1997

Lex Informatica: The Formulation of Information Policy Rules through Technology

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

Texas Law Review

Volume 76, Number 3, February 1998

Articles

Lex Informatica: The Formulation of Information Policy Rules Through Technology

Joel R. Reidenberg*

I. Introduction to Lex Informatica

During the middle ages, itinerant merchants traveling across Europe to trade at fairs, markets, and sea ports needed common ground rules to create trust and confidence for robust international trade. The differences among local, feudal, royal, and ecclesiastical law provided a significant degree of uncertainty and difficulty for merchants. Custom and practices evolved into a distinct body of law known as the "Lex Mercatoria," which was independent of local sovereign rules and assured commercial participants of basic fairness in their relationships.[1]

In the era of network and communications technologies, participants traveling on information infrastructures confront an unstable and uncertain environment of multiple governing laws, changing national rules, and conflicting regulations. For the information infrastructure, default ground rules are just as essential for participants in the Information Society as

---

* Professor, Fordham University School of Law. This paper was prepared and funded during a Fordham University Faculty Fellowship and as part of a sabbatical in the Public Policy Researeh Department at AT&T Network Services Research Laboratory. I am particularly indebted to Paul Resnick at AT&T for discussions of the paper, guidance on technical issues, and comments on earlier drafts. In addition, I want to thank Ira Heffan, Bob Gellman, Mark Lemley, Larry Lessig, and Paul Schwartz for comments on earlier drafts. Any errors remain the sole responsibility of the author.

1. *See* Harold J. Berman & Colin Kaufman, *The Law of International Commercial Transactions (Lex Mercatoria)*, 19 HARV. INT'L L.J. 221, 274-77 (1978).

Lex Mercatoria was to merchants hundreds of years ago.[2] Confusion and conflict over the rules for information flows run counter to an open, robust Information Society. Principles governing the treatment of digital information must offer stability and predictability so that participants have enough confidence for their communities to thrive, just as settled trading rules gave confidence and vitality to merchant communities. At present, three substantive legal policy areas are in a critical state of flux in the network environment. The treatment of content, the treatment of personal information, and the preservation of ownership rights each presents conflicting policies within nations and shows a lack of harmonization across national borders. In addition, serious jurisdictional obstacles confront the enforcement of any substantive legal rights in the network environment.[3] But just as clear accounting rules reassured participants in twentieth century financial markets, ground rules for the access, distribution, and use of information will shape the trust, confidence, and fairness in the twenty-first century digital world for citizens, businesses, and governments.

Historically, law and government regulation have established default rules for information policy, including constitutional rules on freedom of expression and statutory rights of ownership of information.[4] This Article will show that for network environments and the Information Society, however, law and government regulation are not the only source of rule-making. Technological capabilities and system design choices impose rules on participants.[5] The creation and implementation of information policy

---

2. On the essential role and establishment of information policy default rules, see generally Joel R. Reidenberg & Francoise Gamet-Pol, *The Fundamental Role of Privacy and Confidence in the Network*, 30 WAKE FOREST L. REV. 105, 107 (1995); Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 EMORY L.J. 911, 917-18 (1996).

3. For an excellent treatment of personal jurisdiction and prescriptive jurisdictional problems in the United States, see Dan L. Burk, *Federalism in Cyberspace*, 28 CONN. L. REV. 1095, 1107 (1996).

4. *See generally* JAMES BOYLE, SHAMANS, SOFTWARE AND SPLEENS (1996); M. ETHAN KATSH, LAW IN A DIGITAL WORLD (1995).

5. *See* Larry Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869, 896-97 (1996) (arguing that software codes are societal constraints); M. Ethan Katsh, *Software Worlds and the First Amendment: Virtual Doorkeepers in Cyberspace*, 1996 U. CHI. LEGAL F. 335 (exploring the role of software in structuring speech in the on-line environment); Reidenberg, *supra* note 2, at 918, 927-28 (arguing that technical standards set boundary rules and embed policy choices). Some argue that technical standards and legal rules may either supplement each other or, in some circumstances, be substitutes. *See* Joel R. Reidenberg, *Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms*, 6 HARV. J.L. & TECH. 287, 301-04 (1993) [hereinafter Reidenberg, *Rules of the Road*] (arguing that technical considerations establish normative standards which, in turn, impact system practice); Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 508-09 (1995) (arguing that legal rules may be supplemented by technical considerations as well as business practices); Ann Cavoukian, Go Beyond Security—Build in Privacy: One Does Not Equal the Other, CardTech/SecurTech '96 Conference (May 14-16, 1996) (on file with the *Texas Law Review*) (describing technological innovations and arguing for them to be built into systems and applications to enhance privacy). The Canadian government is, for example, exploring technological options for information privacy. *See* Ministerial Conference on Global Information Networks, Bonn, Germany (July 7, 1997) (statement of John Manley, Canadian

are embedded in network designs and standards as well as in system configurations. Even user preferences and technical choices create overarching, local default rules.[6] This Article argues, in essence, that the set of rules for information flows imposed by technology and communication networks form a "Lex Informatica" that policymakers must understand, consciously recognize, and encourage.[7]

