1996

Governing Networks and Rule-Making in Cyberspace

Joel R. Reidenberg
Fordham University School of Law, JREIDENBERG@law.fordham.edu

GOVERNING NETWORKS AND RULE-MAKING IN CYBERSPACE

*Joel R. Reidenberg**

 Associate Professor, Fordham University School of Law. A.B., Dartmouth 1983; J.D., Columbia 1986; D.E.A. droit int'l éco., Univ. de Paris I (Panthéon-Sorbonne) 1987. This Article was presented at the 1996 Randolph W. Thrower Symposium on Legal Issues in Cyberspace at Emory Law School and benefited from comments raised at the conference. The author would also like to thank Brian Kahin and the participants at the John F. Kennedy School of Government/Harvard Law School joint conference on "Information, National Policy and the International Infrastructure" (Jan. 28-30, 1996) for their discussion of an earlier draft and to express appreciation to Mark A. Lemley and Paul M. Schwartz for comments on an earlier draft. Any errors or inaccuracies remain the fault of the author.

I. INTRODUCTION

The information infrastructure has significant implications for the governance of an information society. Despite the popular perception, the global information infrastructure ("GII") is not a lawless place. Rather, it poses a fundamental challenge for effective leadership and governance. Laws, regulations, and standards can, do, and will affect infrastructure development and the behavior of GII participants. Rules and rule-making do exist. However, the identities of the rule-makers and the instruments used to establish rules will not conform to classic patterns of regulation.

The global network environment defies traditional regulatory theories and policymaking practices. At present, policymakers and private sector organizations are searching for appropriate regulatory strategies to encourage and channel the GII.[1] Most attempts to define new rules for the development of the GII rely on disintegrating concepts of territory and sector, while ignoring the new network and technological borders that transcend national boundaries.[2] The GII creates new models and sources for rules. Policy leadership requires a fresh approach to the governance of global networks. Instead of foundering on old concepts, the GII requires a new paradigm for governance that recognizes the complexity of networks, builds constructive relationships among the various participants (including governments, systems operators, information providers, and citizens), and promotes incentives for the attainment of various public policy objectives in the private sector.

---

[1] *See, e.g.*, Chair's Conclusions, G-7 Ministerial Conference on the Information Society, Brussels (Feb. 25-26, 1995) <http://www.ispo.cec.be/g7/keydocs/G7en.html>.

[2] *See, e.g.*, INFO. INFRASTRUCTURE TASK FORCE, REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE (1995) (<http://www.uspto.gov/niiip.html>) [hereinafter NII WHITE PAPER]. Various equivalent foreign reports from Canada, the European Union, and Japan tend to focus similarly on changes to national laws and the applicability in specified territories of "information society" rights. *See, e.g.*, <http://www.ic.gc.ca/ic-data/info-highway/general/report.april94.e.txt> (Canadian report); <http://www2.echo.lu/other/national.htm/> (EU country reports); <http://www.mpt.go.jp/Report/unofficial.html> (unofficial translation of Japanese report with references only to national monopolies).

II. THE DISINTEGRATION OF TRADITIONAL SOVEREIGNTY PARADIGMS

Global communications networks challenge the way economic and social interactions are regulated. In the past, legal rules usually governed behavior in distinct subject areas for defined territories. These national and substantive borders formed the sovereignty paradigms for regulatory authority and decision-making. For example, intellectual property rights and privacy rights—each critical for the ordering of an information society—have been designed as distinct bodies of law. Copyright, patent, trademark, and trade secret law protect specific attributes of information and its economic value, while privacy law guards specific information about individuals from particular harms. Customarily, such distinct rules applied only in the rule-maker's geographically defined territory.[3] Few "transnational rights" in the economic and social sphere truly exist; international treaties and regional obligations typically establish some degree of harmonized, national standards instead of a single, unique "global" right.[4] With the GII, however, territorial borders and substantive borders disintegrate as key paradigms for regulatory governance.

A. Permeable National Borders

For centuries, regulatory authority derived from the physical proximity of political, social, and economic communities. International law grants legitimacy to a governing authority if it exercises sovereignty over a physical territory and its people.[5] Constitutional governance predicates sovereignty on the existence of geographically distinct political and social units.[6]

---

[3] *See, e.g.*, Paris Convention for the Protection of Industrial Property, Mar. 20, 1883, *as last revised*, July 14, 1967, 21 U.S.T. 1583, 828 U.N.T.S. 305; Berne Convention for the Protection of Literary and Artistic Works, Sept. 9, 1886, *as last revised*, July 1, 1967, 828 U.N.T.S. 221; ROBERT A. GORMAN & JANE C. GINSBURG, COPYRIGHT FOR THE NINETIES 873-901 (4th ed., 1993).

[4] *See, e.g.*, Final Act and Agreement Establishing the World Trade Organization, Apr. 15, 1994, Annex 1C, 33 I.L.M. 1197 (<http://itl.irv.uit.no/trade_law/documents/freetrade/wta-94/art/ii.html>). Organization for Economic Cooperation and Development: Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Oct. 1, 1980, 20 I.L.M. 422; Council of Europe: Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, 20 I.L.M. 317 (<http://www2.echo.lu/legal/en/dataprot/counceur/conv.html>).

