be held by more than one person at a time.[199]

Whether an idea is distributed by computer network, printing press, or word of mouth, the lack of physical barriers also makes the distribution costs for disseminating an intellectual good minimal or nonexistent.[200] Once intellectual goods are disclosed, there

---

194. Indeed, Sol Yurick, in his influential and insightful essay exploring the semiotic impulse of the modern information economy, points out that the rise of the global data network is only the latest, if perhaps the most pervasive and potent, manifestation of humanity's penchant for manipulating symbols to represent reality. SOL YURICK, BEHOLD METATRON, THE RECORDING ANGEL 16-24 (1985).

195. *See* ROBERT P. BENKO, PROTECTING INTELLECTUAL PROPERTY RIGHTS: ISSUES AND CONTROVERSIES 15 (1987).

196. *See* Richard P. Adelstein & Steven I. Peretz, *The Competition of Technologies in Markets for Ideas: Copyright and Fair Use in Evolutionary Perspective*, 5 INT'L REV. L. & ECON. 209, 217-19 (1985); Tom G. Palmer, *Intellectual Property: A Non-Posnerian Law and Economics Approach*, 12 HAMLINE L. REV. 261, 274-77 (1989).

197. BENKO, *supra* note 195, at 17.

198. *See* Paul A. Samuelson, *The Pure Theory of Public Expenditure*, 36 REV. ECON. & STAT. 387, 388-89 (1954) (discussing collective consumption goods).

199. *See* MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION: PUBLIC GOODS AND THE THEORY OF GROUPS 14 (1965) (discussing collective goods); Samuelson, *supra* note 198, at 388-89. In this way, intellectual goods appear to resemble public goods, such as national defense, which also may be held by more than one person at a time. *See* BENKO, *supra* note 195, at 17; Palmer, *supra* note 196, at 274-75. However, the potential undersupply of intellectual goods does not pose precisely the same problem as the potential undersupply of public goods. In the case of intellectual goods, unlike that of public goods, an individual consumer benefits only from the first unit consumed and not from any additional units. *See* Adelstein & Peretz, *supra* note 196, at 218-19. Additionally, although public goods can usually be obtained only from the initial source, each consumer of intellectual goods becomes a potential secondary source of supply. *Id.*

200. *See* BENKO, *supra* note 195, at 17; James C. Grant, *Global Trade in Services: A Corporate Perspective on Telecommunications and Data Services*, *in* ELECTRONIC HIGHWAYS

are no real barriers to the free appropriation of the good.[201] Because it is difficult to prevent persons from deriving the benefit of an intellectual good, a significant number of persons may consume the good without recompensing the originator of the good.[202] This lack of recompense may discourage creation of intellectual goods, leaving the market for the good undersupplied.[203] Consequently, where physical barriers are lacking, legal barriers have been designed to provide control over intellectual property.

1. The Patent System

In the United States, the most prominent set of legal barriers designed to correct potential undersupply in the market for technologically valuable intellectual goods is the federal patent system. Article I, Section 8, Clause 8 of the United States Constitution grants Congress authority to "promote the progress of science and the useful arts" by securing to inventors for a limited time the exclusive rights to their work.[204] Congress has chosen to exercise this power by implementing a system of patents that grants a seventeen-year, exclusive right to use a new process, machine, article of manufacture, or composition of matter.[205]

Because patents grant the patent holder an exclusionary right to the patented invention, patents have been loosely termed "monopolies."[206] Patent lawyers have long protested this label,[207] and economists have suggested that a patent does not necessarily confer a true monopoly.[208] Nonetheless, although some patents

---

FOR WORLD TRADE: ISSUES IN TELECOMMUNICATION AND DATA SERVICES 101, 101 (Péter Robinson et al. eds., 1989) [hereinafter ELECTRONIC HIGHWAYS].

201. BENKO, *supra* note 195, at 17.

202. *See id.*

203. *Id.*

204. U.S. CONST. art. I, § 8, cl. 8.

205. 35 U.S.C. §§ 101, 154 (1988).

206. *See* Edmund W. Kitch, *Patents: Monopolies or Property Rights?*, 8 RES. L. & ECON. 31, 33 (1986).

207. The patent merely allows the holder to exclude others from making, using, or selling the invention and does not confer on the holder an affirmative right to make, use, or sell. *See* 1 ERNEST B. LIPSCOMB III, LIPSCOMB'S WALKER ON PATENTS § 1:6, at 45 (3d ed. 1984).

208. *See* Kitch, *supra* note 206, at 33. Unlike the true monopolist, patent holders may face a marketplace containing a variety of substitutes for their product and, therefore, be forced to price their products competitively. *Id.* at 32-33. Additionally, failure to price a patent-derived product competitively may deprive the patent holder of information necessary to identify the boundaries of the market. *Id.* at 38-39. Although this information may be irrelevant to the true monopolist, its absence may prevent the patent holder from dominating the market when the patent expires, because other firms may more easily enter the market and erode the patent holder's preeminence. *Id.*

probably do confer a virtual monopoly on their holders, all patents represent some restraint on trade.[209] Consequently, patents are likely to generate the type of inefficiencies associated with monopolies: higher prices, restricted supplies, and inefficient allocation of resources.[210] Patents are, in fact, specifically designed to create such inefficiencies; otherwise, the respective good might not be produced at all. The societal costs generated by the patent system, however, must not be allowed to exceed the benefits of the intellectual goods the system fosters.[211]

This balance of costs and benefits is struck in large measure by severely restricting the availability of patents.[212] Patents are available only for inventions that meet narrowly defined standards of novelty, usefulness, and nonobviousness.[213] Before a patent issues, its application must pass through an extensive administra-

209. *Id.* at 33; *see* BENKO, *supra* note 195, at 19.

210. BENKO, *supra* note 195, at 19.

211. Several competing theories have been suggested to account for the beneficial effects of patenting. *See generally*, Rebecca S. Eisenberg, *Patents and the Progress of Science: Exclusive Rights and Experimental Use*, 56 U. CHI. L. REV. 1017, 1024-44 (1989) (reviewing major theories of patent rights).

The first of these theories suggests that patents encourage inventors to engage in inventive activity because of the potential rewards to be reaped from exclusive control of their inventions. *See* William F. Baxter, *Legal Restrictions on Exploitation of the Patent Monopoly: An Economic Analysis*, 76 YALE L.J. 267, 268-70 (1966); John S. McGee, *Patent Exploitation: Some Economic and Legal Problems*, 9 J.L. & ECON. 135, 136-38 (1966).

An alternative theory, espoused in many court decisions, holds that patents are socially useful, because they encourage disclosure of inventions that might otherwise be kept secret. *See, e.g.*, Sinclair & Carroll Co. v. Interchemical Corp., 325 U.S. 327, 331 (1945); Universal Oil Prods. v. Globe Oil & Ref. Co., 322 U.S. 471, 484 (1944).

Yet another set of theories suggests that patents offer an incentive for firms to make the investment in innovation through developing existing inventions for practical purposes. At least two major variations of this theory have been proposed. *See* Eisenberg, *supra*, at 1036-44. The first of these suggests that monopoly conditions, such as those attending a patent right, are most conducive to the commercial development of new inventions. *See* JOSEPH A. SCHUMPETER, CAPITALISM, SOCIALISM, AND DEMOCRACY 87, 89 (1950); *see also* Vernon W. Ruttan, *Usher and Schumpeter on Invention, Innovation, and Technological Change*, 73 Q.J. ECON. 596, 600-01 (1959); Carolyn S. Solo, *Innovation in the Capitalist Process: A Critique of the Schumpeterian Theory*, 65 Q.J. ECON. 417, 423 (1951). A different theory of innovation holds that patent rights mimic property rights, and thus the patent holder herself has the greatest interest in managing the invention productively and efficiently. *See* Edmund W. Kitch, *The Nature and Function of the Patent System*, 20 J.L. & ECON. 265, 276-77 (1977); *cf.* Harold Demsetz, *Toward a Theory of Property Rights*, 57 AM. ECON. REV. 347, 354-56 (1967) (arguing that when a community right is affected by externalities, it becomes economic to internalize benefits and costs).

At least some economists have asserted that none of these approaches are correct; rather, they say, patents actually generate more societal costs than benefits. *See* BENKO, *supra* note 195, at 19.

212. *See* Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 146, 150 (1989).

213. 35 U.S.C. §§ 101-103 (1988).

tive review designed to ensure that the invention in question meets these standards.[214] To qualify for a patent, an inventor must disclose in detail how the invention is made and used; at the end of the seventeen-year period of exclusivity, this information will pass into the public domain for all to use.[215]

2. Software Patenting

Computer software is foremost among the valuable and technologically sophisticated information-based products that bear the hallmarks of an intellectual good.[216] As such, software has been deemed a prime candidate for intellectual property protection.[217] Copyright remains the most prominent form of protection for computer programs in the United States; consequently, patent protection is often assumed to be unavailable for software inventions, even by those who should know better.[218] However, patent protection would seem naturally adapted to cover software inventions. Computer software comprises a set of instructions that defines sequential states of a machine. Thus, it follows that software might be protected as a "process" under the patent laws, because software is, in essence, a process or method carried out, in, or by, a computer system.[219] Furthermore, patent protection is often more desirable than copyright protection due to the breadth of protection available under the patent laws and because the scope of patent protection is well tailored to utilitarian articles such as computer programs.[220]

---

214. *Id.* § 112.

215. *See Bonito Boats*, 489 U.S. at 151 (citing United States v. Dubilier Condenser Corp., 289 U.S. 178, 186-87 (1933)).

216. *See* OTA INTELLECTUAL PROPERTY REPORT, *supra* note 123, at 117; Jeffrey S. Goodman, Note, *The Policy Implications of Granting Patent Protection to Computer Software: An Economic Analysis*, 37 VAND. L. REV. 147, 148-49, 156-57 (1984).

217. *See, e.g.*, NATIONAL COMM. ON NEW TECHNOLOGICAL USES OF COPYRIGHTED WORKS, FINAL REPORT 1 (1978).

218. *See, e.g.*, S. REP. NO. 377, 101st Cong., 2d Sess. 21 (1990) ("The only protection afforded to inventors of software is a copyright.").

219. *See* John P. Sumner & Steven W. Lundberg, *The Versatility of Software Patent Protection: From Subroutines to Look and Feel*, COMPUTER LAW., June 1986, at 1, 6.

220. *Id.* Patent protection is considered broader than copyright protection, because independent development of a protected item constitutes infringement under the former but not under the latter. *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 478 (1974) (patent law forbids independent creation as well as copying of subject matter forbidden by copyright). *Compare* 1 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 2.01[A] (1993) (copyright protection is available so long as a work is not copied but is the product of the author's independent efforts) *with* 4 DONALD S. CHISUM, PATENTS § 16.02[2], at 16-9 (1992) (any unauthorized manufacture, use, or sale of a patented item is infringement regardless of the infringer's knowledge, notice, or intent). Copyright protection may also be subject

The judicial application of patent law to software inventions has had a tangled history, which perhaps leads to the notion that such protection is unavailable.[221] The roots of this notion likely begin with the decision of the United States Supreme Court in *Gottschalk v. Benson*,[222] which dealt with patent claims to a method of converting digital signals from one form to another. In *Benson*, the Court held that claims to a mathematical algorithm, or claims that effectively preempt the use of a mathematical algorithm, are invalid, because they are drawn to nonstatutory subject matter.[223] The Court's primary concern appeared to be that mathematical formulae, as laws of nature, might be encompassed by such patent claims.[224] However, this fear appeared in part to arise from the curious definition of algorithm employed by the Court. Rather than giving "algorithm" its broad meaning[225] or even its meaning to computer scientists,[226] the *Benson* Court defined the word as a procedure for solving a mathematical problem.[227]

The resulting ambiguity of the *Benson* holding prompted the Court to return to the question of software patentability twice more

---

to "fair use" exceptions, such as copying to allow reverse engineering. *See* Sega Enters. v. Accolade, Inc., 977 F.2d 1510, 1521 (9th Cir. 1992), *and modified*, No. 92-15655, 1993 U.S. App. LEXIS 78 (9th Cir. Jan. 6, 1993) (copying of computer program permitted under copyright statutes to facilitate reverse engineering).

The copyright laws were originally developed to protect literary and artistic works. In general, the application of these laws to protect technological items has been problematic for the courts. *See* Dennis S. Karjala, *Copyright, Computer Software, and the New Protectionism*, 28 JURIMETRICS J. 33, 41-43 (1987). Indeed, some commentators have asserted that copyright is an altogether inappropriate form of protection for a utilitarian item such as a computer program. *See, e.g., id.* at 49-51; Pamela Samuelson, *CONTU Revisited: The Case Against Copyright Protection For Computer Programs in Machine Readable Form*, 1984 DUKE L.J. 663, 753.