The Article begins in Part II with a sketch of the information policy problems inherent in the legal regulation of content, personal information, and intellectual property on global networks. Part II proceeds to show specific technical solutions and responses to these policy problems as an illustration of the rule-making power of technology and networks. These illustrations serve as a prelude to the articulation of a theory of Lex Informatica.

Part III then defines the theoretical foundation for Lex Informatica by showing technological constraints as a distinct source of rules for information flows. Lex Informatica intrinsically links rule-making capabilities well suited for the Information Society with substantive information policy choices. Lex Informatica may establish a single, immutable norm for information flows on the network or may enable the customization and automation of information flow policies for specific circumstances that adopt a rule of flexibility.

Part IV applies the theory to demonstrate how Lex Informatica can be a useful policy device. The characteristics of Lex Informatica provide ways to accommodate different national public policies for controversial problems, such as content restrictions,[8] the treatment of personal

---

Minister of Industry) (on file with the *Texas Law Review*). Industry Canada has also held an important symposium on privacy enhancing technologies. *See Big Brother: Friend or Foe?*, 1 INDUSTRY CANADA UPDATE 2, ¶ 1-2 (Oct. 1, 1996) <http://www.ic.gc.ca/ic-data/welcomeic.ns>.

6. For example, a telephone subscriber's choice between per line and per call blocking of caller identification information creates a default rule applicable to all users of the particular telephone line. Per line blocking means no information is conveyed; per call blocking requires the caller to act affirmatively to block information for each call.

7. This Article will not address the specific role of community ethos and norms in setting network rules. For a discussion of these aspects, see Edward J. Valauskas, *Lex Networkia: Understanding the Internet Community*, 1 FIRST MONDAY 5, ¶ 10-13 (Oct. 7, 1996) <http://www.firstmonday.dk/issues/issue4/valauskas/index.html> (discussing the role of Internet community practices in normalizing online behavior).

8. *See, e.g.*, Reno v. ACLU, 117 S. Ct. 2329 (1997) (upholding the findings of a three-judge panel that provisions of the Communications Decency Act proscribing transmission of "indecent" material were overly broad and thus violated the First Amendment's guarantee of free speech); Shea v. Reno, 930 F. Supp. 916 (S.D.N.Y. 1996) (reviewing the Communications Decency Act under a standard applicable to content-based legislation), *aff'd*, 117 S. Ct. 2501 (1997). Other countries may also have additional content concerns, such as Germany's and France's prohibitions on holocaust denial and Germany's restrictions on neo-Nazi expression. *See* Tribunal de Grande Instance, Paris, June 12, 1996, Ref. 53061-96 (discussing Art. 24 of the law of July 24, 1881 and its application to anti-Semitic and revisionist messages), *available in* <http://www.aui.fr/Groupes/GT-RPS/UEJF/ordonnance.html>; Ulrich Karpen, *Freedom of Expression as a Basic Right: A German View*, 37 AM. J. COMP. L. 395, 399 (1989) (discussing restrictions on the right of free speech in Germany);

information,[9] and the protection of intellectual property[10] circulating on transnational networks. As a consequence, policymakers can and should look to Lex Informatica as a useful extra-legal instrument that may be used to achieve objectives that otherwise challenge conventional laws and attempts by governments to regulate across jurisdictional lines.

The rise of a new regulatory regime for information policy has striking implications for public officials and government policy. Part V explores redirecting public policy rule-making strategies. Because the formulation of the substantive rules of Lex Informatica bypasses customary legal regulatory processes, the traditional law approach, such as government-issued decisions, will be less effective in achieving desired information policy results than a technological approach, such as the promotion and development of flexible, customizable systems. Technical standards and standard-setting mechanisms acquire important political characteristics. For the development of information policy rules in Lex Informatica, policymakers must use strategies and mechanisms that are different from traditional regulatory approaches.