[5] *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 201 (1987).

[6] *See, e.g.*, U.S. CONST. amend. IX. Even in nondemocratic states, sovereignty was internally equated with distinct territorial borders. *See* JOHN N. HAZARD ET AL., THE SOVIET LEGAL SYSTEM: THE LAW IN THE 1980s 14-17, 25-29 (1984).

Regulatory power has always been defined in terms of national borders. Key rights establishing the structure of an information society, such as intellectual property protections, fair information practice standards, and competition rules, are all territorially based.[7] The adjudication of disputes also typically depends on territorially-empowered courts. Similarly, police powers to enforce regulatory policies and decisions through property seizures or incarceration are territorially restricted.

Transnational information flows on the GII undermine these foundational borders and erode state sovereignty over regulatory policy and enforcement. Geographic limits have diminishing value. Physical borders become transparent and foreign legal systems have local relevance. Network activities may make participants subject to legal rules of distant jurisdictions. Political and economic communities based predominantly on geographic proximity and physical contact have less relevance in cyberspace because network communities can replace physically proximate communities. Political discourse can ignore national borders, while affinities and affiliations transcend distances and human contact. Internet "listservs"[8] and "usenet groups"[9] involve participants from around the world communicating directly with each other on topics of mutual interest. Economic relationships need no physical situs. With electronic cash and new means of electronic stored value, such as those developed by Cybercash and Mondex, Internet transactions may take place entirely on the network without the physical delivery of goods or services and without resort to any national payment system. Even social relationships now evolve in the absence of physical contact. On-line chat rooms provide live, but remote, contact, and cybersex offers the very intimate, albeit electronic, relationships.[10]

---

[7] *See, e.g.*, PAUL B. STEPHAN III ET AL., INTERNATIONAL BUSINESS AND ECONOMICS: LAW AND POLICY 397-405, 420-21 (1993).

[8] A listserv is a feature of electronic mail software that automatically distributes messages to subscribers of a specified list. To participate, a computer user sends a subscription message to the host computer. Once the host computer accepts the subscriber, the person may post messages to all participants on the list by sending a single e-mail to the host. Depending on the type of list, each single, incoming message may automatically be copied to all members on the list, whether the list has 10 or 10,000 members, or may be copied to all members on the list only after screening by a list moderator.

[9] Usenet groups allow computer users to post messages on a bulletin board at a host site. Access to the bulletin board is unrestricted.

[10] For an illustrative experience, adult-oriented chat rooms may be found on the Internet at <http://chat.bianca.com/cgi-bin/displaychat/shack/quickref.html>. *See also* Anastasia Toufexis, *Romancing the Computer*, TIME, Feb. 19, 1996, at 53 (reporting on cyber-romances and the filing of a divorce petition in New Jersey because of a spouse's alleged "on-line" affair).

The permeability of national borders destabilizes territorial rights. Inevitably, differences will exist among various key national rights in an information society. The scope, for instance, of intellectual property rights is not uniform across state lines.[11] Even the mechanisms by which countries may assure rights such as privacy may vary significantly.[12] Yet the GII creates simultaneous "global" rightholders. A given activity may be subject to differing rights at the same time, such as trademark or antitrust protections, because the activity transcends the borders of any single nation. This by itself imposes conflict. In addition, the temptations to apply national laws and standards extraterritorially further compound the legal uncertainty. The patent law of the United States, for example, has extended to restrict foreign activities that were legal where conducted,[13] while the new data protection directive of the European Union requires the evaluation of foreign data processing standards.[14] Nevertheless, the erosion of national borders places an important degree of network activity beyond the physical grasp of state authorities, although states may still force individuals or corporations within their borders to behave in particular ways. This enforcement problem challenges the uniformity of any right.

B. Ambiguous Substantive Borders

Beyond the disintegration of territorial borders, the GII also undermines substantive legal sovereignty. Governance has relied historically on clear distinctions and borders in substantive law. For example, telecommunications law has been distinct from financial services law, and intellectual property law has been distinct from privacy law. Similarly, the borders of protection within any particular field were usually well defined. A "common carrier" had a set of regulations quite apart from those of a "cable" provider[15] or broadcaster.

---

[11] *See, e.g.*, Symposium, *Fordham Conference on International Intellectual Property Law and Policy*, 4 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1 (1993).

[12] *See* Joel R. Reidenberg, *The Privacy Obstacle Course: Hurdling Barriers to Transnational Financial Services*, 60 FORDHAM L. REV. S 137 (1992); Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471 (1995).

[13] *See* 35 U.S.C. § 271(g) (1994) (extending the scope of U.S. process patent protection to prevent the importation of legally manufactured foreign products).

[14] *See* Directive 95/46 of the Eur. Parliament and of the Council, arts. 25-26, 1995 O.J. (L 281) 31, 45-46 [hereinafter Privacy Directive].

[15] *See* ROBERT R. BRUCE ET AL., FROM TELECOMMUNICATIONS TO ELECTRONIC SERVICES 153-68 (1986).