221. *See generally* Donald S. Chisum, *The Patentability of Algorithms*, 47 U. PITT. L. REV. 959 (1986) (reviewing history of software patent decisions); R. Lewis Gable et al., *The Intelligent Patent Drafter and Compliance With the Requirement of Statutory Subject Matter*, *in* ELECTRONIC AND COMPUTER PATENT LAW 145 (Robert G. Sterne ed., 1990) (same); Marilyn G. Smith, *Patentable Subject Matter*, *in* ELECTRONIC AND COMPUTER PATENT LAW, *supra*, at 119 (same); Richard H. Stern, *Tales From the Algorithm War:* Benson *to* Iwahashi, *It's Deja Vu All Over Again*, 18 AM. INTELL. PROP. L. ASS'N Q.J. 371 (1991) (reviewing history of algorithm software patent decisions).

222. 409 U.S. 63 (1972).

223. *Id.* at 71-72.

224. *Id.* at 67.

225. *See* Alfred Z. Spector, *Software, Interface, and Implementation*, 30 JURIMETRICS J. 79, 80 (1989) (defining algorithm in a broad sense).

226. *See* Allen Newell, *Response: The Models Are Broken, The Models Are Broken!*, 47 U. PITT. L. REV. 1023, 1024 (1986) (defining algorithm).

227. 409 U.S. at 65.

for clarification. In *Parker v. Flook*,[228] the Court again considered a process invention that included steps for solving a mathematical equation. Returning to its concern that natural laws or their equivalent not be patented, the Court stressed that some other inventive concept aside from the discovery of a natural phenomenon, such as a mathematical algorithm, is required for patentability.[229] Additionally, the Court held that simply reciting a post-solution application of the result of an algorithm, as Flook had done, does not transform an unpatentable method claim into statutory subject matter.[230]

In a later case, *Diamond v. Diehr*, the Court reiterated its position that a mathematical algorithm executed by a digital computer to solve a mathematical equation is tantamount to a law of nature and, therefore, cannot be statutory subject matter.[231] However, the Court appeared to soften its stance by emphasizing that a claim drawn to otherwise statutory subject matter did not become unpatentable simply because it employed a mathematical formula, computer program, or digital computer.[232] The Court also emphasized that claims must be considered as a whole to determine patentability.[233] Applying its new and less stringent test in *Diehr*, the Court held the disputed claims to be patentable, reasoning that the *Diehr* claims were not an attempt to patent a mathematical formula but rather a patent application for an industrial process with steps that involved a mathematical formula.[234]

In view of the similarity of the subject matter of these cases, particularly that of *Flook* and *Diehr*, the distinction which made one set of claims patentable and the others unpatentable has

228. 437 U.S. 584 (1978). *Flook* involved a method claim for updating at least one variable involved in a process for the catalytic conversion of hydrocarbons. *Id.* at 586. The novelty of the claim depended on the use of a mathematical algorithm for calculating an updated alarm limit. *Id.* at 585. Flook argued that his claims circumvented the *Benson* doctrine by reciting a use for the alarm limit after its calculation and by limiting the claim to a particular technological field. *Id.* at 589-90. However, the Court found Flook's method unpatentable because of the relationship of the algorithm to the claimed invention. *Id.* at 594-95.

229. *Id.* at 589.

230. *Id.* at 590.

231. 450 U.S. 175, 185-86 (1981). The claims reviewed in *Diehr* concerned a process for curing rubber in a heated press. *Id.* at 177. The method required continuous measurements to be made of the temperature in the press; the measurements were then fed into a digital computer that, using a well-known mathematical formula, calculated the curing time and opened the press when the proper time had elapsed. *Id.* at 177-79.

232. *Id.* at 187.

233. *Id.* at 188.

234. *Id.* at 191.

escaped most commentators.[235] The distinction drawn by the Court appeared to be primarily one of context: The claims in *Flook* simply concerned a number and a method for obtaining it. In contrast, the claims in *Diehr* specified a particular application of the calculated value to a physical apparatus.[236]

In the wake of the *Benson-Flook-Diehr* trilogy of cases, lower courts have themselves developed an algorithm of sorts—a two-part test to determine whether claims reciting mathematical steps are patentable.[237] First, the court determines whether a given patent claim directly or indirectly recites a mathematical algorithm.[238] If a mathematical algorithm is involved, the court then determines whether the invention, taken as a whole, is no more than the algorithm itself or whether the algorithm simply plays a functional role in either one or more steps of a process claim or the elements of an apparatus.[239] In the latter situations, the claim is held to meet the statutory subject matter requirement.[240]

The end result is that for all practical purposes, most forms of software are patentable in the United States, unless the software comprises an unapplied mathematical equation.[241] Since naked mathematical equations have never met the requirements for patentable subject matter, software stands on an equal footing with other process inventions.[242] Consequently, as with other inventions, the patentability of software will largely depend on how the invention is claimed.[243] The United States Patent Office now routinely issues patents for software that is claimed in the correct manner.[244]

A variety of approaches are available to claim software inventions successfully. Because software configures a physical machine, the drafter of the patent claims may use "means plus function" claims to focus on the functional components of the spe-

235. *See, e.g.*, Irah Donner, *Patenting Mathematical Algorithms That 'Embrace' Mother Nature*, COMPUTER LAW., May 1992, at 1, 5.

236. *See* Gable et al., *supra* note 221, at 152-53, 155-57.

237. *See* Arrhythmia Research Technology v. Corazonix Corp., 958 F.2d 1053 (Fed. Cir. 1992); *In re* Meyer, 688 F.2d 789, 795-96 (C.C.P.A. 1982); *In re* Abele, 684 F.2d 902, 905-08 (C.C.P.A. 1982).

238. *Arrhythmia Research*, 958 F.2d at 1058.

239. *Id.*

240. *Id.*

241. *See* Sumner & Lundberg, *supra* note 219, at 3.

242. *Id.*

243. *See* Gable et al., *supra* note 221, at 149; Stern, *supra* note 221, at 376.

244. *See* Gable et al., *supra* note 221, at 149.

cial purpose machine created by the software.[245] Claims to a software invention may also be allowable if phrased in terms that refine or limit process steps or that define the structural relationship between physical elements of an apparatus claim.[246] The claim may be directed toward transforming something from one physical state to another.[247] Alternatively, the steps of a program may be defined as method claims, or the software itself may sometimes even be claimed as a product or article of manufacture.[248]

B. Territorial Limits

The issue of software patentability has not been limited to the United States; the same inquiry has been played out in a variety of nations with a variety of results. As a general rule, there is no general rule; criteria for patent protection vary from nation to nation.[249] Some nations have no patent system at all; others have patent laws at odds with those of the United States. Concerning the protection of software, the diversity of approaches ranges from nations such as Denmark and Panama, which grant full patent protection to software, to nations such as Brazil and Bulgaria, which grant no patent protection to software.[250] Nations like the United States and many others fall somewhere in between.[251] As might be expected, these variations in protection can, and do, come into conflict when activities proscribed in one nation cross over into another.

1. Territoriality and the Courts

It follows from the variation in patent criteria between nations that some inventions which are patented in the United States will be free for public use in other nations. It is predictable that some enterprising individuals will attempt to take advantage of this disparity in patent protection. For example, in *Deepsouth Packing*

245. *See id.* at 169; Meador & Brunell, *supra* note 64, § 12.3.2.1; Rick D. Nydegger, *Practical and Legal Considerations in Drafting A U.S. Patent Application for Computer-Related Inventions*, 18 RUTGERS COMPUTER & TECH. L.J. 109, 125 (1992).

246. Gable et al., *supra* note 221, at 168-69; Meador & Brunell, *supra* note 64, § 12.3.3.3.

247. Meador & Brunell, *supra* note 64, § 12.3.3.3.

248. *Id.* §§ 12.3.2.2, 12.3.2.3.

249. *See generally id.* (cataloging the patent requirements of various jurisdictions).

250. *See generally* Baxter, *supra* note 211 (comparing the patent law protections of several nations).

251. *See generally* Robert Bigelow, *Proprietary Rights in Software—The 1991 Experience*, TRANSNAT'L DATA & COMM. REP., Jan.-Feb. 1992, at 10, 11-12 (summarizing international availability of software protection).

Co. v. Laitram Corp.,[252] an accused infringer exported the components of a shrimp-deveining machine, which were assembled outside the country into an allegedly infringing device.[253] The Supreme Court held that these actions did not constitute infringement of the patent.[254]

In reaching this decision, the Court obviously considered the potential for intruding on the sovereignty of other nations. The fully assembled infringing device was never within U.S. territory, and the Court stressed that "[o]ur patent system makes no claim to extraterritorial effect; 'these acts of Congress do not, and were not intended to, operate beyond the limits of the United States.' "[255] United States courts have since extended this principle to hold that no infringement exists for the foreign sale of a machine for the manufacture of an infringing product[256] or for the sale of equipment capable of infringing a U.S. process patent.[257] These decisions effectively limit the range of patent protection to within the U.S. territorial market.

The courts are not always so sanguine about the extraterritorial implications of patent enforcement. For example, in *Spindlefabrik Suessen-Schurr v. Schubert & Salzer Maschinenfabrik Aktiengesellschaft*,[258] the United States Court of Appeals for the Federal Circuit upheld an injunction preventing a foreign infringer from engaging in activity relating to the manufacture, sale, use, or commercialization of an infringing product for use in the United States.[259] The defendant argued that, because the injunction applied to devices manufactured abroad, it impermissibly extended American patent authority beyond the boundaries of the United States.[260] The Federal Circuit rejected this argument, stating that the prohibition did not represent an extraterritorial application of American jurisdiction, because it involved only products for use in

252. 406 U.S. 518 (1972), *reh'g denied*, 409 U.S. 902 (1972).

253. *Id.* at 519.

254. *Id.*; *accord* Amstar Corp. v. Envirotech Corp., 823 F.2d 1538, 1546 (Fed. Cir. 1987) (export of unassembled elements of infringing apparatus was not infringement).

255. *Deepsouth Packing*, 406 U.S. at 531 (quoting Brown v. Duchesne, 60 U.S. (19 How.) 183, 195 (1857)). By contrast, assembly of an infringing device within the United States—even if intended only for sale abroad—has been held to constitute infringement. *See* Packard Instrument Co. v. Beckman Instruments, 346 F. Supp. 408, 411 (N.D. Ill. 1972).

256. Ductmate Indus. v. Lockformer Co., 226 U.S.P.Q. (BNA) 278, 279 (N.D. Ill. Feb. 12, 1985).

257. John Mohr & Sons v. Vacudyne Corp., 354 F. Supp. 1113, 1116 (N.D. Ill. 1973).

258. 903 F.2d 1568 (Fed. Cir. 1990).

259. *Id.* at 1578.

260. *Id.* at 1577-78.

the United States.[261] Thus, although careful to honor the letter of the *Deepsouth Packing* decision, the *Spindelfabrik* Court's holding suggests a strong commitment by current U.S. courts to enforce patent exclusivity against foreign infringers as soon as any nexus with U.S. territory is established.

2. Territoriality and the Legislature

The courts have not always adopted the most protective attitude toward extraterritorial infringement of U.S. patents. Congress has been quick to intervene when it has perceived gaps in U.S. patent protection. For example, in response to the *Deepsouth Packing* decision, Congress added a new section to the patent statutes, which effectively overruled the specific holding of *Deepsouth Packing*.[262] The general rule articulated in *Deepsouth Packing*, of course, remains sound, based as it is on respect for fundamental principles of sovereignty in international law. However, when these principles created a loophole in the protection of the patent law, Congress responded by carving out a limited exception going beyond the U.S. territorial market. This presaged a wave of similar enactments through the end of the 1980s, each aimed at plugging some territorial loophole in the U.S. patent law.[263]

a. Process Patent Protection

Four years after enacting the provision to plug the *Deepsouth Packing*'s gap concerning product patents, Congress enacted even more comprehensive legislation to fill another conspicuous gap

261. *Id.* at 1578.

262. 35 U.S.C. § 271(f) (1988); *see also* Amstar Corp. v. Envirotech Corp., 823 F.2d 1538, 1546 (Fed. Cir. 1987) (observing that Congress's 1984 enactment of § 271(f) effectively overruled *Deepsouth Packing*). Section 271(f) actually goes beyond the situation in *Deepsouth Packing* by providing that only a "substantial portion" of the components need be shipped outside the country to trigger certain types of liability. *See* 4 CHISUM, *supra* note 220, § 16.02[7].