II. Information Policy Problems and Technical Solutions

Cyberspace, as the virtual world is known, enables beneficial as well as nefarious activities to thrive. Global networks are a powerful infrastructure for national and transnational human interactions involving commerce, entertainment, and politics. The regulation of content on networks, the circulation of personal information, and the distribution of intellectual property raise profound conflicts for national and international law. The substantive standards, jurisdictional authority, and enforcement

---

Christopher P. Winner, *Contemporary Views of Holocaust Are in Constant State of Flux*, USA TODAY, Feb. 17, 1997, at 8A (discussing the sentencing of a German neo-Nazi for inciting racial hatred).

9. *See, e.g.*, Council Directive 95/46 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31 [hereinafter European Privacy Directive] (attempting to harmonize the protection of personal information within the European Union); PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF U.S. DATA PROTECTION (1996) (exploring the approach taken by American law to the problem of protecting privacy in a modern, computerized era and comparing that approach to European standards); Symposium, *Data Protection Law and the European Union's Directive: The Challenge for the United States*, 80 IOWA L. REV. 431 (1995) (debating data privacy issues as they relate to the European Directive).

10. *See, e.g.*, INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS (1995) [hereinafter WHITE PAPER] (canvassing the current law of copyright, patent, trademark, and trade secret and making recommendations for possible changes to the Secretary of Commerce); Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 1019-30 (1996) (arguing that legal protection for copyright-management technologies might violate the First Amendment); Pamela Samuelson, *The Copyright Grab*, WIRED, Jan. 1996, at 134 (arguing that Congress should wait to see what kind of free market protections evolve before pursuing the White Paper's legislative recommendations).

powers all clash. Just as technology creates and compounds these conflicts, technology also offers new solutions for information policy rules in these controversial legal arenas.

A. *Content*

1. A Basic Policy Dilemma.—The legal regulation of content on global networks poses intricate philosophical, practical, and political complications. Censorship of information is anathema in some legal cultures, like the United States,[11] but not in others, like Singapore and China.[12] Even within any single jurisdiction, the regulation of information content poses a fundamental political issue for democratic societies. For example, in the United States, concerns over the easy access that children had to pornography and obscenity on the Internet resulted in the Communications Decency Act,[13] which imposed liability on information service and access providers who were conduits to the dissemination of offensive material to minors. Two separate federal courts have held the statute unconstitutional on various grounds,[14] and the Supreme Court has affirmed that the indecency section of the statute violates the First Amendment with its overbroad sweep—without reaching the argument that it violates the Fifth Amendment as well.[15] The Supreme Court let stand the prohibitions on obscenity.[16] Yet at the same time, the operator of a pornographic bulletin board may be held liable for trafficking in illegal content across state lines.[17]

---

11. *See* U.S. CONST. amend. I (prohibiting governmentally imposed restrictions on speech).

12. Singapore has recently required all Internet traffic to pass through monitored gateways. *See Silencing the Net: The Threat to Freedom of Expression On-line*, 8 HUM. RTS. WATCH 2, ¶ 46-50 (May 1996) <http://www.epic.org/free_speech/intl/hrw_report_5_96.html> [hereinafter HUMAN RIGHTS WATCH]; *see also* Poh-Kam Wong, Implementing the NII Vision: Singapore's Experience and Future Challenges, Paper presented at Harvard Symposium on National and International Initiatives for the Information Infrastructure (Jan. 24-26, 1996) (discussing Singapore's governmental policy toward public access to network content), *available in* <http://ksgwww.harvard.edu/iip/GIIconf/wongpap.html>. China similarly filters all in-bound and out-bound Internet traffic. *See* Minutes of the 21st Meeting of the International Working Group on Data Protection in Telecommunications 5, Paris, (Apr. 3, 1997) (report of Stephen Lau, Data Protection Commissioner of Hong Kong) [hereinafter Minutes] (on file with the *Texas Law Review*).

13. *See* H.R. REP. NO. 104-458, at 189 (1996) ("[R]equiring that access restrictions be imposed to protect minors from exposure to indecent material . . . merely puts it in its appropriate place: away from children."); *see also* Communications Decency Act § 502, 47 U.S.C.A. § 223 (West Supp. 1997).

14. *See* Shea v. Reno, 930 F. Supp. 916 (S.D.N.Y. 1996), *aff'd*, 117 S. Ct. 2501 (1997); ACLU v. Reno, 929 F. Supp. 824 (E.D. Pa. 1996), *aff'd*, 117 S. Ct. 2329 (1997).

15. Reno v. ACLU, 117 S. Ct. 2329, 2347 (1997).

16. *Id.* at 2350.

17. *See* United States v. Thomas, 74 F.3d 701, 711 (6th Cir.) (rejecting the defendant's claim that obscenity must be judged against the standards of a cyberspace community rather than a geographic community), *cert. denied*, 117 S. Ct. 74 (1996).