The GII obscures these substantive boundaries; critical substantive rights become muddled. The new technological abilities of a telephone company to offer "video" dial tone and a cable company to propose voice communications undercut the well-defined borders of communications law. The digital environment challenges the applicability of basic information society rights, such as copyright, as well as the boundaries among other intellectual property rights. Designers of information products can, to a certain extent, package their works to pick and choose legal protection. Processing instructions can, for example, be embedded in a semiconductor chip to benefit from sui generis legal protection,[16] stored on a floppy disk to be covered under copyright,[17] or incorporated in a device to obtain patent protection.[18] This substantive blurring of rights creates significant uncertainty; the degree and scope of protection become variable.

In addition, network interactions defy clear disciplinary categorization. The regulation of an information transfer or transaction can easily cross sectoral lines. For example, a packet of information may contain electronic cash or payment instructions, along with digitally reconstructed images of an individual. In such a case, the legal interests cross many sectoral lines, including telecommunications, financial services, intellectual property, and privacy. Even pure information processing activity may cross sectoral lines. For example, a third party may process transaction information for a retail chain that includes netting of payments. In one sense, this activity is unregulated information processing; yet in another sense it is a banking activity and might be subject to bank safety and soundness requirements.

More significantly, digitalization and the information infrastructure enable the objectives of one distinct body of law, such as privacy, to be achieved by application of the rules of another field of law, such as intellectual property. Secondary use of personal data, for example, is a core issue for information privacy law, but in the multimedia context, copyright law can also regulate the manipulation of data relating to individuals.[19] In essence, functional activity is more relevant than sectoral legal boundaries.

---

[16] *See* 17 U.S.C. §§ 901-914 (1994).

[17] *See* §§ 101-102, 106, 117.

[18] *See* 35 U.S.C. §§ 1-376 (1994).

[19] *See* Joel R. Reidenberg, *Multimedia as a New Challenge and Opportunity in Privacy: The Examples of Sound and Image Processing*, 22 Materialien zum Datenschutz 9 (1995).

III. THE EMERGENCE OF NETWORK SOVEREIGNTY

Just as traditional foundations for governance are breaking down, new boundaries are emerging on the GII. The infrastructure itself contains visible borders. Network borders replace national borders. Network service providers, as well as the infrastructure architecture, each establish rules of participation for defined network areas. These rules form visible borders on the GII. In addition to these visible borders, network communities also develop distinct sovereign powers. Thus, infrastructure organizations acquire attributes of the traditional territorial sovereigns.

A. Visible Network Borders

The demarcation lines among network service providers such as America OnLine, CompuServe, EUNet, or Prodigy create important boundaries. Private contractual arrangements determine the availability and the conditions of access for network connections. These contractual arrangements define distinct borders among various service providers. Participants on the GII will be subject to different contractual rules, benefit from different resources, and adhere to different pricing plans, according to network service agreements.[20] In essence, the reach of a service provider's network establishes an important boundary line in an information society.

Network architecture also creates a significant type of border. System design imposes rules of order on an information society. Technical choices are policy decisions that have inherent consequences for network participants. For example, integrated services digital network (ISDN) technology and the World Wide Web transmission protocol offer superior interactive capabilities and choices when compared to analog technology and simple file transfer protocols. Gateways between different systems or between a proprietary network like America OnLine and the Internet establish fundamental rules of conduct; without a gateway, interactions are effectively prohibited. In effect, technical standards exert substantial control over information flows.[21] The degree of system interoperability thus determines the

---

[20] *See* Robert L. Dunne, *Deterring Unauthorized Access to Computers: Controlling Behavior in Cyberspace Through a Contract Law Paradigm*, 35 JURIMETRICS J. 1 (1994) (arguing for model contracts).

[21] *See, e.g.*, Mark A. Lemley, *Shrinkwraps in Cyberspace*, 35 JURIMETRICS J. 311, 322 (1995) (arguing for technical self-help as an alternative to model contracts).

openness of the information society and determines whether network architectural "borders" can be crossed.

Technical standards set default boundary rules in the network that tend to empower selected participants. For example, transmission protocols can embed rules of control on the use of personal information collected by the network. World Wide Web browsers such as Netscape record transaction data on Internet users' hard drives and make the information available to host sites.[22] The JavaScript in Netscape similarly allows Web sites to collect real-time data on visitors' activities and to examine the directory of a visitor's hard drive.[23] These designs set as a default rule the empowerment of Web sites. Yet, at least in the case of Netscape, the software allows savvy users to override the recording feature.[24] Other protocols tend to enable producer choice in the use of intellectual property.[25] For example, copy protection techniques for digital audio tapes assist producers to control the reproduction of perfect digital copies.[26] Electronic rights management protocols are emerging to enable on-line protection of intellectual property.[27]

These visible network borders arise from complex rule-making processes. Technical standardization may be the result of a purely market-driven process or alternatively may be adopted through a standards body. The classic example of a market-promulgated standard is the QWERTY keyboard. Once the now famous keyboard configuration became popular, public acceptance

---

[22] Netscape creates a log file (usually named <cookies.txt>) in the program directory that allows Web sites to record the pages viewed by the user. The Web site may access this data from the user's personal computer when the user revisits the site. *See* Cookies Technical Specifications <http://home.netscape.com/newsref/std/cookie_spec.html>.