263. Currently, few noticeable gaps seem to be recognized by the courts. First, the selling of an item for extraterritorial use in a patented process is not actionable by itself. *See* Standard Havens Prods. v. Gencor Indus., 953 F.2d 1360, 1374 (Fed. Cir. 1991), *cert. denied*, 113 S. Ct. 60 (1992). Second, extraterritorial use of a patented component in a noninfringing process is not actionable. *See* Amgen, Inc. v. United States Int'l Trade Comm'n, 902 F.2d 1532, 1540 (Fed. Cir. 1990). Legislation has been introduced in Congress to close the latter gap, at least with regard to biotechnology. *See Biotechnology Patent Protection Act of 1991: Hearings Before the Subcomm. on Intellectual Property and Judicial Administration of the Senate Comm. on the Judiciary*, 102d Cong., 1st Sess. (1991); S. REP. No. 260, 102d Cong., 2d Sess. (1992) (Report of S. 654); S. REP. No. 260, 102d Cong., 2d Sess. 1-17 (1991), *reprinted in* 1991 U.S.C.C.A.N. 1228-55.

involving the exclusivity of process patents.[264] For many years, imported goods produced through an infringing process presented a problem to process patent holders. Because the ambit of American patent law is limited to the territory of the United States, patented processes could be practiced offshore, and unless the product of the extraterritorial activity was patented, it could be brought into the United States and sold in competition with the fruits of the patentee's process. This, it was feared, greatly diluted the value of process patents that yielded valuable but nonpatentable products.[265] The problem was particularly acute in industries, such as biotechnology, that were heavily dependent on process patent protection.[266]

One remedy that Congress allowed process patent holders was the ability to initiate a proceeding with the United States International Trade Commission (ITC).[267] Under § 337 of the Tariff Act of 1930,[268] the ITC is empowered to exclude goods from entering the United States and to issue cease and desist orders to purveyors of goods already in the country.[269] Process patent holders may seek such remedies by showing in an ITC proceeding that imported goods were manufactured using their process, that an efficiently and economically run domestic industry uses the patented process, and that the importation of the infringing goods tends to destroy or substantially injure the domestic industry.[270] Before prohibiting the importation of such goods, the ITC must also determine that the injunction is in the public interest.[271]

Although § 337 offered patent holders some relief from the sale of infringing goods,[272] it quickly became apparent that the provision was not primarily designed for that purpose. Section 337 is first and foremost an unfair trade statute and, therefore, was found

264. *See generally* 4 CHISUM, *supra* note 220, § 16.02[6] (discussing 1988 Process Patent Amendments); Elizabeth R. Hall, Comment, *The Process Patent Amendments Act of 1988: Closing A Loophole in United States Patent Law*, 13 HOUS. J. INT'L L. 343 (1991) (same); Glen Law, Note, *Liability Under the Process Patent Amendments Act of 1988 for the Use of a Patented Process Outside the United States*, 60 GEO. WASH. L. REV. 245 (1991) (same); Glenn E.J. Murphy, Note, *The Process Patent Amendments of 1988*, 9 J.L. & COM. 267 (1989) (same).

265. S. REP. No. 83, 100th Cong., 1st Sess. 29, 31 (1987).

266. *Id.* at 30, 36.

267. *See id.* at 36-39.

268. 19 U.S.C. § 1337 (1988).

269. *Id.* § 1337(d), (f); S. REP. No. 83, at 36.

270. 19 U.S.C. § 1337(a)(1)(A).

271. *Id.* § 1337(d).

272. *See* S. REP. No. 83, at 36-37.

generally unsatisfactory as a means of guaranteeing a patent holder his term of exclusivity.[273] Whereas patent law generally assumes that a patent holder is entitled to his period of exclusivity in return for simply disclosing his invention, § 337 required more.[274] In an ITC proceeding, the patent holder was required to make burdensome showings regarding the existence of, and harm to, a domestic industry.[275] Remedies were predicated on the harm to the general public interest rather than on infringement of the patent holder's rights. More troublesome, however, was the lack of any penalty for importing goods manufactured by an infringing process. Because the ITC had no power to award damages for infringement, the only remedy available to a patent holder was injunctive relief.[276] Consequently, proceedings under § 337 did little to deter the importation of products manufactured by infringing processes; the importer would simply sell the goods until ordered to stop and keep whatever profits he made in the interim.[277]

This state of affairs prompted the introduction of several process patent amendment bills in Congress.[278] Because of sovereignty concerns, little could be done about the use of a U.S. patent holder's process in another nation; however, the importation of goods made by the infringing process could be addressed by measures stronger than the previous ITC exclusion order. A new provision to the patent statute, 35 U.S.C. § 271(g), created a cause of action for the importation into the United States of a product produced outside the United States by a process that would infringe a U.S. process patent. This made the full range of injunctive relief and damages available to process patent holders. Additionally, the evidentiary burden required for an ITC exclusion order to issue was greatly diminished, making this type of relief easier to obtain.

b. Patents In Space

A more specialized gap in U.S. patent protection was closed in 1990 with the enactment of legislation dealing with patents in

273. *See id.*

274. *Id.* at 36.

275. *Id.* at 37.

276. *Id.*

277. *Id.* at 38.

278. *See Process Patent Legislation: Hearings Before the Subcomm. on Patents, Copyrights and Trademarks of the Senate Comm. on the Judiciary*, 100th Cong., 1st Sess. 5-20 (1987) [hereinafter *Process Patent Hearings*].

space.[279] Commercial research in outer space holds the promise of developing valuable industrial property; however, it was unclear whether U.S. patent protection would extend to such activity.[280] Outer space is considered to be an area outside the territory of any nation,[281] and the U.S. patent statutes contain language limiting their scope to U.S. territory.[282] Given the international character of outer space, and in light of the *Deepsouth Packing* ruling, these statutory provisions made extension of U.S. patent laws to outer space a doubtful legal proposition.[283]

One proposed analysis concerning outer space patents implies that no problem exists at all, because U.S. spacecraft are in some sense equivalent to U.S. territory.[284] This view is based primarily on the holdings of certain older patent cases that considered American ships on the high seas as "floating islands" of U.S. territory for purposes of patent law analysis.[285] According to these cases, "[U.S. patent law] jurisdiction extends to the decks of American vessels on the high seas, as much as it does to all the territory of the country . . . ."[286] The same principle, it was argued, could be extended to American spacecraft.[287]

---

279. Patents in Space Act, Pub. L. No. 101-580, 104 Stat. 2863 (1990) (codified at 35 U.S.C. § 105 (West Supp. 1992)).

280. *See generally* Dan L. Burk, *Application of United States Patent Law to Commercial Activity in Outer Space*, 6 SANTA CLARA COMP. & HIGH TECH. L.J. 295 (1991) (discussing the extension of U.S. patent law to commercial activity in outer space); Glen H. Reynolds, *Legislative Comment: The Patents in Space Act*, 3 HARV. J.L. & TECH. 13 (1990) (same).

281. *See generally* Helen Shin, *"Oh, I have slipped the surly bonds of earth": Multinational Space Stations and Choice of Law*, 78 CAL. L. REV. 1375, 1379-82 (1990) (discussing the international character of outer space); Fred Kosmo, Note, *The Commercialization of Space: A Regulatory Scheme That Promotes Commercial Ventures and International Responsibility*, 61 S. CAL. L. REV. 1055, 1073-74 (1988) (same).

282. *See* 35 U.S.C. § 271(a) (1988) (liability for infringement committed "within the United States"); *id.* § 100(c) ("The terms 'United States' and 'this country' mean the United States of America, its territories and possessions.").

283. *See* S. REP. No. 266, 101st Cong., 2d Sess. 5 (1990), *reprinted in* 1990 U.S.C.C.A.N. 4058, 4061.

284. *See* Harry M. Saragovitz, *The Law of Intellectual Property in Outer Space*, 17 IDEA 86, 89-92 (1975) (suggesting this rationale for spacecraft).

285. *See* Gardiner v. Howe, 9 F. Cas. 1157, 1157-58 (C.C.D. Mass. 1865) (No. 5219); Marconi Wireless Tel. Co. v. United States, 53 U.S.P.Q. (BNA) 246, 259 (Ct. Cl. Apr. 6, 1942), *aff'd in part and vacated in part on other grounds*, 320 U.S. 1 (1943); *see also* Brown v. Duchesne, 60 U.S. (19 How.) 183, 198-99 (1857) (holding that French patent law applied to a French ship in an American port).

286. *Gardiner*, 9 F. Cas. at 1158.

287. *See* Saragovitz, *supra* note 284, at 89-92.

More recent patent cases have indicated that the courts are uncomfortable with the notion of "floating island" jurisdiction.[288] As one court stated, "a decision founded on the fiction that for purposes of the Patent Laws, U.S. ships and planes wherever found, are United States territory, would be founded on water."[289] In addition, this legal theory had been explicitly rejected in areas outside patent law. The U.S. Supreme Court has stressed that the jurisdictional character of ships derives more from registry than from territoriality.[290] Consequently, although the application of the "floating island" theory to U.S. spacecraft might lead to the correct result, there was little surety that courts would in fact employ such a problematic doctrine.[291]

As an alternative to "floating island" theories, Congress was urged to clarify the patent law by stating explicitly that it extends to activities aboard U.S. spacecraft.[292] Legislation to this effect was introduced as early as 1985 under the title of the Patents in Space Act[293] and was eventually enacted in 1990. The legislation added a new section, 35 U.S.C. § 105, to the patent statutes, explicitly extending U.S. patent law to activity aboard U.S. registry spacecraft and to foreign registry craft if provided for in an international treaty.[294]

C. *Extraterritorial Infringement*

The dissolution of geographic, political, and temporal barriers made possible by global computer networks may pose a new challenge to the operation of U.S. patent law—a challenge not yet fully

288. *See* Ocean Science & Eng'g v. United States, 595 F.2d 572, 573 (Ct. Cl. 1979); Decca, Ltd. v. United States, 544 F.2d 1070, 1073-74 (Ct. Cl. 1976).

289. *Decca*, 544 F.2d at 1074; *accord Ocean Science & Eng'g*, 595 F.2d at 574 ("[T]he constitutional power of Congress to make our patent laws applicable to processes carried out on U.S. flag ships and planes at sea is not challenged; the question is whether Congress has done so . . . .").

290. *See* United States *ex rel.* Claussen v. Day, 279 U.S. 398, 401 (1929); Cunard S.S. Co. v. Mellon, 262 U.S. 100, 123 (1923); Scharrenberg v. Dollar S.S. Co., 245 U.S. 122, 127 (1917).

291. *See* Reynolds, *supra* note 280, at 24-25.

292. *See, e.g.*, *Patents in Space: Hearings Before the Subcomm. on Courts, Intellectual Property, and the Administration of Justice of the House Comm. on the Judiciary*, 101st Cong., 1st Sess. 9 (1989) (testimony of Robert F. Kempf, Associate General Counsel for Intellectual Property, National Aeronautics and Space Administration); *id.* at 13 (testimony of Alan J. Kreczko, Deputy Legal Advisor, Department of State); *id.* at 16-17 (testimony of James E. Denny, Acting Assistant Commissioner for Patents, United States Patent and Trademark Office).

293. *See* H.R. REP. No. 788, 99th Cong., 2d Sess. pt. 1, at 1-11 (1988).

294. 33 U.S.C. § 105(a).

realized and likely impossible for the framers of the present patent code to anticipate, but a challenge whose parameters can already be seen. Differences between the laws of jurisdictions mean that network users run the risk of violating the law in one country or another.[295] Indeed, in some situations information service providers may consciously seek to use the disparity between the intellectual property laws of different nations to their advantage.[296]

Several possible infringement scenarios can be envisioned.[297] The first postulates the existence of a computer network user situated in the United States, who logs onto the network, accesses a machine that is physically outside of the United States, and runs software that would infringe a U.S. patent. The converse situation is also conceivable: a computer user outside of the United States, who runs software that would infringe a domestic patent were the user situated within U.S. territory and employs such software to access a computer or database that is within the United States. Either of these situations, or some combination of them, will likely pose a patent enforcement challenge with which the present patent law is ill-equipped to deal.

1. Defining "Use"

The patent law of the United States provides that persons who make, use, or sell a patented invention without the authorization of the patent holder are liable for infringement.[298] Method patent claims, such as those that might be drawn to patentable software, are most likely to be infringed by use, since processes are generally not considered "made" or "sold."[299] In the context of computer software, this generally means that the software will have to be running—configuring some machine—for infringement to take place.[300]

When global computer networks are concerned, however, the parameters for infringing use may be less than clear. On the network, infringing software may be running on remote nodes. In

295. Peter Robinson, *From TDF to International Data Services*, 11 TELECOMM. POL'Y 369, 373 (1987).

296. *See* Lynch, *supra* note 2, at 19.

297. *Cf.* Linda O. Smiddy, *Choosing the Law and Forum for the Litigation of Disputes*, *in* TOWARD A LAW OF GLOBAL COMMUNICATIONS NETWORKS, *supra* note 15, at 299, 299-300 (listing various possibilities for transnational incidents leading to data communications liability disputes).

298. 35 U.S.C. § 271(a) (1988).

299. *See* Meador & Brunell, *supra* note 64, § 12.3.3.1.

300. *See id.*

fact, where distributed processing takes place, the software may be running at several places at once, or portions of the program may run sequentially in different places.[301] Forays are now being conducted into configuring several networked machines into a "metacomputer," and it is conceivable that all the computers on a given network could run as a single computer.[302]

Much or all of this activity will be invisible to the computer network user. The simple act of logging onto the network may initiate the running of infringing software at some remote site; sending or receiving messages or accessing a remote computer may initiate more infringing activity of which the computer operator may be unaware.