A similar debate is raging in France with the passage of the new Telecommunications Reform Act,[18] which requires information service providers to offer technical means for users to filter content.[19] The French Constitutional Court, however, struck down companion sections regulating indecency for reasons of separation of powers and vagueness.[20] Nevertheless, two presidents of Internet service providers were indicted under existing French law for making illegal material available over their networks.[21] Elsewhere, at least one country—Singapore—has sought to monitor all information content entering its physical jurisdiction. Singapore requires the registration of all Internet service providers and also monitors their activities in Singapore.[22]

While these debates are just beginning in national capitals around the world, the practical implications are significant. Global access to information content means that information providers may face liability for actions that, although legal where performed, were illegal where viewed.[23] Fundamental political freedoms in one jurisdiction thus may be threatened by the risk of liability in another jurisdiction. In other words, network service providers may opt for the overly cautious route of self-censorship and adopt policies of "when in doubt, take it out."

2. A Technical Solution.—The Platform for Internet Content Selection (PICS) is a prime example of a technological solution designed to resolve the policy problem of accommodating different standards for content without compromising free speech values.[24] A consortium of computer-science scholars and industry representatives designed PICS to facilitate the selective blocking of access to information on the Internet and to provide an alternative to legal restrictions on the dissemination of content on the Internet.[25] PICS is a set of technical specifications that define a standard

---

18. Law No. 96-659 of July 26, 1996, art. 15, J.O., July 27, 1996, p. 11384, *available in* LEXIS, Loireg Library, JO File.

19. *See id.* at art. 15.

20. Cons. const., Décision No. 96-378 DC, July 23, 1996, *available in* LEXIS, Public Library, Consti File, *and in* <http://www.conseil-constitutionnel.fr/decisions/96/96378.doc>.

21. *See* HUMAN RIGHTS WATCH, *supra* note 12. Similarly, the head of CompuServe's German subsidiary was indicted for facilitating the trafficking in pornography. *See* Edmund L. Andrews, *CompuServe Unit Chief Is Indicted in Germany*, INT'L HERALD TRIB., Apr. 17, 1997, at 13, *available in* LEXIS, World Library, Allnws File.

22. *See supra* note 12.

23. *See, e.g.*, United States v. Thomas, 74 F.3d 701, 711 (6th Cir.), *cert. denied*, 117 S. Ct. 74 (1996) (affirming the application of Tennessee's community obscenity standards to material placed by the defendant on an electronic bulletin board located in California but viewed in Tennessee).

24. *But see* Jonathan Weinberg, *Rating the Net*, 19 HASTINGS COMM. & ENT. L.J. 453, 455, 454-55 (1997) (warning that the self-rating of Internet sites presents free speech concerns and that self-rating may be increased as PICS makes it easier to "create and market such ratings").

25. Industry was particularly interested in proposing nonregulatory responses to Senator Exon's efforts promoting antipornography Internet legislation. PICS was developed by W3C, the World Wide Web Consortium, co-chaired by James Miller of MIT and Paul Resnick of AT&T. *See Platform for*

format for rating labels describing materials available on the Internet and a standard mechanism for distributing those labels.[26] As originally conceived, parents or other supervisors could then set filtering rules that would selectively block a child's access to materials associated with the chosen rating labels, much like the way a parent might prohibit a child from seeing an "R" rated movie.[27] In essence, the set of specifications sought to empower parents with a means to screen out inappropriate materials for their children without hindering the dissemination to the child next door or to anyone else.

The PICS standard itself is neutral with respect to the terms used in rating labels, the actual rating of materials, and the filtering criteria.[28] Multiple terms and rating labels may coexist for the same information. For example, one set of ratings may use the terms "violence" and "nudity," while another set may adopt "blood" and "sex." Content providers can rate their own material and distribute corresponding rating labels for the information.[29] Third parties may also associate rating labels with particular information disseminated over the Internet.[30] With the existence of standardized labels, a supervisor, such as a parent, may then set criteria for filtering, including which rating sources to use and which rating terms indicate acceptable or inappropriate materials.[31] Software mechanisms built into web browsers or elsewhere in the network may accomplish this filtering.[32]

Internet Content Selection (last modified July 18, 1997) <http://www.w3.org/PICS/>. For an explanation of the technology and its development, see Paul Resnick & James Miller, *PICS: Internet Access Controls Without Censorship*, COMMUNICATIONS OF THE ACM, Oct. 1996, at 87, 87-93.

26. *See* Resnick & Miller, *supra* note 25, at 87.

27. *See id.* at 88.

28. *See id.* at 92.