[23] *See* John Robert LoVerso, Netscape Navigator 2.0 Exposes User's Browsing History, RISKS DIGEST, Feb. 23, 1996 <http://catless.ncl.ac.uk/Risks/17.79html> (describing bug that allows collection of real-time data); John Robert LoVerso, Report of Netscape 2.01 JavaScript Problems <http://www.osf.org/~loverso/javascript/www-sec-Mar22.html> (describing ability to browse a user's directory).

[24] Users concerned about their privacy may disable the feature by changing the attributes of the <cookies.txt> file to a read-only file.

[25] *See, e.g.*, Peter H. Lewis, *Microsoft Backs Ratings System for the Internet*, N.Y. TIMES, Mar. 1, 1996, at D1.

[26] *See* Julie E. Cohen, *Reverse Engineering and the Rise of Electronic Vigilantism: Intellectual Property Implications of "Lock Out" Programs*, 68 SO. CAL. L. REV. 1091 (1995); Pamela Samuelson, Technological Protection for Copyrighted Works, Paper presented at the Randolph W. Thrower Symposium on Legal Issues in Cyberspace at Emory Law School (Feb. 22, 1996) (on file with the author).

[27] *See* U.S. CONGRESS OFFICE OF TECHNOLOGY ASSESSMENT, INFORMATION SECURITY AND PRIVACY IN NETWORK ENVIRONMENTS 110 (1994) [hereinafter INFORMATION SECURITY]; Interactive Media Ass'n, IP Requirements Forum: Electronic Commerce for Content <http://www.ima.org/forums/ip/ip_meet.html>.

of other, more user-friendly configurations was unlikely. In contrast, standards bodies seek to identify and recommend technical specifications for particular network needs such as security. Standards bodies range from industry groups to combined industry/government organizations. These organizations, such as the American National Standards Institute (ANSI) and the International Organization for Standards (ISO), play a critical role in the development and promotion of technical standards. In essence, these organizations assure and reinforce the contours of network borders.

B. Powerful Network Communities

In addition to the new "geography" of borders, networks may now even supplant substantive, national regulation with their own rules of citizenship and participation.[28] Networks themselves take on political characteristics as self-governing entities. Networks determine the rules and conditions of membership. Private contracts mediate the rights and responsibilities of participants.[29] Service providers offer different terms of adherence. America OnLine and Prodigy, for example, have varying policies on user privacy,[30] while Counsel Connect's message-posting rules for lawyers differ from those for law students.[31] Discussion groups on the Internet have their own rules of access and participation. Usenet groups are open to all, while listserv groups are available only to subscribers authorized by the list owner according to some criteria, such as knowledge of a particular field, although a list owner may open the list to anyone without restriction.

Networks also determine the rules of participant behavior. This characteristic can result in rules that reverse established territorial laws. For example, by means of private contract with network participants, Counsel Connect reversed, in effect, the traditional copyright allocation of rights of authorship for bulletin board message postings.[32] Alternatively, network conduct rules

---

[28] *See* David Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 49 STAN. L. REV. (forthcoming 1996).

[29] Networks have the rule-making capability of private associations. *See* I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. PITT. L. REV. 993, 1028-32 (1994).

[30] *Compare* "Prodigy Service Agreement" §§ 6-7 *with* "America Online's 'Rules of the Road'" § 7c (<www.cdt.org/privacy/online_services/chart.html>).

[31] For example, the Law Schools Online service allows law students to "listen in on one of LCC's 350 discussion groups as practicing lawyers, judges and law professors discuss law as it's really practiced." Lexis-Nexis Law Schools Online, version Win 3.1 (1996).

[32] *See* Hardy, *supra* note 29, at 1031.

may be sui generis. Microsoft, for example, is endorsing a ratings system for information distributed on the World Wide Web to allow voluntary screening of material inappropriate for children.[33] In contrast, CompuServe and Netcom each initially chose to exclude all participants worldwide from various Internet discussion groups because of an inquiry by a German provincial state prosecutor into the availability of pornographic content and the fear of potential criminal liability. These on-line services could have tailored more narrowly the restrictions, if in fact they would have incurred German liability for use of their networks within Germany. For the nonproprietary Internet, an entire body of customary rules of behavior has even been formulated as "netiquette."[34]

Like nation-states, network communities have significant powers to enforce rules of participant conduct. In the case of proprietary networks such as America OnLine or CompuServe, service providers may terminate access for offending participants. Netiquette rules for the Internet may even be enforced through the use of technologies by individual members of the network community. For example, the Internet has the equivalent of self-appointed policemen and policymakers. "Spamming," the sending of unsolicited messages, results in "cancelbots," programs that delete messages circulating on the Internet from offending senders. Even the Guardian Angels have begun to patrol the Net with their "CyberAngels" to look for crime and safety problem areas.[35] Similarly, "technologies of justice" will regulate and enforce behavioral standards or expectations.[36] For example, software developers have created filters for the World Wide Web protocol to allow network participants to mask commercial advertisements while viewing Web sites. Even collective efforts in adjudication of disputes are likewise emerging in the network community. There is at least one mechanism, the Virtual Magistrate, for on-line dispute settlement with network-based tribunals of experts.[37]

---

[33] *See* Lewis, *supra* note 25, at D1.