Even if the operator is aware, or suspects, that his network use has initiated infringing software activity, it may not be within his control to halt or bypass the activity—packet routing and other network functions may proceed automatically through avenues not of his choice.[303] Where such situations are possible, the operator's lack of knowledge and control, coupled with his indirect connection to remote or distributed infringing software, might suggest that he is not "using" it under the statute.

However, the network user's employment of the infringing software, even if indirect and inadvertent, probably satisfies the statute's terms. The network user's lack of intent or knowledge in initiating infringing activity is almost certainly immaterial; it is well established that even unconscious or inadvertent infringement triggers liability under the patent statutes.[304] A more difficult issue arises from the question of control over remote and, possibly, automatic software infringement. Courts have seldom been called on to interpret the term "use," perhaps because the term is generally believed to be well understood.[305] However, the term, as employed in the patent statutes, is so very broad that there is little activity involving the patented item that would escape the term's scope. In a 1913 case, the Supreme Court stated that "[t]he right

301. *See* M. Peter Jurkat, *What Is a Computer Program in a Network Environment?*, *in* THE INFORMATION WEB, *supra* note 14, at 101, 103.

302. *See* Schultz, *supra* note 113, at 73 (discussing MEMNET network configuration).

303. *See supra* notes 72-86 and accompanying text.

304. *See, e.g.*, A. Stucki Co. v. Schwam, 634 F. Supp. 259, 264 (E.D. Pa.) (finding of patent infringement does not require knowledge or intent), *and vacated on other grounds*, 638 F. Supp. 1257 (E.D. Pa. 1986); Metal Film Co. v. Metlon Corp., 316 F. Supp. 96, 111 (S.D.N.Y. 1970) (same); Blair v. Westinghouse Elec., 291 F. Supp. 664, 670 (D.D.C. 1968) (same), *aff'd sub nom.*, Blair v. Dowd's, Inc., 438 F.2d 136 (D.C. Cir. 1970).

305. *See* 4 CHISUM, *supra* note 220, § 16.02[4], at 16-17.

to use is a comprehensive term and embraces within its meaning the right to put into service any given invention."[306]

The use of the phrase "to put into service" seems to imply that some measure of control and benefit is involved in infringing use. Thus, in a building constructed with flooring that infringes a patent, ownership and occupation of the building may constitute infringing use.[307] Simple occupation by a tenant of an infringing building, however, may not constitute infringement.[308] Similarly, mere possession of an infringing article does not constitute infringing use[309] nor does buying the product of a patented process constitute use of the process.[310] Presumably, in the latter examples, the actions associated with the infringing article are too passive and the benefits derived from it are too few to reach the level of putting the invention into "service."[311] However, logging onto and deriving benefits from a computer network's services seem likely to reach the necessary level for service and use.

2. Extended Instrumentalities

Even if network activity constitutes use of remote software, the use must be "within the United States" in order to infringe a patent under 35 U.S.C. § 271(a). Where global computer networks are concerned, however, it may be difficult to tell whether a use occurs within the United States. The host computer running an infringing program and the user accessing that program may be in different nations. When processing is distributed, only part of a program may run in the United States.[312] When many computers are configured as one, the physical components of the virtual machine may extend beyond the territorial borders of the United States.[313]

---

306. Bauer & Cie v. O'Donnell, 229 U.S. 1, 10-11 (1913).

307. Flat Slabs Patents Co. v. Wright, Barrett & Stilwill Co., 283 F. 345, 349 (D. Minn. 1920.).

308. *See generally* Turner v. Quincy Mkt. Cold Storage & Warehouse Co., 225 F. 41, 43-44 (1st Cir. 1915) (tenant occupying building with infringing steel skeleton concrete did not infringe).

309. *See* Beidler v. Photostat Corp., 10 F. Supp. 628, 630 (W.D.N.Y. 1935), *aff'd*, 81 F.2d 1015 (2d Cir. 1936). *But see* Olsson v. United States, 25 F. Supp. 495, 497-98 (Ct. Cl. 1938) (stockpiling of infringing howitzer guns for purposes of national defense constituted infringing use).

310. *See* 4 CHISUM, *supra* note 220, § 16.02[6].

311. *Cf.* Bauer & Cie v. O'Donnell, 229 U.S. 1, 11 (1913).

312. *See* Jurkat, *supra* note 301, at 114.

313. *See* Johnson, *supra* note 54, at 57; Schultz, *supra* note 113, at 73 (discussing MEMNET network configuration).

The United States Supreme Court has held that the patent law has no extraterritorial effect; however, in all the potential situations described above, the infringing activity has some connection to U.S. territory.[314] As previously discussed, when some connection with U.S. territory is established, Congress and the courts have generally taken the opportunity to enforce U.S. patent law.[315] Consequently, the enforceability of U.S. patent law in the context of global computer networks hinges on what type of connection to U.S. territory is necessary to trigger patent enforcement.

The answer to the question of patent territoriality may partly lie in legal decisions addressing the use of patented inventions that extend beyond the territory of the United States. For example, in *Rosen v. NASA*,[316] the Patent Office Board of Appeals was called on to determine the date on which a device for orienting a satellite was first reduced to practice.[317] The standard for reduction to practice requires that all the elements of the invention be operated in combination under conditions demonstrating that they "worked as intended to work in its practical contemplated use."[318] For the satellite, such conditions could only have occurred on its first use within the earth's orbit, raising the issue of whether the "reduction to practice" occurred "in this country" for purposes of the patent laws.[319]

In deciding this issue, the Board relied heavily on the "floating island" jurisdiction cases discussed above.[320] The Board also looked in part to an earlier interference decision, *Alford v. Loomis*,[321] for guidance in determining whether the use of the satellite occurred outside the United States.[322] The *Alford* decision concerned the conception and reduction to practice of a transmitter system; two of the transmitters were located within the boundaries of the United States, but the third was located on a U.S. craft. The Board in *Alford* held:

---

314. *See supra* notes 297-98 and accompanying text.

315. *See supra* notes 252-94 and accompanying text.

316. 152 U.S.P.Q. (BNA) 757 (Patent Off. Bd. of Patent Interferences Sept. 30, 1966).

317. *Id.* at 766-68; *see also* Robert F. Kempf, *Reduction to Practice of Space Inventions*, 50 J. PAT. OFF. SOC'Y 105, 116-19 (discussing *Rosen*).

318. *Rosen*, 152 U.S.P.Q. (BNA) at 765 (quoting Bedford v. Boothroyd, 319 F.2d 200, 209 (Ct. Cl. 1963)).

319. *Id.* at 766.

320. *Id.* at 767; *see supra* notes 279-94 and accompanying text (discussing "floating island" jurisdiction cases).

321. 252 F.2d 571 (Ct. Cl. 1958).

322. *Rosen*, 152 U.S.P.Q. (BNA) at 767.

> We are inclined to view the operation of an integrated instrumentality, a substantial portion of which is within the United States, and which is operated by and for residents of the United States, as not removed from the United States by reason of the projection of some elements of the instrumentality beyond the political boundaries of the United States because of the space requirements of the instrumentality in its field of practical application.[323]

Similarly, the satellite at issue in *Rosen*, when considered with its ground control as a system, was held to constitute an invention extending beyond the geographic boundaries of the United States; however, it was considered situated "in this country" for purposes of reduction to practice.[324]

Rosen and *Alford* might be distinguished from the present question, because they involved reduction to practice rather than infringement. Accordingly, it could be argued that the phrase "in this country," which applies to conditions of patentability,[325] has a different meaning than the phrase "within the United States," which applies to infringement of patents.[326] However, the rationale of *Rosen* was applied to an infringement case in *Decca Ltd. v. United States*,[327] suggesting that the "extended instrumentality" exception to territoriality is equally applicable to the realm of patent enforcement.

The *Decca* case involved the Omega system, a worldwide broadcast system built by the U.S. government.[328] The system was alleged to infringe the plaintiff's patent.[329] Like the system considered in *Alford*, the Omega system extended beyond the borders of the United States. It enabled ships and aircraft to determine their locations based on synchronized signals from transmitters located both in the United States and in various other nations.[330] Based on the theory articulated in *Rosen*, infringement was found to have occurred within the United States.[331]

This same extended instrumentality approach could easily be applied to an international computer linkage that coupled non-

323. *Id.* (quoting Patent Off. Bd. of Patent Interferences decision No. 84,143, *rev'd on other grounds*, Alford v. Loomis, 252 F.2d 571 (Ct. Cl. 1958)).

324. *Id.* at 768.

325. *See* 35 U.S.C. § 102(a), (b), (d) (1988).

326. *See id.* § 271(a).

327. 544 F.2d 1070 (Ct. Cl. 1976).

328. *Id.* at 1074.

329. *Id.*

330. *Id.*

331. *Id.* at 1073.

infringing U.S. activity with infringing extraterritorial activity. Particularly when the network user is situated within U.S. territory, the infringement could easily be viewed as operated or controlled within the United States if portions of the system projected beyond U.S. borders.

3. Inducement

A finding of patent infringement under 35 U.S.C. § 271(a), as discussed above, requires sufficient connection with U.S. territory so that the infringement could be considered to have occurred within the United States.[332] Under certain circumstances, however, a U.S. patent may be enforced against an infringer whose infringing activity occurs entirely outside the United States.

Specifically, inducement to infringe under 35 U.S.C. § 271(b) applies not only to domestic activity but also to wholly extraterritorial activity. Unlike the statutory sections defining direct infringement, § 271(b) does not include language limiting its scope to activity within the United States.[333] Consequently, although the direct infringement induced takes place within the United States, activity outside the United States may trigger this provision.[334] Thus, in the context of infringement on a global computer network, direct infringement within the United States would first have to be found under one of the theories discussed above. Liability for inducement might then be applied to the extraterritorial party controlling or employing the infringing software.

For liability to attach to an extraterritorial party, however, knowledge or activity, not required under the direct infringement provisions, must be present.[335] Inducement to infringe requires active steps to urge or encourage direct infringement.[336] Consequently, even though § 271(b) does not use the term "knowingly,"

332. *See supra* notes 312-13 and accompanying text.

333. *See* Hauni Werke Koerber & Co. v. Molins, Ltd., 183 U.S.P.Q. (BNA) 168, 170 (E.D. Va. June 11, 1974) ("[Section 271(b)] does not, on its face, limit application to acts committed 'within the United States.' A reasonable inference is that such limitation was intentionally omitted."); *cf.* I.C.E. Corp. v. Armco Steel Corp., 201 F. Supp. 411 (S.D.N.Y. 1961) ("35 U.S.C. § 271(c), which defines contributory infringement, does not include the limitation that such infringement must occur 'within the United States' which is found in subdivision (a) of that section. . . ."). *Compare* 35 U.S.C. § 271(b) (1988) *with id.* § 271(a).

334. *See* Honeywell, Inc. v. Metz Apparatewerke, 509 F.2d 1137, 1141 (7th Cir. 1975); Akzona, Inc. v. E.I. du Pont de Nemours & Co., 662 F. Supp. 603, 613 (D. Del. 1987). *See generally* 4 CHISUM, *supra* note 220, § 16.06[6].

335. *See generally* 4 CHISUM, *supra* note 220, § 17.04[2].

336. *See, e.g.*, Goodwall Constr. v. Beers Constr., 216 U.S.P.Q. (BNA) 1006, 1008 (N.D. Ga. Sept. 24, 1981).

courts have required some knowledge of the infringed patent and the consequences of the actions that result in infringement.[337] Knowledge may be inferred from the inducer's actions.[338] Such actions need not include active solicitation of infringement[339] but may include the entire "range of actions by which one in fact causes, or urges, or encourages, or aids another to infringe a patent,"[340] such as advertising or giving instruction regarding infringement.[341]

Consequently, this provision of the patent statutes provides an important deterrent to those whose extraterritorial activity contributes to direct infringement within the United States. In the context of a global computer network, then, liability for inducement could be applied to extraterritorial users of infringing software if they openly invited or solicited the use of that software or software-based service. More specifically, this provision might be applied to offshore "patent havens," which could otherwise offer infringing services on the network using the territorial limits of the patent law as a shield from liability.[342]

4. Importation

The transfer of data across international borders over computer networks implies a type of electronic trade, with information as the import and export. A computer operator employing international remote log-on and access functions is unlikely simply to manipulate data in the foreign machine; more often than not, the operator will want to download the results of the extraterritorial data processing to his own computer or printer. Such results might include data gathered by remote equipment, information retrieved from a remote database, or mathematical models generated by a remote supercomputer.