29. This is the approach taken by RSACi and SafeSurfing. The respective groups have defined distinct rating terms and content providers self-label according to those terms. *See* Recreational Software Advisory Council on the Internet, *About RSAC* (visited Aug. 29, 1997) <http://www.rsac.org/>; SafeSurf, *The Original Internet Rating System* (visited Aug. 29, 1997) <http://www.safesurf.com/>; *see also* Weinberg, *supra* note 24, at 462-64 (comparing RSACi with SafeSurfing and noting the inherent limitations of self-rating). Self-labelling, however, runs the danger that content providers may mislabel their materials. Dishonest labelling may be discouraged by legal sanctions for deceptive behavior as well as possible marketplace retribution.

30. This is the approach taken by SurfWatch and Cyber Patrol. *See Internet Cyber Patrol* (last modified Sept. 15, 1997) <http://www.cyberpatrol.com/>; *SurfWatch* (visited Sept. 15, 1997) <http://www.surfwatch.com/> (showing that both services rate the sites of third parties). Independent labelling runs the risk that someone might distribute rating labels falsely purporting to come from another. This practice is known as "spoofing." Cryptographic techniques can be used to detect and deter such spoofs.

31. *See* Resnick & Miller, *supra* note 25, at 63. Microsoft's Internet Explorer 3.0, for example, can read PICS labels from any source, whether self-labelled or third-party labelled, and allows users to specify the filtering rules. *See* Paul Resnick, *Filtering Information on the Internet*, SCI. AM., Mar. 1997, at 62, 62.

32. *See* Resnick & Miller, *supra* note 25. Various techniques may also be deployed to make it difficult for children or others to bypass the filters installed by parents or supervisors. *See Internet*

The structure of PICS allows several different content-evaluation standards to be applied to the same information on a web site and different viewers to use different filter criteria.[33] Thus, PICS can work well to segment permissible content in various jurisdictions.[34] If laws conflict between jurisdictions, network proxy servers can use PICS technology as part of a firewall to filter content that is impermissible in the local jurisdiction but legal elsewhere.[35] Similarly, if laws use potentially incompatible standards such as the "local community standard" for pornography classifications,[36] PICS technology allows different filters within a single jurisdiction. This technology provides individual choice of filtering rules, yet it still offers automatic enforcement.[37] Finally, PICS technology can allow transborder enforcement by providing a means to label material that is located elsewhere. Third-party rating labels may be distributed through a server that is separate from the labelled documents.[38] Thus, the document authors and web sites where the documents are posted need not cooperate with law enforcement efforts.

B. Personal Information

1. The Policy Problem.—The fair treatment of personal information in an Information Society poses another enormous challenge for legal regulation. Over the last three decades, fair information practice principles have been enshrined in industrialized societies.[39] The penetration of

---

Cyber Patrol (last modified Sept. 15, 1997) <http://www.cyberpatrol.com/> (noting the presence of multiple safeguards that prevent users from disabling Cyber Patrol or renaming blocked materials).

33. *See* World Wide Web Consortium, *PICS Statement of Principles* (visited Aug. 29, 1997) <http://www.w3.org/pub/WWW/PICS/principles.html> (explaining how the standards devised by PICS facilitate third-party labelling).

34. However, the platform will only be effective if there is a critical mass of labels and rated web sites. *See* Weinberg, *supra* note 24. An incentive structure still needs to emerge that will encourage the development of the critical mass. *See* Joel R. Reidenberg, *The Use of Technology to Assure Internet Privacy: Adapting Labels and Filters for Data Protection*, LEX ELECTRONICA (forthcoming 1997), *draft available in* <http://home.sprynet.com/reidenberg/picprv.htm> (discussing the critical-mass problem for personal information).

35. This is the approach in Singapore and China. *See* HUMAN RIGHTS WATCH, *supra* note 12; Minutes, *supra* note 12.

36. *See, e.g.*, United States v. Thomas, 74 F.3d 701, 711, 710-11 (6th Cir.) (subjecting pornographic, electronic materials to the community standards of "the geographic area where the materials are sent"), *cert. denied*, 117 S. Ct. 74 (1996).

37. This is the basis for CyberPatrol or Microsoft Internet Explorer Content Advisor. *See* Resnick, *supra* note 31 (noting that both services use the PICS standard).

38. *See* Resnick & Miller, *supra* note 25, at 89; Federal Trade Comm'n, *Public Workshop on Consumer Privacy on the Global Information Infrastructure*, F.T.C. Project P954807, Washington, DC (June 4, 1996) (statement of Paul Resnick, AT&T Research) (transcript available at <http://www.ftc.gov/bcp/privacy/privacy.htm>) [hereinafter FTC Testimony].