[34] An Internet guide to netiquette is available at <ftp://ds.internic.net/rfc/rfc1855.txt>.

[35] *See* <http://proxis.com/~safetyed/cyberangels/cyberangels05.html>.

[36] *See* Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869 (1996).

[37] The Virtual Magistrate Project was launched in March 1996 to "assist in the rapid, initial resolution of computer network disputes" by a pool of on-line neutral arbitrators. The project is based on the Internet at <http://vmag.law.vill.edu:8080/>. The National Center for Automated Information Research, a prominent nonprofit foundation, is similarly supporting work exploring on-line dispute mediation and held an invitational meeting, "The On-Line Dispute Resolution Conference," in May 1996.

IV. THE INCONGRUITY OF TRADITIONAL REGULATORY POLICYMAKING

When faced with these new dimensions of network governance, existing regulatory approaches are incongruous and ill-situated to resolve the challenges of the network environment. Despite the fundamental impact of the GII on governance, U.S. regulation and the American policy decision-making process remain wedded to the traditional paradigms of distinct legal fields and territorial borders. The U.S. approach to regulation and its philosophical preference for narrowly targeted law obscure the dramatic evolution of the information society. At the same time, European regulation similarly anchors rules in territorial and substantive jurisdictional areas, although it tends to favor proactive government intervention. These differing approaches offer a contrasting set of difficulties arising from the problems governments have in coping with the speed and magnitude of change in this area.

A. Obscured Vision

The U.S. approach to regulatory policy gives decision-makers an obscured vision of the new structural boundaries on the GII. The American legal tradition eschews a powerful state role in society and draws on a deep-seated philosophy of limited government.[38] The constitutional structure itself, by emphasizing a citizen's rights against the state, expresses a commitment to limits on state power. Even in the wake of increases in government regulation following the New Deal and Progressive Eras, U.S. law-making rhetoric remained hostile toward the regulation of industry.[39] Whether the boundary is between the federal and state governments or between legal disciplines, legal standards evolve primarily in response to discrete identified problems or crises, and jurisdictional lines are vitally important.

In the area of information policy, the U.S. approach has a distinct preference for self-regulation in the private sector. For example, important fair

---

[38] *See* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497 (1995).

[39] *See* Morton J. Horwitz, *The History of the Public/Private Distinction*, 130 U. PA. L. REV. 1423, 1426 (1982).

information practice standards are not typically found in legislation, but rather are determined by company activities.[40] Legal rules tend to be narrowly drawn, as for example, the strong protections for video rental records[41] and the scant protections for health care records,[42] or they purport to seek only minor adjustments to existing regimes, such as the National Information Infrastructure Task Force work on intellectual property rights.[43] Over the last decade, intellectual property laws and information privacy rules have evolved only modestly, as compared to the dramatic evolution of information technology. Perhaps the most significant legal response to the GII thus far has been the arduous process of telecommunications reform.[44] Despite the de facto restructuring of communications industries, fragmented policymaking in Congress had extraordinary difficulty dealing with the complexity of both the change in information technology and special interests. The resulting law is a striking display of well-funded special interest lobbying.[45] Congress did not even try to deal with many of the intertwined issues of privacy and intellectual property.

The consequence of the U.S. approach is that policymaking for global information flows is widely dispersed and ill equipped to face the governance challenges.[46] Under the U.S. system, no single government organization is in a position to assess the redefinitions of traditional regulatory borders. Multiple federal agencies, including the State Department, the United States Trade Representative, the Federal Communications Commission, the Commerce Department's National Telecommunications and Information Administration, and the National Institute for Standards and Technology, each have narrow and overlapping claims to various discrete aspects of information policy. Regulators then compete with one another for jurisdictional power. The National Telecommunications and Information Administration, the Federal Trade Commission, and the Federal Communications

---

[40] *See* Reidenberg, *supra* note 38, at 508-11.

[41] 18 U.S.C. § 2710 (1994).

[42] *See* Paul M. Schwartz, *The Protection of Privacy in Health Care Reform,* 48 VAND. L. REV. 295 (1995).

[43] *See* NII WHITE PAPER, *supra* note 2. However, these adjustments are not truly "minor."

[44] This two-year process resulted in the Telecommunications Act of 1996. Telecommunications Act of 1996, Pub. L. No. 104-104, 1996 U.S.C.C.A.N., 110 Stat. 56.

[45] *See id.*; *Telecom Bill Rated One of Top Sweetheart Deals in 1995*, WASH. TELECOM. NEWS, Jan. 8, 1996.

[46] *See, e.g.,* THE NEW INFORMATION INFRASTRUCTURE: STRATEGIES FOR U.S. POLICY (William J. Drake ed., 1995).