Of course, the information transferred is probably not itself patentable, because it does not constitute one of the categories of patentable subject matter.[343] However, where such information is

337. Water Tech. Corp. v. Calco, Ltd., 850 F.2d 660, 668 (Fed. Cir. 1988), *cert. denied*, 488 U.S. 968 (1988).

338. *Water Tech.*, 850 F.2d at 668; Oak Indus. v. Zenith Elecs. Corp., 726 F. Supp. 1525, 1542-43 (N.D. Ill. 1989); Drexelbrook Controls v. Magnetrol Int'l, 720 F. Supp. 397, 407 (D. Del. 1989), *aff'd*, 904 F.2d 45 (Fed. Cir. 1990).

339. *Oak Indus.*, 726 F. Supp. at 1542-43.

340. Fromberg, Inc. v. Thornhill, 315 F.2d 407, 411 (5th Cir. 1963).

341. *See generally* 4 CHISUM, *supra* note 220, § 17.04[4][f].

342. *See* Lynch, *supra* note 2, at 19 (discussing offshore information havens).

343. *See* Miller & Blumenthal, *supra* note 20, at 230.

retrieved or processed by offshore software that would infringe a valid U.S. patent, there exists a very real possibility that provisions regarding importation of the products of an infringing process may be triggered. Software, if patented, is patented as a process or method,[344] and the provisions of 35 U.S.C. § 271(g) and 19 U.S.C. § 1337(a) grant relief to the owner of an infringed process when the process is used outside of the United States to produce a product that is imported into the United States—even if the product itself is unpatented or unpatentable.

There is no explicit language in the legislative history of the Process Patent Amendments that would indicate that Congress was concerned with the ramifications of data transfer across national boundaries.[345] Thus, it seems unlikely that a numerical model or database search result is the sort of "product" contemplated by Congress when it enacted the provisions regarding offshore process patent infringement. Similarly, it seems unlikely that transborder computer network transmission is the type of "importation" that Congress had in mind. However, there is no language in the legislative history or on the face of the statutes that would limit their application to physical goods or to physical transport.[346] At least one commentator has concluded that the broad language of 35 U.S.C. § 271(g) does not differentiate between traditional processes that modify physical structure and computer processes that modify informational content.[347] Consequently, the statute could well be applied to the result of a software process.[348]

The plain language of the importation statutes in question offers few clues as to their scope,[349] and judicial interpretation of the relevant terms has been sparse. One court that considered the meaning of "imports" under the Process Patent Amendments stated that it has its "plain and ordinary meaning of bringing goods into

344. *See supra* notes 241-48 and accompanying text.

345. *See generally Process Patent Hearings*, *supra* note 278 (discussing process patent amendments); H.R. CONF. REP. No. 576, 100th Cong., 2d Sess. 486-90, 1085-91 (1988) (same); H.R. REP. No. 60, 100th Cong., 1st Sess. 1-113 (1987) (same); S. REP. No. 83, 100th Cong., 1st Sess. 29 (1987) (same). For an exhaustive listing of legislative documents relating to the Process Patent Amendments of 1988, see Law, *supra* note 264, at 251 n.27.

346. *See generally* Sources cited *supra* note 345.

347. *See* Blaney Harper, *Domestic Manufacturer Infringement Liability Under the Process Patent Act*, COMPUTER LAW., Oct. 1991, at 24, 25.

348. *Id.* at 25-26.

349. *See* Law, *supra* note 264, at 250-51 (noting that the language of 35 U.S.C. § 271(g) is simple; however, its meaning is ambiguous).

the United States from another country."[350] The use of the term "goods" in this interpretation might or might not include data or information. Certainly, the usual use of goods implies something tangible rather than ephemeral pulses of digitized information. However, international exchange in data services is increasingly conceptualized in terms of goods-based trade concepts.[351] The court in question was not considering the statute in terms of international computer networks and need not have employed the term "goods"—which does not appear on the face of the statute—had it undertaken such an interpretation.[352]

A court actually considering the electronic importation of data products derived from an infringing software process might be compelled, in the absence of clear guidance from the plain language of the relevant statutes, to look to the legislative history of these provisions.[353] The purpose of the legislation was clearly to provide process patent holders with protection against infringers who simply moved out of the physical territory of the United States but who still competed with the legitimate patent holder here.[354] A court considering offshore use of infringing software might well find that it closely parallels, if not duplicates, the situation Congress sought to remedy and, thus, would be an appropriate situation for application of the statute.

IV. The Price of Patent Enforcement

The potential for infringement of U.S. software patents through the medium of international computer networks seems to dictate that courts apply the patent provisions discussed above to deter such activity. Failure to do so could well dilute the value of software patents; using the inexpensive and elusive medium of the computer network, information services could be offered from offshore locations in countries, particularly underdeveloped countries, where intellectual property laws are not recognized or well enforced.[355] In situations when the patent fails to provide exclusiv-

350. Bristol-Meyers v. Erbamont, Inc., 723 F. Supp. 1038, 1044 (D. Del. 1989), *and dismissed*, 734 F. Supp. 661 (D. Del. 1990), *aff'd*, 918 F.2d 186 (Fed. Cir. 1990).

351. *See* Sauvant, *supra* note 5, at 360.

352. *Bristol-Meyers*, 723 F. Supp. at 1044. However, 19 U.S.C. § 1337(a)(1)(B) explicitly uses the term "articles," which might also have a connotation of tangibility.

353. *See, e.g.*, Blum v. Stenson, 465 U.S. 886, 896 (1984) (courts look first to statutory language, then to legislative history if the language is unclear); Amgen, Inc. v. United States Int'l Trade Comm'n, 902 F.2d 1532, 1538 (Fed. Cir. 1990) (same).

354. *Amgen*, 902 F.2d at 1538-40.

355. *See* Lynch, *supra* note 2, at 19.

ity, the patent becomes essentially worthless and the market for software inventions may become undersupplied as though no patents were available.

In the absence of a legal deterrent, the emergence of such offshore patent havens would be a straightforward function of economics: when access to an offshore version of useful software is cheaper than access to an on-shore legitimate copy, offshore havens would supply the demand for cheaper access. Although the price of access is likely to have several components, the major competing price constituents would likely be the cost of transmitting data offshore versus the cost of obtaining a software license. In order to quell competition from an offshore haven, the holder of a software patent would have to provide licenses for less than the cost of computer network transmission. Since network transmission is generally very cost-effective,[356] pricing software licenses lower than the cost of transmission might well mean that the patent holder could not recover her development costs.

As unpleasant as such a scenario may be, rash, reflexive, or mechanical enforcement of the patent laws could also have unpleasant results. As the Supreme Court has observed, "We cannot have trade and commerce in world markets and international waters exclusively on our terms, governed by our laws, and resolved in our courts."[357] Indeed, attempts to do so may well hamper the goals we would hope to accomplish in enforcing the patent laws: "The expansion of American business and industry will hardly be encouraged if . . . we insist on a parochial concept that all disputes must be resolved under our laws and in our courts."[358] This suggests that U.S. courts considering patent enforcement for international computer networks should be wary of decisions implicating national sovereignty, international trade negotiations, and research disincentives. Accordingly, courts should fashion appropriate doctrines to ameliorate unsuitable results.

356. *See supra* notes 122-25. The term "cost" here would include not only the actual charge for using the network but also factors such as the availability of sufficient bandwidth, delay in transmitting and receiving data, error rates, etc.

357. M/S BREMEN v. Zapata Off-Shore Co., 407 U.S. 1, 9 (1972) (discussing forum selection in international contracting).

358. *Id.*

A. *Offending National Sovereignty*

The previous extensions of U.S. patent law, as detailed above, have generally adhered to the spirit of the *Deepsouth Packing* holding by requiring some nexus of activity within the physical territory of the United States.[359] When U.S. patent law has been extended to activity outside of the United States, this analysis has been invoked only when the sovereignty of other nations was unlikely to be threatened. For example, in extending the jurisdiction of U.S. patent law to activity aboard U.S. flag spacecraft, the United States could feel fairly comfortable that no other nation's sovereignty was infringed. Outer space, like international waters, cannot be appropriated by any nation.[360] Thus, extending U.S. patent protection to activity aboard U.S. spacecraft would not conflict with the policies of any other sovereign.[361]

The situation may be quite different, however, in the case of an "extended instrumentality," such as an international computer network. Matters of international data exchange are already loaded with difficult, volatile, and perhaps unsolvable questions of sovereignty that could well be aggravated by the courts' injudicious application of U.S. patent law. These questions likely require congressional attention. In the meantime, the courts must at least proceed cautiously while cognizant of the challenges to sovereignty that have been posed by the global data network and which could be posed by enforcement of U.S. patent law in this context.

1. Information and Sovereignty

The primary challenge posed by international information exchange is essentially political and is caused by the erosion of political boundaries.[362] Countries have responded differently to the development of global electronic information capabilities. Some countries have embraced the new information network, some have sought to avoid it, others have sought to appropriate it for state purposes, and still others have sought to exploit it to enhance their economic position.[363] All nations, however, are beginning to

359. *See supra* notes 258-94 and accompanying text.

360. *See supra* note 281 and accompanying text.

361. *See Patents in Space: Hearings Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the House Judiciary Comm.*, 99th Cong., 1st Sess. 18-19 (1985) [hereinafter *1985 Patents in Space Hearings*] (statement of Professor Donald S. Chisum, University of Washington).

362. *See* Manet, *supra* note 7, at 18, 19.

363. Roche, *supra* note 26, at 24.

grapple with the same impact of the data net; where international data communications are concerned, national boundaries have become technologically irrelevant, because the technology simply bypasses traditional physical barriers.[364] Additionally, the functional economic boundaries generated by data exchange may overlap many political boundaries.[365]

This increasing porosity of national boundaries has made it difficult for nations to exercise traditional aspects of sovereignty, such as monitoring and controlling the flow of goods into and out of the country.[366] As a consequence, it has been suggested that the concept of political boundaries is rapidly becoming obsolete and requires reappraisal.[367] The nation-state may have been the political organization best suited to the industrial age, but it is not necessarily suited to an informatics age.[368]

This impact of the data network has been of particular concern to developing nations, which have had to deal with an additional economic effect impacting their sovereignty.[369] The development of the global data net has not proceeded evenly; data services have clearly become concentrated in developed nations with market economies and well-developed telecommunications infrastructures.[370] Underdeveloped nations, by contrast, have primarily been data suppliers and data purchasers.[371] This disparity between "information-rich" and "information-poor" nations has tended to cut off the information-poor countries from the benefits of the network, because the value-added benefits of data services tend to accrue at the processing and distribution stages.[372] Consequently, the continued growth of global computer networks is likely to increase the gap between developing and developed nations.[373]

---

364. Peter Robinson, *Sovereignty and Data: Some Perspectives*, TRANSNAT'L DATA REP., Oct.-Nov. 1984, at 419, 419.

365. Jake V. TH Knoppers, *National Policies and Boundaries in an Informatics Age*, TRANSNAT'L DATA REP., Aug.-Sept. 1984, at 351, 353.

366. *Id.*

367. *Id.*

368. *Id.*; Walter F. O'Connor, *Information—The Next Trade Problem?*, DATA COMM., Mar. 1986, at 186, 187.

369. Thomas Ennison, Jr., *Sovereignty Considerations in TDF—Developing Country Perspective*, TRANSNAT'L DATA REP., Apr.-May 1984, at 175, 177-80.

370. Sauvant, *supra* note 5, at 364.

371. SAUVANT, *supra* note 22, at 114; Sauvant, *supra* note 5, at 364-65.

372. Sauvant, *supra* note 5, at 366.

373. *See* Dertouzos, *supra* note 56, at 64-65.

The concentration of data in developed countries does not simply have economic ramifications; it has international political ramifications as well. Information is a vital resource.[374] The ability to collect, store, access, and process data confers political, economic, and social advantages on the nation controlling the data.[375] Effective control over the storage, processing, and transmittal of another country's information confers clear economic and military control over that country.[376]

By contrast, inability to control information undermines the sovereignty of developing nations by impairing their competence to make decisions about their own futures.[377] Indeed, in many instances, the information-rich nations may have more accurate information about the population, economy, and resources of an underdeveloped nation than has the underdeveloped nation itself.[378] This aspect of data communications technology has led to charges that developed nations are employing information superiority in a form of "neo-colonization."[379] Commentators in the "*dependencia*" school charge that information technology comprises a sort of imperialist tool to concentrate control of data processing and information generation in developed countries, while denying the benefits of information control to underdeveloped countries.[380]

Other commentators have suggested that information technology leads not only to informational dependence but also to cultural dependence.[381] This more subtle challenge to national identity and sovereignty is said, by members of the "structuralist" school of thought, to threaten cultural identity through the export of information that bears the imprint of alien selection, ordering, and arrangement.[382] This allows the dominance of one culture or language

374. Sauvant, *supra* note 5, at 359.

375. *Id.* at 367.

376. M.D. Kirby, *Urgent Need to Solve TDF Difficulties*, TRANSNAT'L DATA REP., Aug.-Sept. 1984, at 347, 349.

377. Sauvant, *supra* note 5, at 367.

378. *See Latins Embrace Informatics for Greater Sovereignty*, TRANSNAT'L DATA REP. Aug.-Sept. 1984, at 288, 288.