39. *See* SCHWARTZ & REIDENBERG, *supra* note 9, at 6-13 (showing the emergence of rights in the private and public sectors in the United States, but also demonstrating a more significant commitment to the free flow of information); Symposium, *supra* note 9 (observing that fair information practices have become law throughout Europe).

information technology around the world during the last decade, however, has provoked re-examination of the application of core fair information practice principles in network environments.[40] In the United States, legal rights are limited, and public concern for privacy invasions is high.[41] Public-policy debates continue to search for a consensus on privacy standards. In Europe, comprehensive legal rights exist and government enforcement plays an important role.[42] At the same time, public-policy debates throughout Europe reflect similar concerns for the development and application of privacy standards to information circulating on global networks.[43] The widely ranging legal standards for fair information practice in different countries present conflicts for global information flows.[44]

---

40. *See* Privacy Working Group, Information Infrastructure Task Force, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information* (last modified June 6, 1995) <http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niiprivprin_final.html> (articulating basic principles for the "fair use of personal information" by users of the National Information Infrastructure); U.S. DEPT. OF COMMERCE, PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION (1995) (recommending a re-evaluation of existing telecommunications laws in light of the threat that information technology poses to privacy); European Privacy Directive, *supra* note 9 (providing harmonized European Union standards for the privacy rights and free flow of personal data); COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS [C.N.I.L.], VOIX, IMAGE ET PROTECTION DES DONNÉES PERSONNELLES (1996) (discussing the risks and applicability of data protection principles to the digitalization of sound and images); International Working Group on Data Protection in Telecommunications, *Data Protection and Privacy on the Internet: Report and Guidance* (Nov. 19, 1996) <http://www.datenschutz-berlin.de/diskus/13_15.htm> (recommending increased privacy safeguards on the Internet).

41. *See* SCHWARTZ & REIDENBERG, *supra* note 9, at 6-7 (recognizing the American commitment to the free flow of information, the limited scope of existing legal rights, and the public concern over privacy). Public opinion polls over the last decade consistently show that more than 75% of Americans feel as though they have lost control of their personal information. *See, e.g.*, LOUIS HARRIS & ASSOCS. & ALAN F. WESTIN, THE EQUIFAX REPORT ON CONSUMERS IN THE INFORMATION AGE, at xxi (1990) (reporting survey results indicating that 79% of Americans were either "somewhat" or "very" concerned about threats to their personal privacy); Humphrey Taylor, *Opportunities and Minefields in Interactive Services*, PRIVACY & AM. BUS., Mar. 1995, at 9 (reporting that 76% of the public believes business asks for too much personal information); *see also* LOUIS HARRIS & ASSOCS., EQUIFAX-HARRIS CONSUMER PRIVACY SURVEY 71 (1996) (reporting that 64% of Americans believe on-line service providers should not track users' Internet surfing habits).

42. *See* European Privacy Directive, *supra* note 9, at Art. 1 (requiring that all member states protect their citizens' privacy); COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 192 (1992) (describing the regulatory approaches taken in Sweden, West Germany, the United Kingdom, and the United States).

43. The European Commission has, for example, sponsored a comprehensive study of data protection and on-line services to be completed by the end of 1997. *See* European Commission, Invitation to tender No. XV/96/20/D. The French National Commission on Informatics and Freedom has established a "Study Group on International Networks" composed of European data privacy commissioners, *see* COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS [C.N.I.L.], 17IÈME RAPPORT ANNUEL 65 (1997), and the Berlin Privacy Commission devoted much of the 21st Meeting of the International Working Group on Data Protection in Telecommunications to Internet issues. *See* International Working Group on Data Protection in Telecommunications, Agenda for the 21st Meeting of the International Working Group on Data Protection in Telecommunications in Paris (Mar. 20, 1997) (on file with the *Texas Law Review*).

44. *See, e.g.*, Joel R. Reidenberg, *The Privacy Obstacle Course: Hurdling Barriers to Transnational Financial Services*, 60 FORDHAM L. REV. S137 (1992).