Commission have each, for example, tried to stake out claims to privacy issues.[47] The significance of the paradigmatic shift in borders becomes lost in the bureaucratic maze. For example, government agencies do not generally have the combination of technical skills and public policy mandates to examine the impact of choices in technological standards on regulatory policy or objectives. No agency has a complete perspective on the structural changes taking place in society as a result of the GII. Even the Clinton Administration's present effort to develop a vision for the information infrastructure and its governance through the work of the Information Infrastructure Task Force (IITF) remains captive to sectoral thinking and reactive tendencies. The study groups are divided along sectoral lines and some of the most time-consuming projects, like privacy and intellectual property, remain focused on territorial borders and the transposition of status quo interests to cyberspace. In addition, the subcommittee groups compete with one another for recognition. For privacy alone, the U.S. Advisory Council (expert advisors to the IITF), the Working Group on Privacy, the Government Services Group, and the Security Issues Forum have each issued separate policy statements.

Although the GII has its origins in the United States, the U.S. regulatory policy process is beginning to appear as a serious impediment to effective leadership. The incongruity of American regulatory practices with the GII's multidisciplinary character and rapid technological pace seems to enshrine significant inefficiency and narrowness in the development of GII policies. The United States can no longer assume that its legal and policy standards will dominate the GII merely by the strength of the American market. In the case of information privacy, the European Union has already set the global agenda with its 1995 data protection directive. The United States, like other countries, must develop new governance paradigms that encompass the shifting borders of the GII.

---

[47] *See, e.g.*, U.S. DEPT. OF COMMERCE, NAT'L TELECOMMUNICATIONS & INFO. ADMIN., PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION (1995); Calling Number Identification Service—Caller ID, 60 Fed. Reg. 29,489 (1995) (to be codified at 47 C.F.R. §§ 64.1600-64.1604); Fed. Trade Comm'n Workshop: Consumer Protection and the Global Information Infrastructure (Apr. 10-11, 1995) <http://www.ftc.gov/opp/gii.htm>. The Federal Trade Commission also runs a privacy discussion listserv on the Internet at <http://www.ftc.gov/ftc/privacy.htm>.

B. Overloaded Vision

By contrast to the American experience, other regulators outside the United States confront the GII from comprehensive vantage points. In Europe, unlike the United States, comprehensive government regulation is not anathema to society.[48] For example, European policymaking often comes from centralized institutions, such as the independent "data protection agencies," which play an important role in the formulation of information policy, with mandates that attach to information flows rather than narrow sectoral regulations.[49] Omnibus rules such as data protection legislation[50] and sui generis laws, such as relatively new intellectual property rights,[51] present far-reaching views on information policy rather than ad hoc solutions to narrow problems. Central government agencies with comprehensive powers institutionalize broad policy planning and issue debates. The European Union, for example, has established an Information Society Project Office to coordinate a number of wide-ranging European Commission activities. Yet at the same time, an omnibus view cannot possibly address the full scope of issues simultaneously confronting the GII. As an illustration of this crucial problem, the European Commission had to narrow the range of issues addressed in its recent Green Paper on copyright.[52]

Although the omnibus approach to regulation may offer a broader vision for public policy in a global network environment than the U.S. approach, the vision inherent in European efforts still tends to preserve important, yet evaporating, foundations, based on territorial principles and subject matter distinctions. National application remains pre-eminent. The principle of "subsidiarity" in European Community law reflects this continued commit-

---

[48] *See* MARY ANN GLENDON, RIGHTS TALK: THE IMPOVERISHMENT OF POLITICAL DISCOURSE 1-17 (1991) (observing differences in the political culture of "rights" between the United States and European societies).

[49] *See* Privacy Directive, *supra* note 14, at arts. 1, 28.

[50] *See* Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445 (1995).

[51] *See* Council Directive 91/250/EEC on the Legal Protection of Computer Programs, 1991 O.J. (L 122) 42 (requiring European Community member states to adopt a special set of rules for the copyright protection of computer software). Previously, France, when faced with the problem of software protection, added an essentially sui generis protection into the French copyright law. *See* Loi No. 85-660, 1985 A.L.D. 357.

[52] *See* European Comm'n, Green Paper on Copyright and Related Rights in the Information Society, *reprinted in* 43 J. COPYRIGHT SOC'Y 50, 55 (1995) (noting that the Green Paper addresses only a subset of intellectual property issues for the information society).

ment to territorial and sectoral boundaries.[53] Under "subsidiarity," the European Community may only act on matters that are not more properly within the boundaries of member-state competence. When actions are taken at the European level through "Directives," each European member state must enact conforming national rights that implement the legal standards defined in the relevant Directive; Directives do not in themselves create supranational rights that can be invoked directly by citizens.

The broad approach also illustrates the problems of omnibus control. No matter how an omnibus regulatory policy is decided, the extraterritorial impact foreshadows difficulties. Under the European data protection rules, for example, personal information may not be transferred outside the European Union unless adequate privacy protections exist at the destination.[54] The very omnibus character of European rules makes appropriate comparisons to other legal systems, like that of the United States, complex.[55] Similarly, reciprocity provisions in intellectual property rules offer disparate treatment depending on the type of available foreign protections.