379. Manet, *supra* note 7, at 19.

380. *See* Roche, *supra* note 26, at 24.

381. James C. Grant, *Impact of Transnational Data Flows on Developing Countries*, TRANSNAT'L DATA REP., June-July 1984, at 233, 235; E. Gonzalez Manet, *New Media: Cultural Trojan Horse*, TRANSNAT'L DATA & COMM. REP., Mar. 1986, at 17-18; A. Sattar, *Implications of TDF for Developing Countries*, TRANSNAT'L DATA REP., Aug.-Sept. 1984, at 355, 357.

382. *See* Roche, *supra* note 26, at 25-26.

over another by virtue of information, data, and entertainment exports from the developed world.[383] Thus, it is suggested that, through the export of information, the culture of a few industrialized nations may be imposed on the rest of the world, resulting in homogenization of global culture.[384]

The disparity in benefit from the global data network has prompted information-poor countries to adopt strategies that would allow acquisition of data resources either physically or functionally.[385] Some nations have moved toward becoming "data havens" in order to capture international information resources within their territory.[386] The minimal cost of data transmission has already fostered offshore data processing—information is shipped by fiber optic cable to developing nations for processing, then transmitted back to the United States.[387] By offering juridical sanctuaries with a more lenient attitude toward data use than the country of origin, less-developed nations stand an even better chance of attracting not only data processing activity but also data storage.[388] In other instances, notably that of Brazil, policies have been adopted that disfavor export of local data and require foreign interests to deal locally in data processing procurement.[389]

2. Recent Incidents

Against this backdrop of nationalism and global tension, creative enforcement of U.S. patents is likely to be viewed as an attempt to manipulate data communications to the advantage of the United States. Underdeveloped nations already tend to view patents as a device employed by industrialized nations to maintain a monopoly over new technology, thereby crippling the development

383. Kirby, *supra* note 376, at 349.

384. *See* Roche, *supra* note 26, at 25.

385. *See* SAUVANT, *supra* note 22, at 165-66.

386. *See* G. Russell Pipe, *TDF Priorities: Building Infrastructures and Cooperation*, TRANSNAT'L DATA REP., Aug.-Sept. 1984, at 253, 259; *cf. Bahamas Wants Business Data*, TRANSNAT'L DATA & COMM. REP., Mar. 1986, at 8 (describing offshore "data free zone").

387. *See* G. Russell Pipe, *Telecommunications*, *in* THE URUGUAY ROUND: SERVICES IN THE WORLD ECONOMY, *supra* note 176, at 105, 111; Sidney Gorham, *Conference Report: Developing Countries Enter Data Services Market*, TRANSNAT'L DATA & COMM. REP., Mar.-Apr. 1991, at 14, 14-15.

388. *See* Lynch, *supra* note 2, at 19; De Sola Pool & Solomon, *supra* note 20, at 128; *see also* Pipe, *supra* note 387, at 105 (discussing a "relaxing" of regulation by developed nations in order to capture increased communications traffic).

389. *See* SAUVANT, *supra* note 22, at 169-77; João C.F. Albernaz, *Brazil's TDF Policy Builds National Independence*, TRANSNAT'L DATA REP., Jan.-Feb. 1984, at 49, 49; Jane Bortnik, *National and International Information Policy*, J. AM. SOC'Y INFO. SCI., May 1985, at 164, 166, 167; Ennison, *supra* note 359, at 177.

of nonindustrialized nations.[390] A finding of patent liability against a foreign network user attempting to access a U.S. information service effectively raises a nontariff barrier to international information access—as does imposition of liability against an American network user attempting to access a foreign information service. To the extent that such findings implicate the ability of other nations to control vital information flows, international animosity will be aroused.

This scenario is presaged by the international reaction of suspicion and outright hostility that has already attended U.S. actions involving transborder data flow implicating direct and indirect threats to the sovereignty of other nations. Concern over the manipulation of information access has been heightened, for example, by the actions of the United States against a French subsidiary of Dresser Industries.[391] In order to prevent the completion of an industrial contract for the Soviet Union, the United States cut off a French company's access to its North American database.[392] This resulted not only in stoppage of the Soviet work but also in the loss of millions of dollars from other uncompleted contracts.[393] Similary, the United States froze Iranian assets during the Iranian revolution and hostage crisis[394] and sought to sever Iranian access to the international Intelsat satellite information service.[395]

More direct encroachment of foreign sovereignty by the United States has also been the subject of international criticism. U.S. courts have twice enforced contempt orders against a foreign bank that refused to divulge confidential banking records protected by Bahamian banking laws.[396] The sanctions imposed in these cases have prompted an increasing international consensus that although "extraterritoriality" is usually defined as the attempt by one sovereign state to assert control over persons situated or conduct occurring in another sovereign state, the term has come to

390. *See* BENKO, *supra* note 195, at 28-29.

391. *See* Anne W. Branscomb, *Legal Rights of Access to Transnational Data*, *in* ELECTRONIC HIGHWAYS, *supra* note 200, at 287, 296.

392. *Id.*

393. Grant, *supra* note 381, at 233; *OECD Debates Data Trade and Access Rights*, TRANSNAT'L DATA & COMM. REP., Apr. 1986, at 5, 5 [hereinafter *OECD Debates*]; Peter Robinson, *Extraterritoriality and Data Flows*, TRANSNAT'L DATA & COMM. REP., June 1986, at 27, 28.

394. *See* Branscomb, *supra* note 391, at 296.

395. *See* Bortnik, *supra* note 389, at 166.

396. United States v. Bank of N.S., 691 F.2d 1384, 1391 (11th Cir. 1982); *see also* Robinson, *supra* note 393, at 28 (describing incident); Robinson, *supra* note 295, at 373 (same).

mean the enforcement of U.S. laws abroad.[397] These incidents of heavy-handed extraterritorial application of U.S. law have already prompted several nations, including France, the United Kingdom, Australia, and New Zealand, to enact statutes forbidding compliance with extraterritorial judicial orders requiring the transfer of data.[398]

In contrast to the prevailing U.S. approach, other nations have recognized the sensitivity and complexity of the issues raised by the protection of national interests through data-access restrictions.[399] The Canadian government has advocated the practices of prenotification and consultation with foreign governments before restricting its data access or that of its nationals.[400] Concerning extraterritorial application of laws relating to information flow, a similar awareness has grown of the need for discretion. For example, Norway has chosen to take a cautious approach to extraterritorial application of its data-protection laws.[401] Norwegian policy applies the laws to Norwegian ships in international waters and to offshore Norwegian platforms on the continental shelf but does not apply them to Norwegian holdings in Spitzbergen, where the laws could conflict with interests of Russian settlements.[402]

Such cautiousness should be at the forefront of extraterritorial application of U.S. patent law as indicated by the Supreme Court in *Deepsouth Packing*.[403] Indeed, such considerations are not unfamiliar to the formulation of the patent statutes. For example, the Patents in Space legislation was introduced into Congress on several occasions, each version entailing small but important textual changes.[404] Many of the revisions made in the language of the Patents in Space Act prior to its enactment were calculated to tailor the legislation to the milieu of the international space station *Freedom*.[405] In particular, the language of the Act was altered to avoid

397. John T. Burnett, *Information, Banking Law and Extraterritoriality*, TRANSNAT'L DATA & COMM. REP., Jan. 1986, at 17, 18; *see also* Robinson, *supra* note 393, at 27 (quoting Jonathan Fried).

398. Robinson, *supra* note 364, at 419, 420.

399. *See* Robinson, *supra* note 393, at 27.

400. *Id.* at 28; *OECD Debates*, *supra* note 393, at 6.

401. *See Norway: Extraterritoriality of Data Act*, TRANSNAT'L DATA REP., Aug.-Sept. 1984, at 299-300 (discussing Norwegian Ministry of Justice opinion concerning the application of Norway's Data Protection Act).

402. *See id.*

403. *See supra* note 252-57 and accompanying text.

404. For a history of the Patents in Space Act, see Burk, *supra* note 280, at 335-38.

405. *See id.* at 338-39. The Freedom space project is a multinational venture which, when completed, will comprise four connected modules, built by the United States, Japan, and

offending the interests of the United States' international partners. For example, nations involved in the space station project expressed concern that, due to the United States' dominance in the project, the language in the legislation extending U.S. patent law to space objects under the "jurisdiction or control" of the United States might affect modules on the registry of other nations.[406] In response to this concern, certain exclusionary language was incorporated into the Act's final form.[407] Such alterations were considered crucial to avoid offending the sovereignty of partner nations when applying U.S. patent law to activity in outer space;[408] similar considerations should be weighed before application of the patent law to activity in cyberspace.

International data services are beginning to figure importantly in discussions concerning international trade.[409] First, international information exchange forms the infrastructure for international trade.[410] For example, transnational computer communication systems are routinely used in, and are crucial to, the internal operations of international corporations.[411] Such networks may be used to integrate and coordinate simultaneous or sequential operation of production facilities in several different countries.[412] Computer networks are equally important in coordinating activities between international corporations, particularly in their capacity for Electronic Data Interchange (EDI).[413] Such electronic exchange of business information is rapidly replacing physical exchange of documents on paper.[414]

---

the European Space Agency and carried respectively on the registry of the nation or agency that built them. *See generally* OFFICE OF TECHNOLOGY ASSESSMENT, U.S. CONGRESS, OTA-BP-ISC-41, SPACE STATIONS AND THE LAW: SELECTED LEGAL ISSUES—BACKGROUND PAPER (1986) (discussing the legal issues raised by multinational space station activity); Mary B. McCord, Note, *Responding to the Space Station Agreement: The Extension of U.S. Law Into Space*, 77 GEO. L.J. 1933 (1989) (same).

406. Burk, *supra* note 280, at 345-49.

407. *Id.*

408. *Id.*

409. Robinson, *supra* note 295, at 374.

410. *See* SAUVANT, *supra* note 22, at 104-05.

411. *See id.*

412. *Id.* at 107; O'Connor, *supra* note 368, at 186.

413. *See* Grant, *supra* note 200, at 112. EDI is paperless communication of business matters between computers. *See* BENJAMIN WRIGHT, EDI AND AMERICAN LAW: A PRACTICAL GUIDE at xiii (1989). Documents commonly exchanged through EDI include purchase orders, transportation orders, invoices, and check stubs. *Id.*

414. Grant, *supra* note 200, at 112; *see also* BENJAMIN WRIGHT, THE LAW OF ELECTRONIC COMMERCE § 1.1.4 (1991) (describing EDI).

Second, exchange in information itself has become an important part of the international market. The exchange of services has traditionally been tied to a relatively limited geographic market; services, after all, tend to be intangible and nonstorable.[415] However, this has been radically changed by international communications networks, which allow instantaneous interaction over long distances between the producers and consumers of information-based services.[416] Consequently, international exchange in data services is increasingly conceptualized as an important part of international trade.[417] Indeed, many observers have gone farther, recognizing that data exchange is, in fact, the exchange of a commodity.[418] As a consequence, goods-related principles may be applicable to international data exchange.[419]

3. Data Exchange Policies

In contrast to the strategies of less-developed nations discussed in the previous section, the general strategy of nations with well-developed information resources has been to attempt to promote an international environment largely free of barriers to information-based trade.[420] Information-rich nations have asserted that regulatory restrictions impede development of the information industry and trade.[421] In particular, these nations have sought the removal of trade-restricting governmental policies to provide a stable and predictable framework for trade in services.[422] Such an international environment, it is believed, will foster capital-intensive corporate investment in information markets.[423] Consequently, the developed nations have used every available diplomatic and economic means to promote open market access to foreign data suppliers.[424]

---

415. Karl P. Sauvant, *Introduction* to ELECTRONIC HIGHWAYS, *supra* note 200, at 3, 4.

416. *Id.* at 5.

417. R. Brian Woodrow, *Trade in Telecommunication and Data Services*, *in* ELECTRONIC HIGHWAYS, *supra* note 200, at 15, 34.

418. *See* Sauvant, *supra* note 5, at 360.

419. *See OECD Debates*, *supra* note 393, at 5-6.

420. *See* SAUVANT, *supra* note 22, at 180.

421. *See* Sidney Dell, *Services: National Objectives*, *in* ELECTRONIC HIGHWAYS, *supra* note 200, at 43, 44; Sogo Okamura, *Economic Consequences of Information and Communication*, TRANSNAT'L DATA & COMM. REP., July 1986, at 14, 15.

422. *See* Sauvant, *supra* note 415, at 3.

423. *See* SAUVANT, *supra* note 22, at 180; Sauvant, *supra* note 415, at 3.

424. For an example of the use of diplomatic means to promote such open access, see *OECD Debates*, *supra* note 393, at 5-6.