Information flows defy national jurisdiction. European data protection authorities have the legal right to interdict transborder data flows if the destination does not have adequate standards for information privacy.[45] However, the supervision of foreign data processing and the actual enforcement of interdiction powers are extremely difficult to implement for transnational networks.[46]

2. *Technical Solutions*.—Several technical solutions provide valuable tools to establish fair information practice policy on global networks. At the first level, technological mechanisms can anonymize information that would otherwise be associated with particular individuals. Identity masks, such as anonymous remailers for electronic mail[47] or anonymous browsers[48] for Internet surfing, offer users control of their personal information. One company, I/PRO, developed mapping features that enable web sites to learn demographic and other information about site visitors without those sites' discovering the identities of the individuals, unless an individual affirmatively chooses to reveal personal information.[49] A user reveals demographic information to a trusted third party, in this case I/PRO. When the user connects to a web site, the user gives the web site a numeric identifier. The web site then can gain access to some of the demographic data from the trusted third party. If the user grants authorization, the user's name and other personal information may be released to the web site. These technical configurations allow information flows to avoid problems with privacy issues because the technical configurations can resolve issues of conflicting privacy standards either with data that no longer relates to specific individuals or with data that relates to identified persons who have expressly agreed to particular use of their information.[50]

---

45. *See id.* at S160-65 (discussing European policies on restricting transborder data flows); *see also* European Privacy Directive, *supra* note 9, at Art. 25.

46. *See* C.N.I.L., *supra* note 40, at 1995.

47. An anonymous remailer is an Internet site that forwards mail to a specified address and masks the identity of the original sender. *See* A. Michael Froomkin, *Anonymity and its Enmities*, 1995 J. ONLINE L. art. 4, ¶ 10 (Aug. 29, 1997) <http://www.law.cornell.edu/jol/froomkin.htm> (explaining that the common characteristic of all anonymous remailers is that they delete identifying information on electronic mail and they replace the sender's name with that of the remailer or attach an anonymous name tag).

48. While Internet surfing does not necessarily reveal any information about an individual other than the Internet Protocol address for the particular surfing session, fully anonymous browsing may be accomplished by directing all traffic through an anonymizing web site. *See, e.g.*, *Anonymizer.com* (visited Oct. 22, 1997) <http://www.anonymizer.com/open.html> (providing anonymous web browsing through its anonymizer buffer).

49. *See* FTC Testimony, *supra* note 38 (statement of I/PRO). Although I/PRO has discontinued this particular service, the technological concept remains valid. For configurations like I/PRO's, however, aggregations of information must be carefully constructed to avoid the inadvertent disclosure of identities. For example, the level of detail may indirectly identify particular individuals when few people could actually match the disclosed information.

50. If particular legal rules for data processing may not be waived by individuals, then technical mechanisms that allow user choice may not be effective in reconciling conflicting policy rules.

PICS-based rating labels and software filters similarly offer promise for the resolution of conflicting legal privacy rules on the Internet.[51] Where legal standards differ, such as between the United States and most European countries,[52] and where an individual may consent to deviations from default legal standards,[53] filter configurations using the PICS protocol allow users to make determinations about the use of personal information and to assure the implementation of those decisions on the Net.[54] Users may express their privacy preferences, and web sites may be rated for their treatment of personal information.[55] When the preferences and treatment defaults do not match, a software filter can be designed to disclose the discrepancy to the user and to stall the transaction.[56] Users may choose either to proceed or to cancel the interaction.[57] The PICS-based model can also support explanations of information practices by web sites to assist users in making their decision.[58] This vehicle can thus create disclosure-of-information practices even in the absence of a legal requirement, and it can automate the negotiation of information policies that are satisfactory to the user. This automation of notice and choice permits customization of information privacy to individual needs without imposing a time or information processing burden on individuals.[59]

The PICS-based filters and configuration arrangements are not, however, a complete solution. Unlike the context of PICS rating labels for content, information privacy rating labels cannot readily be made without

---

51. For a description of PICS technology, see *supra* section II(A)(2).

52. *See generally* SCHWARTZ & REIDENBERG, *supra* note 9 (comparing U.S. fair information practices to European norms).

53. For example, there is a basic data privacy requirement in Europe that information only be used to achieve the purpose for which it was collected. *See id.* at 14. Secondary uses of personal information are permissible only with the consent of the individual concerned. *See id.* at 15. The default rule limits the purposes of data use, and the legal rule allows individuals to waive those limitations.

54. *See* Reidenberg, *supra* note 34, Part IV (arguing that a PICS-based mechanism may be able to satisfy the conflict between European and American privacy law); FTC Testimony, *supra* note 38, at 96-99.

55. *See* FTC Testimony, *supra* note 38, at 96-97.

56. *See id.* at 98.

57. *See id.*

58. This application is technically feasible, but it is not yet built into the existing PICS standard. *See id.* In April 1997, the World Wide Web Consortium launched a development effort to create a negotiation protocol for privacy that provides for this functionality. *See* W3C, *Platform for Privacy Preferences (P3P) Project: Platform for Privacy Preferences Initiative* (visited Oct. 29, 1997) <http://www.w3.org/P3/Overview.html>. P3P seeks to set up an interoperable way of expressing privacy preferences by web sites and users. Users will be able to decide whether to accept the terms of the web site before browsing.