In the rapidly developing GII, the institutionalized vigilance for information flows that follows from an omnibus approach risks becoming rigid. The very process of adopting and implementing a European Directive is slow. For example, the first draft of the data privacy directive was released in 1990, the final text was adopted in 1995, and member state implementation need not be completed before 1998. By the time standards are implemented in national legislation, certain rules may be obsolete due to the rapid pace of technological development. Similarly, bureaucratic processes do not lend themselves well to rapidly changing technologies. The information system registration schemes common in some European countries over the last twenty years frequently relied on concepts such as "data files." While this made sense initially, techniques for the storage of personal information in an age of distributed databases no longer associate data with particular identifiable locations.

---

[53] Maastricht Treaty on European Union, 1992 O.J. (C 224) 1 (Feb. 7, 1992). *See* GEORGE A. BERMANN ET AL., CASES AND MATERIALS ON EUROPEAN COMMUNITY LAW, 1995 Supp., 11-14 (1995); George A. Bermann, *Taking Subsidiarity Seriously: Federalism in the European Community and the United States*, 94 COLUM. L. REV. 331 (1994).

[54] *See* Privacy Directive, *supra* note 14, at art. 25.

[55] *See* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION (1996).

Because the omnibus approach encourages extensive and customarily slow deliberation, regulatory policies risk network circumvention. If participants structure their network activities to avoid a jurisdiction, the omnibus approach makes a government response difficult and enforcement uncertain.

V. A NETWORK GOVERANCE PARADIGM

The development of a new model for governing networks is crucial for effective policy leadership on the GII. The new paradigm must recognize all dimensions of network regulatory power. As a complex mix of rule-makers emerges to replace the simple, state sovereign model, new policy instruments must appear that are capable of establishing important norms of conduct for networks. Policymakers must begin to recognize network sovereignty and begin to shift the regulatory role of states toward indirect means that develop network rules.

A. Complex Mix of Rule-Makers

On the GII, governance can no longer be viewed as an exercise in state edict. The relationships among the different participants in the information infrastructure become interactive. States have direct interests in the development of an information society. The private sector has a crucial role in the creation of the GII. Technologists have a pivotal position for policy choices and the GII empowers citizens to establish rules of their own. Policymaking among these different interest centers is intertwined. For example, technological choices may frustrate or support state interests or citizen goals. Overlapping jurisdiction and the rapid evolution of information technology defy the traditional forms of state control.

For global networks, governance should be seen as a complex mix of state, business, technical, and citizen forces. Rules for network behavior will come from each of these interest centers. Within this framework, the private sector must be a driving force in the development of the information society and governments must be involved to protect public interests. At the same time, policymaking cannot ignore technological concerns and technologically-driven decision-making.

B. *New Policy Instruments*

The recognition of new network borders opens new instruments for the achievement of regulatory objectives. Executive and legislative fora lose a degree of relevance to technical standards organizations. Standards decisions affect fundamental public concerns and are no longer technical rules of purely commercial interest. Standards now contain significant policy rules. The availability of "clickstream," or keystroke, data such as those contained in the Netscape file <cookies.txt> is, for example, a default policy rule.[56] The debate over encryption standards and key escrow mechanisms similarly reflects the critical new instrumentality of standards-setting.[57]

In the network governance paradigm, standards bodies will not be able to avoid robust public policy debates. Already, the Canadian Standards Association has tried to incorporate policy debate through the promulgation of a privacy standard,[58] and other national government agencies are encouraging technical decision-makers to implement policy objectives.[59] This recognition will change the process of making decisions at standards organizations. At present, citizen interests are either weakly or indirectly represented in setting standards. For example, the American National Standards Institute ("ANSI") is an umbrella organization in the United States that has prepared a framework for identifying requirements for national information infrastructure standards.[60] The Information Infrastructure Standards Panel only indirectly considers user needs through the standards developers and technology vendors.[61] Governments can and should seek standards that facilitate or incorporate broader policy objectives. Without a widening of the policy concerns inherent in technical standards, the results may be distorted. For instance, standards of electronic rights management for intellectual

---

[56] *See supra* note 22.

[57] *See* INFORMATION SECURITY, *supra* note 27, at 111-34; U.S. CONGRESS, OFFICE OF TECH. ASSESSMENT, ISSUES UPDATE ON INFORMATION SECURITY AND PRIVACY IN NETWORK ENVIRONMENTS 1-34 (1995); Joel R. Reidenberg & Françoise Gamet-Pol, *The Fundamental Role of Privacy and Confidence in the Network*, 30 WAKE FOREST L. REV. 105, 109 (1995).

[58] *See* CANADIAN STANDARDS ASS'N, MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION (1996).

[59] *See* INFORMATION & PRIVACY COMM'R OF ONTARIO, CANADA & REGISTRATIEKAMER OF THE NETHERLANDS, PRIVACY ENHANCING TECHNOLOGIES: THE PATH TO ANONYMITY (1995).

[60] *See* ANSI, Framework for Identifying Requirements for Standards for the National Information Infrastructure, Apr. 11, 1995 (visited Mar. 15, 1996) <http://www.ansi.org/iisp/fram4nii.html>.