The United States, as a major provider of information-based services, has assumed such a posture and has pushed other nations to permit free access to information services and to eliminate barriers to international data and information exchange.[425] The United States has also sought to use negotiations at the ongoing, international General Agreement on Tariffs and Trade (GATT)[426] as a vehicle for moving towards a more open information trade.[427] Spurred by U.S. policy, international discussion regarding data services and telecommunications has begun to shift toward a framework recognizing the importance of international trade in services.[428] Additionally, negotiations have commenced regarding the free exchange of services, particularly telecommunication and network services, under the GATT.[429]

This process is fragile and could easily be set back or compromised by the advent of a new patent-based restriction on access to foreign databases and information services.[430] Barriers to free information flow are likely to escalate through retaliation; restrictive practices by one nation are likely to prompt similar actions by other nations.[431] Protective actions by a few governments could start a "chain reaction of restrictions" as other governments follow suit or retaliate.[432] Protectionist practices of this type distort the trading system and the market mechanism at a time when trade is critical both to the recovery from global recession and to laying the foundation for a new global economy.[433]

---

425. *See* Dell, *supra* note 421, at 45; *see also* Fred Lazar, *Services and the GATT: U.S. Motives and a Blueprint for Negotiations*, 24 J. WORLD TRADE 135, 141-45 (1990) (discussing U.S. strategy for negotiations on services).

426. The term "GATT" is commonly used to refer to a complex incremental series of treaties that is constantly being revised and expanded. *See generally* JOHN H. JACKSON, WORLD TRADE AND THE LAW OF GATT app. at 888 (1969). The original 1947 GATT treaty provided a framework to which new provisions and new signatories are added almost yearly. *See id.* at 888-97 (listing over one hundred supplemental GATT treaties).

427. JACKSON, *supra* note 426, at 9-10; Bortnik, *supra* note 389, at 167.

428. Klaus W. Grewlich, *Information Economies and the Uruguay Round*, TRANSNAT'L DATA & COMM. REP., July 1987, at 13, 14; Stephen D. McDowell, *The Shaping of TDF Policy*, TRANSNAT'L DATA & COMM. REP., May 1989, at 19, 22.

429. *See* Arthur Dunkel, *Telecom Services and the Uruguay Round*, TRANSNAT'L DATA & COMM. REP., Jan.-Feb. 1992, at 17.

430. *See* Richard H. Snape, *Principles in Trade in Services*, *in* THE URUGUAY ROUND: SERVICES IN THE WORLD ECONOMY, *supra* note 176, at 5, 7; O'Connor, *supra* note 368, at 188.

431. *See* Sauvant, *supra* note 176, at 120; O'Connor, *supra* note 368, at 188.

432. OFFICE OF THE U.S. TRADE REPRESENTATIVE, U.S. NATIONAL STUDY ON TRADE IN SERVICES: TELECOMMUNICATIONS, DATA PROCESSING AND INFORMATION SERVICES TRADE PROBLEMS (1984), *reprinted in* 7 TRANSNAT'L DATA REP. 144, 148 (1984).

433. *Id.*; O'Connor, *supra* note 368, at 188.

The potential for the courts to precipitate such a foreign relations fiasco is heightened by recent experience involving U.S. patent law and international trade negotiations. Enforcement of the Process Patent Amendments has already raised issues with regard to the United States' obligations under the GATT. Under GATT,[434] the United States is required to refrain from discriminating against foreign goods.[435] Consequently, the drafters of the Process Patent legislation went to some length to point out that the legislation would apply to both foreign and domestic products even though foreign products were clearly the problem and domestic infringers were already subject to the full range of sanctions under U.S. patent law.[436]

However, these protestations have done little to convince the international community.[437] Under GATT, international trade disputes may be adjudicated by a three-member panel that makes findings and recommendations to the full GATT Council.[438] Following an unsuccessful challenge to Section 337 by the Dutch chemical company Akzo,[439] the European Community Commis-

434. General Agreement on Tariffs and Trade, Oct. 30, 1947, 61 Stat., Pts. 5 & 6, 55 U.N.T.S. 188.

435. *See* S. REP. No. 83, *supra* note 265, at 46.

436. *Id.* The Senate Report that eventually accompanied the proposed patent process legislation admitted that the inclusion of domestic infringers was simply a formality to comply with the GATT and had no impact upon domestic patent enforcement. *Id.*

437. *See generally* John W. Rogers III, *The Demise of Section 337's GATT-Legality*, 12 EUR. INTELL. PROP. REV. 275 (1990) (arguing that § 337 is inconsistent with GATT). *But see* Mark Modak-Truran, Comment, *Section 337 and GATT in the* Akzo *Controversy: A Pre- and Post-Omnibus Trade and Competitiveness Act Analysis*, 9 NW. J. INT'L L. & BUS. 382 (1988) (arguing that § 337 complies with fair treatment of foreign nationals requirement).

438. *See* John Richards, *Trade Related Intellectual Property Issues (TRIPS)*, 72 J. PAT. & TRADEMARK OFF. SOC'Y 906, 909 (1990) (describing procedure of GATT panel recommendation and GATT council approval); *EC Endorses Panel's Ruling That § 337 Violates GATT Non-Discrimination Rules*, 37 Pat. Trademark & Copyright J. (BNA) 302, 302 (1989) [hereinafter *EC Endorses Panels' Ruling*] (same).

439. *See* Akzo N.V. v. United States Int'l Trade Comm'n, 808 F.2d 1471, 1485 (Fed. Cir. 1986), *cert. denied*, 482 U.S. 909 (1987). Akzo argued that proceedings before the ITC, which resulted in an order excluding Akzo from importing products of a U.S. patented process into the United States, discriminated against Akzo as a foreign corporation. *Id.* According to this argument, foreign corporations accused of importing infringing products may be brought before the ITC rather than before a federal district court and may be denied procedural safeguards or rights available in a district court. *Id.* Consequently, Akzo argued, the proceeding under § 337 violated United States treaty obligations to treat foreign and domestic corporations alike. *Id.*

This argument was rejected by the United States Court of Appeals for the Federal Circuit, which stated that "[t]he appropriate inquiry is whether Akzo was afforded the same rights afforded to domestic firms in a § *337 proceeding before the Commission*." *Id.* The appellate court concluded that both Akzo and the U.S. complainant, DuPont, had been afforded the same rights. *Id.* Moreover, the court observed that other courts addressing this argument had con-

sion brought a proceeding against the United States under the GATT.[440] A GATT panel was appointed and, after an investigation, ruled that § 337 unfairly discriminates against foreign companies by denying them the choice of forum and procedural safeguards available to U.S. companies in federal district courts.[441]

Although the United States Trade Representative (USTR) could have blocked adoption of the report by the GATT Council, U.S. opposition was withdrawn in the face of possible international sanctions.[442] The USTR has since published, in the Federal Register, possible options for modifying U.S. trade laws to conform with the GATT ruling.[443] In the face of such controversy and international criticism against the United States for protectionist practices in communications and information trade,[444] attempts to extend

---

cluded that § 337 was not discriminatory, because it allowed ITC proceedings against foreign importers not only of allegedly infringing products but also against domestic importers of such products. *Id.*

440. *See Leak of GATT Panel Ruling Against U.S. Patent Clause Surprises USTR*, 37 Pat. Trademark & Copyright J. (BNA) 171, 171 (Dec. 8, 1988) ("The EC launched its challenge despite the fact that the original patent dispute was resolved privately by the two firms involved—Akzo N.V. of the Netherlands and DuPont."); *see also Judicial Conference—Federal Circuit*, 133 F.R.D. 245, 256-82 (1990) (review of Akzo incident and history of § 337 conflict with GATT).

441. *See USTR Proposes Changes in U.S. Patent Enforcement System Under Section 337*, 39 Pat. Trademark & Copyright J. (BNA) 259, 259 (Feb. 8, 1990) [hereinafter *USTR Proposes Changes*]; *Changes to § 337 Procedures Will Depend on Results of Uruguay Round*, 40 Pat. Trademark & Copyright J. (BNA) 131, 131 (June 7, 1990).

442. *See EC Endorses Panel's Ruling*, *supra* note 438, at 302 ("[F]ailure of the U.S. to respond to the panel ruling . . . could lead to retaliation against the U.S. by EC countries."); *USTR Proposes Changes*, *supra* note 441, at 259 ("The United States blocked the presentation of the GATT panel ruling until November 1989, when it withdrew its opposition and the GATT council adopted the panel report.").

443. Revisions to U.S. Patent Enforcement Procedures, 55 Fed. Reg. 3503 (1990) (request for public comments). There have been numerous suggestions as to how § 337 proceedings could be brought into compliance with the United States' international treaty obligations. *See, e.g.*, Committee on Patents, *Recommendations Addressing Proposed Amendments to Section 337 of the Tariff Act of 1930*, 46 REC. ASS'N B. CITY N.Y. 149, 150 (1991); Jeffrey S. Neeley & Hideto Ishida, *Section 337 and National Treatment Under GATT: A Proposal for Legislative Reform*, 13 FORDHAM INT'L L.J. 276, 289-297 (1989-90); New York Patent, Trademark and Copyright Law Ass'n, *Comments on Possible Amendments to Procedures for Enforcement of Patent Rights Responsive to GATT Criticism of Tariff Act § 337*, 72 J. PAT & TRADEMARK OFF. SOC'Y 700, 713-18 (1990); Lisa Barons, Note, *Amending Section 337 to Obtain GATT Consistency and Retain Border Protection*, 22 L. & POL'Y INT'L BUS. 289, 325-331 (1991). Legislation has also been proposed to harmonize § 337 with the GATT. *See* S. 148, 103d Cong., 1st Sess. (1993); *see also Bills Amend § 337 for GATT Compliance, 'Special 301' to Target Japan Patent Law*, 10 Int'l Trade Rep. (BNA) 199, 199 (Feb. 3, 1993) (legislation introduced by Senator Rockerfeller).

444. *See U.S. Accused of Protectionist Telecom Practices*, TRANSNAT'L DATA & COMM. REP., May-June 1992, at 7, 7.

U.S. trade protection to international computer networks are probably ill-advised.

4. Jurisdiction and Justiciability

An additional, related concern for courts entering the arena of international information exchange is the enormous complexity of the negotiations in this field. For each agreement reached regarding international data exchange, accommodation must be achieved among a multitude of participants, each with a particular area of responsibility to assert and a particular set of interests to protect. In the United States alone, governmental agencies likely to be involved in international negotiations over telecommunications and data services include the Department of Commerce, the Department of State, the Federal Communications Commission (FCC), the United States Trade Representative (USTR), and others.[445] Some of these entities are executive branch agencies, whereas others, such as the FCC, are independent regulatory agencies responsible to Congress.[446] All of them have some authority to engage in international negotiations and policymaking concerning computer network data exchange. In addition, as might be imagined, the agencies share a common propensity for jurisdictional disputes, uncoordinated efforts, and general confusion.[447]

This interagency Babel stems in part from the lack of any clear delineation of responsibility and authority in the legislation and executive orders that created these agencies. Thus, both the Commerce Department's National Telecommunications and Information Administration (NTIA) and the FCC are involved in fashioning telecommunications policy.[448] Considerable overlap exists even between agencies in the same branch of government and, in fact, may exist within a given agency. Within the State Department, for example, the Bureau of International Communications and Information Policy (CIP), which reports to the Under Secretary of State for Security Assistance, Science, and Technology, has responsibility for developing international telecommunications policy, and the Bureau of Economic and Business Affairs, which

445. *See* Jill Hills, *Dynamics of U.S. International Telecom Policy*, TRANSNAT'L DATA & COMM. REP., Feb. 1989, at 14, 16-17.

446. NATIONAL TELECOMMUNICATIONS AND INFO. ADMIN., U.S. DEP'T. OF COMMERCE, NTIA TELECOM 2000, at 171 (1987).

447. *Id.* at 173-74.

448. *Id.*

reports to the Under Secretary for Economic Affairs, has responsibility for handling telecommunications trade problems.[449]

To complicate matters further, in any given negotiation, any or all of these U.S. agencies may be dickering with any or all of the counterpart agencies in one or more foreign nations. Additionally, the negotiations may involve one or more official or quasi-official international agencies with jurisdiction over telecommunication or data exchange services, including the Directorate of the General Agreement on Tariffs and Trade, the Organization for Economic Cooperation and Development, the European Telecommunication Standards Institute, the International Standards Organization, and the International Telecommunication Union.[450]

The intricate political dance in which all these entities join to define the parameters of international computer network traffic has little elbow room for the additional, inexperienced participation of courts attempting to enforce U.S. patent interests. Heavy-handed or mechanical enforcement of the patent statutes in this setting could have unforeseen results, such as compromising carefully crafted U.S. positions in various international negotiations or even provoking trade retaliation.[451] The administrative agencies and executive-branch departments that regularly conduct international trade negotiations must be aware of such possibilities and conduct their business accordingly.