[61] *Id.* ¶ 1.

property may transgress policy goals for fair information practices if the technical decisions do not consider the privacy implications. The Canadian experience and growing government interest in technologies of privacy, including encryption, are beginning to force this broader consideration at standards bodies.

Nevertheless, the practicality and consequence of embedding regulatory policy in technical standards pose a number of important dilemmas. If technical systems implement policy decisions through particular standards, desirable policy changes might necessitate rebuilding the infrastructure. Some policy objectives might also be more readily incorporated into standards than others. For example, the basic data protection principle that personal information not be retained any longer than necessary to accomplish the purpose for which it was collected may easily translate into a standard for data purging, but the principle that data may only be used for the purpose for which it was collected is far more difficult to build into the system, because data may be reused and recycled.

C. Network Federalism

Governance in the network environment suggests a need to recognize network systems as semi-sovereign entities.[62] Networks have key attributes of sovereignty: participant/citizens via service provider membership agreements, "constitutional" rights through contractual terms of service, and police powers through taxation (fees) and system operator sanctions. In effect, network users become stakeholders in transnational political and economic communities. As CompuServe's elimination of certain Internet usenet groups illustrates, network management affects participant discourse.[63] These characteristics warrant a degree of network independence from state intervention.

Nevertheless, where networks develop parallel to physical society, traditional governments retain crucial public responsibilities and significant interests. For example, distance learning through video conferencing may substitute for local schools, but it does not diminish or replace the public interest in an educated citizenry. Similarly, physical points of contact be-

---

[62] *See, e.g.*, Johnson & Post, *supra* note 28 (arguing that cyberspace should be recognized as its own jurisdiction).

[63] *See* text accompanying notes 33-34.

tween networks and states as a result of the location of users, as well as the location of network infrastructure (such as cables and nodes), give states a direct interest in network activities.

The overlap of interests between the physical world and the virtual world suggests a governance model that contains distinct rules for the separation of powers. Territorial borders will retain an important role in structuring overlaps between network boundaries and state jurisdictions. Principles of federalism offer a valuable lesson for the relationship between territorial governments and cyberspace. Just as Lex Mercatoria did not displace the law of the situs of trade fairs,[64] a new Lex Informatica suggests that sovereign states should act only within particular spheres or zones of influence.[65] State governments can and should be involved in the establishment of norms for network activities, yet state governments cannot and should not attempt to expropriate all regulatory power from network communities. In some ways, the European principle of subsidiarity[66] fits the network model. States can act to govern behavior on networks only when state competence and direct state interests are established or when they are more capable of doing so than networks.

D. Role of the State

Even though national borders have less meaning in an information society, states retain a critical ability to influence rule-making by networks themselves. States can provoke the creation of network standards like the development of content filters on the CompuServe network.[67] With power over physical situs points (users and infrastructure), states have the capability to set conditions of network operations, such as free expression or minimal service obligations, in exchange for legally permissible access to users or infrastructure situs points. States have a potent tool in the ability to impose and enforce a certain degree of liability on networks and their participants. This power thus gives states the capacity to influence network behavior as well as the capacity to create legal conflicts.

---

[64] *See* Hardy, *supra* note 29, at 1020.

[65] *See id.* at 1025.

[66] *See* text accompanying note 53.

[67] *See* Michael Meyer, *A Bad Dream Comes True in Cyberspace*, NEWSWEEK, Jan. 8, 1996, at 65.

As the GII moves forward, the governance of networks suggests a movement toward a system of state-provided incentives through encouragement, as well as allocation of liability, that will induce networks themselves to adopt desirable public policies.[68] For example, as stakeholders in a network system, users may pressure networks to adopt principles of democracy for network decisions, as seen in the vigorous on-line debates regarding CompuServe's action. However, under different circumstances, public interests may dictate that governments actively seek elements of network democracy as a condition of network operation. With physical power over persons and infrastructure, states can exercise a control over key network situs points. The allocation of liability might evolve as a policy instrument to promote network self-regulation. Yet this policy instrument requires cautious use. State intervention that imposes an excessive burden of liability may impede the advantages of a robust network and result in censorship of valuable information flows.

VI. CONCLUSION

The GII poses a fundamental challenge to the conventional foundations of governance. Global networks structurally alter regulatory decision-making. National borders and sectoral boundaries lose an important degree of relevance while network borders and network communities gain prominence. Basic regulatory policymaking, whether under the anti-statist American approach or the comprehensive European approach, is ill suited to the GII. Instead, a new "network governance paradigm" must emerge to recognize the complexity of regulatory power centers, utilize new policy instruments such as technical standardization to achieve regulatory objectives, accord status to networks as semi-sovereign entities, and shift the role of the state toward the creation of an incentive structure for network self-regulation.

[68] Professor Hardy makes a similar point in arguing for strict liability of network operators as the best means of achieving a desired regulatory policy outcome. *See* Hardy, *supra* note 29, at 1041-48. This runs the risk, however, that network operators will adopt a policy of "when in doubt, take it out" and consequently engage in broad censorship.