Consequently, this is an area in which the courts should proceed slowly, if at all. In general, the United States Supreme Court has recognized that foreign affairs are, both as a practical matter and as a constitutional matter, properly the provenance of Congress and the executive branch.[452] Sound policy suggests that the variety of U.S. interests involved in such patent enforcement should be weighed and considered by Congress, which created the patent quid pro quo bargain in the first place. Until Congress considers the competing interests in this area and reaches some resolution

449. *Id.* at 171.

450. *See* PETER ROBINSON, IT IMPERATIVES: COMPUTERS AND COMMUNICATIONS FOR THE 21ST CENTURY 107-09 (1990) (discussing several international telecommunications organizations); Ester Stevers & Christopher Wilkinson, *Appropriate Regulation for Communication and Information Services*, *in* ELECTRONIC HIGHWAYS, *supra* note 200, at 156, 179 (stating the inevitability of several international organizations in negotiations covering international telecommunications trade).

451. *See supra* note 432 and accompanying text.

452. *See, e.g.*, Goldwater v. Carter, 444 U.S. 996, 996 (1979) (dismissing a foreign relations dispute between the executive and legislative branches); *see also* Baker v. Carr, 369 U.S. 186, 211-13 (1962) (including matters of foreign affairs among nonjusticiable issues).

regarding the weight to be accorded each, the courts should exercise caution in crafting decisions which could hamper or stymie the efforts of the other branches of government enganged in negotiating the future development of international data exchange.

B. The Innocent Infringer

Application of U.S. patent law to the international data exchange environment also promises to create significant problems of "innocent infringement." As discussed above, the patent grant is extremely broad, and unintentional or unwitting infringement leads to liability.[453] However, there may be nothing that would put a network user on notice that he is infringing, and there may be nothing that he can do to avoid infringement.[454] In such a situation, simply signing on to the network may inevitably lead to liability. In order to avoid the level of control and benefit that constitutes infringing use on the network, a computer operator might choose the only safe level of activity—no activity at all. Computer users can be relatively certain that software on their own machines does not infringe some patent; however, the same software on any other machine may be suspect. Thus, liability for inadvertent or unintentional infringement could prove a significant deterrent to network use, prompting computer users to return to stand-alone computing and thereby diminishing the benefits of the network.[455]

On the other hand, a significant level of unintentional infringement will deny a patent holder the benefit of her patent just as surely as will intentional infringement. Moreover, the holder of a software patent may have difficulty in detecting or proving even intentional infringement in a system as convoluted, fluid, and ephemeral as that of a global data communications network. Unlike physical goods, which can often be interdicted at their point of entry, data travelling as electromagnetic impulses over copper wire, fiber optic cable, or through the air will be difficult to detect, let alone interdict.[456] Striking the proper balance between deter-

453. *See supra* note 304 and accompanying text.

454. *See supra* notes 302-04 and accompanying text.

455. The cost of lost benefits accrues not only to the user that chooses not to take advantage of the network and its services but, due to network externalities, also accrues incrementally to every network user—the fewer users on the network, the less it is worth to those users who remain. *See supra* notes 122-23 and accompanying text.

456. *See* Lynch, *supra* note 2, at 19.

rence of infringement and deterrence of beneficial research may be a perplexing exercise in this environment.

Similar concerns attended the enactment of the Process Patent Amendments discussed above.[457] The sponsors of this legislation were aware that, due to the foreign situs of the infringement contemplated by the legislation, patent holders would have significant problems in obtaining information about the origin of a product.[458] The introduced bills therefore addressed the discovery problems that might beset domestic patent holders attempting to prove use of an infringing process in another country; the burden of showing that a noninfringing process was used was shifted to the seller, who presumably stood in the best position to obtain such information.[459]

It was argued, however, that the proposed legislation entailed a significant possibility of harming certain domestic businesses, particularly retailers that might sell imported products unaware that the products were produced by an infringing process.[460] These potentially "innocent infringers" also feared that extended process patent protection might be used in bad faith to harass sellers of products legitimately produced by noninfringing processes outside of the United States.[461] Additionally, there was concern that unwitting purchasers of products produced by an infringing process could be found liable for infringement through use, thus extending a chain of liability downstream from the retailer.[462]

Retailers therefore vigorously opposed the bills as originally introduced and demanded safeguards against unfair use of such extended process patent protection.[463] In order for the legislation to pass Congress, compromises had to be made between the importers' and retailers' interests and those of patent holders.[464] Among the compromise provisions were limitations on the remedies available to patent holders against noncommercial or retail "users" of infringing products.[465] Special care was also taken to guard against injuring innocent sellers of infringing goods, while

457. *See supra* notes 264-78 and accompanying text.

458. S. REP. No. 83, 100th Cong., 1st Sess. 39 (1987).

459. *Id.*; *see also* Hall, *supra* note 264, at 346-47 (discussing Act's presumption that importer is in best position to determine product's origin).

460. S. REP. No. 83, at 42-43; *see also* Hall, *supra* note 264, at 345 (discussing concerns raised by retailers and generic drug industry).

461. S. REP. No. 83, at 43.

462. *See id.* at 48.

463. *See Process Patent Hearings*, *supra* note 278, at 64-77 (statement of David R. Haarz., Esq., National Retail Merchants Association).

464. *See id.* at 2; S. REP. No. 83, at 29.

465. S. REP. No. 83, at 48.

still requiring the sellers to make good faith efforts to determine the origin of the goods they purchased.[466]

The final version of the legislation, enacted as part of the Omnibus Trade and Competitiveness Act of 1988,[467] provided that patent holders could not sue the seller of infringing goods without providing notice of infringement.[468] Under the statute, patent holders must disclose the processes potentially infringed.[469] This requirement shifts the burden of proving good faith in raising the issue to the patent holder. The statute also creates a rebuttable presumption of infringement if there is a substantial likelihood of infringement and the patent holder has made reasonable efforts to show infringement.[470]

Thus, the Process Patent legislation, as finally enacted, constituted a carefully crafted compromise between the competing interests of patent holders and importers.[471] The clear purpose of this legislation calls into question its application in a rather different setting, that of global computer networks, where the balance of interests may be somewhat different. However, the history of the Process Patent Amendments at least indicates the type of competing interests that should be weighed by the courts, if not by Congress, in meeting this new challenge to the patent bargain.

C. *Temporary Presence*

Unless and until Congress weighs the benefits and burdens of patent enforcement in the context considered here, this task will fall to the courts. It therefore seems likely that the courts will be faced with initially determining how patent enforcement will proceed in the context of global computer networks. Congress tends to react slowly, if at all, to emerging problems; usually, it only acts in response to an impending crisis.[472] In the meantime, those problems will come relatively quickly to the attention of the judici-

466. *Id.* at 40-41; *see also* Hall, *supra* note 264, at 352.

467. Omnibus Trade and Competitiveness Act of 1988, Pub. L. No. 100-418, §§ 1342, 9001-9005, 102 Stat. 1107, 1212, 1563-66 (1988) (codified at 19 U.S.C. § 1337, 35 U.S.C. §§ 271, 287, 295 (1988)).

468. 35 U.S.C. § 287(b)(5) (1988). *See generally* Comment, *The Process Patent Amendments Act of 1988: Solving an Old Problem, but Creating New Ones*, 1989 B.Y.U. L. REV. 567 (discussing patent provisions of the Omnibus Trade and Competitiveness Act of 1988).

469. 35 U.S.C § 287(b)(5)(B) (1988).

470. *Id.* §§ 287(b)(5)(D), 295.

471. *See Process Patent Hearings*, *supra* note 278, at 2; S. REP. No. 83, at 29.

472. *See* Dan Rosen, *A Common Law for the Ages of Intellectual Property*, 38 U. MIAMI L. REV. 769, 795 (1984).

ary, which cannot simply put them on hold until better data is available.[473] Additionally, Congress has clearly placed enforcement of the patent law into the hands of the judiciary. Thus, in the absence of further legislative direction, the courts will have to decide how such enforcement will proceed.[474]

Consideration of fresh questions concerning patent enforcement will therefore require caution as suggested above[475] but may also require innovation to meet new situations. These requirements are not necessarily contradictory; indeed, the development of new legal doctrine may be essential to a cautious approach. As outlined in the sections above, the patent enforcement problems generated by international data exchange are rife with considerations that may not have been taken into account in the present patent law. Courts considering these matters for the first time will have to take such policy matters into account when determining the parameters of patent exclusivity and enforcement. The principle of *Deepsouth Packing* should form the bedrock provision for such consideration and the courts should make doctrinal forays from this principle only under extreme circumstances.

This would not be the first time that courts have modulated patent enforcement to the necessities of international commerce. For example, in *Brown v. Duchesne*,[476] the United States Supreme Court developed a judicially created exception to patent enforcement known as the "temporary presence" doctrine.[477] The *Brown* case was in some sense the reverse of the "floating island" jurisdictional cases discussed above;[478] at issue in *Brown* was the presence in an American port of a French seagoing vessel that carried a device conforming with French law but infringing an American patent.[479] Although the Court recognized that the vessel was within U.S. jurisdiction and that Congress had the power to extend the American patent law to the vessel, the Court refused to read the

473. *See* D.H. Kaye, *On Standards and Sociology*, 32 JURIMETRICS J. 535, 538 (1992).

474. *See in re* Sarkar, 588 F.2d 1330, 1333 (C.C.P.A. 1978) ("Congress cannot be expected to foresee, or to annually amend Title 35 to incorporate, every future breakthrough into an entirely new technological terrain.").

475. *See supra* notes 451-52 and accompanying text.

476. 60 U.S. (19 How.) 183 (1857).

477. *See id.* at 198-99; *see also* 4 CHISUM, *supra* note 220, § 16.05[4] (discussing temporary presence). Interestingly, the *Brown* case was one of the principal cases relied on by the Supreme Court in formulating the *Deepsouth Packing* doctrine on extraterritorial application of the patent laws. *See* Deepsouth Packing Co. v. Laitram Corp., 406 U.S. 518, 531 (1972), *reh'g denied*, 409 U.S. 902 (1972); *see also supra* notes 252-55 and accompanying text.

478. *See supra* notes 284-86 and accompanying text.

479. *Brown*, 60 U.S. (19 How.) at 193-94.

patent statutes literally to find that Congress had done so.[480] Rather, the Court carved out a public policy exception to the patent grant, finding that the prejudice to foreign relations that would result from enforcing the letter of the patent laws outweighed the slight damage that the patent holder would suffer from occasional and temporary entry into the United States of an infringing product.[481]

This view was later incorporated into treaties governing the international application of intellectual property law, including the Paris Convention and the Convention on International Civil Aviation.[482] In the United States, the doctrine was eventually codified as 35 U.S.C. § 272. In interpreting § 272, courts have held that even regular, repeated landings by aircraft carrying an otherwise infringing device are "temporary" and are not a basis for damages.[483]

The temporary presence doctrine represents judicial recognition that the balance struck in the quid pro quo patent bargain may be upset by international policy considerations, particularly when the harm to the patent holder is slight.[484] Courts that are asked to enforce patent rights infringed by international data communications will be required to engage in a similar calculus: the patent incentive created by Congress must not be eroded, but at the same time, mechanical application of its provisions cannot be allowed to compromise important international goals. Systematic, substantial inroads into a patent holder's exclusivity by, for instance, an offshore data haven, are likely to render the patent worthless and must be discouraged. Particularly when such activity by data service providers or subscribers knowingly encroaches on the patent, imposition of liability for direct infringement and inducement would be appropriate. By contrast, when computer network activity occasionally and unwittingly impinges on the scope of a U.S. patent, the burdens on the U.S. international position imposed on society by judicial enforcement of the patent may exceed the value of the patent incentive.

---

480. *See id.* at 195-96; *see also* 4 CHISUM, *supra* note 220, § 16.05[4], at 16-68.8 to 16-72 (discussing the *Brown* holding).

481. *See Brown*, 60 U.S. (19 How.) at 195-96.

482. *See* Convention on International Civil Aviation, Dec. 7, 1944, art. 27, 61 Stat. 1180, 1187-88, T.I.A.S. No. 1591; Industrial Property Convention, Nov. 6, 1925, art. 5 TER, 47 Stat. 1789, 1801-02, T.S. No. 834.

483. *See* Cali v. Japan Airlines, 380 F. Supp. 1120, 1127 (E.D.N.Y. 1974), *aff'd unpublished op.*, 535 F.2d 1240 (2d Cir. 1975).

484. *Cf. supra* notes 206-15 and accompanying text.

V. CONCLUSION

The anomalies of patent enforcement explored in this Article are perhaps the inevitable product of our present concepts of nationality and territory. One commentator has observed that "separate patent systems for each country of the world is a necessary evil at best since technology by its very nature flows easily to wherever it may be effectively utilized."[485] Global computer networks enhance that flow and, by weakening the concept of territoriality, may hasten the time when the evil of separate patent systems will no longer be necessary. Until that presumably far-off day, however, our present legal construct must begin to adapt to the realities of enforcing patents in cyberspace.

485. *See 1985 Patents in Space Hearings*, *supra* note 361, at 18 (statement of Professor Donald S. Chisum, Univ. of Washington).