59. Although the coexistence of multiple rating terms and preference choices may suggest a confusing array of decisions for an individual, this downside of the PICS standard can be minimized with competing default settings. For example, organizations such as the Direct Market Association could make one set of rating terms and default preferences available to the public, just as Privacy International, at the other end of the spectrum, could distribute rating terms and default settings.

the cooperation of the web site.[60] The entity actually performing the data processing must assist third-party labellers if the third parties are to be able to assign appropriate ratings.[61] Self-reported rating labels by web sites do, however, offer a novel connection with legal rules. If self-reported rating labels do not accurately reflect information practices, nonprivacy legal claims may be created as a result, including potential claims such as misrepresentation under tort law and breach of promise under contract law. In either case, however, independent verification and certification of rating labels will provide a vital element of confidence and trust in the site's information practices.[62] In addition, the efficacy of PICS for information privacy depends on the emergence of rating vocabularies[63] and a critical mass of sites with rating labels. If widely acceptable rating terms do not exist and if few sites are given rating labels, then PICS-based filters will not offer a very robust means of solving the problem of conflicting information policy rules because the choice for individuals would remain a theoretical possibility rather than a real, automated process.

The possibility that PICS can facilitate transborder data flows in the face of restrictions contained in the European Directive on data privacy illustrates more specifically the value of technology as an instrument for information policy.[64] PICS technology can provide a means to assure foreign regulatory agencies of the adequacy of off-shore standards of fair information practice. If the private sector develops appropriate rating terms based on accepted fair information practice principles and rating labels are attributed to sites according to those terms, European data-protection authorities can be assured of technical rules that impose fair information practices in the absence of law.[65] Filters using the PICS protocol can read the rating labels and match site ratings to the user's

60. Web content can readily be observed and characterized by outside observers. The extent or lack of fair treatment of personal information at a web site, however, will not be observable to an outsider without access to the processing activities.

61. For a third party to be able to label accurately the information practices of a web site, the outside observer will need access to the site's files and will need to conduct an audit of the processing activities.

62. *See* Reidenberg, *supra* note 34, Part II; *see also Internet Privacy Survey*, PRIVACY & AM. BUSINESS 7 (1997) (showing a lack of trust in business use of personal information on the Internet).

63. At least one set of labelling terms based on the Canadian Standards Association Model Code of Fair Information Practices exists, as well as one based on the European Privacy Directive, *supra* note 9. *See* FTC Testimony, *supra* note 38 (statement of Paul Resnick); Reidenberg, *supra* note 34, at app.

64. *See* Reidenberg, *supra* note 34, Part IV.

65. European data protection commissions will still need to accept that the rating terms are satisfactory. Under the European Directive, the rating terms can be approved as a form of a code of conduct. *See* European Privacy Directive, *supra* note 9, at Art. 27 (encouraging the adoption of codes of conduct to help implement the national provisions).

preferences.[66] This electronic handshaking assures the user's consent to the use of the personal information. In contrast to the difficult legal problems associated with enforcement of standards for extraterritorial data processing, a PICS-based filtering system directly implements and enforces fair information practices. "Certification agents" that verify the accuracy of rating labels at the filtering stage can also achieve decentralized supervision of information practices. In other words, PICS allows configurations that include rating labels and certifications of those labels before web browsing software makes the connection to the web site for an interactive session.[67] If the private sector does not develop these mechanisms, European data protection regulators could encourage the implementation of PICS technology. Rather than prohibit transborder data flows because of uncertain information policies, regulators would be able to require rating labels by particular entities based on specific rating terms and would be able to accredit "certifying agents" so that supervision would be assured.[68] In other words, through the application of PICS technology European data protection agencies may identify as well as create a subset of locations outside the European Union that assure "adequate" protection in the absence of a legal regime.

C. *Ownership Rights*

1. The Policy Issue.—Beyond a few possible solutions for content and information privacy policies, technology also presents a valuable response to some of the legal-policy problems associated with the management of intellectual property rights. Application of the existing intellectual property regimes of copyright, patent, trademark, and trade secret to the electronic world reveals problems similar to those found in the regulation of both content and information privacy. Intellectual property rights are territorial and the scope of national rights remains to a certain degree uncertain for digital works.[69] For example, the treatment of file caching under

66. To satisfy the European Directive's "adequacy" standard, European data protection commissions may stipulate to the use of a default set of preferences for the filtering process. *See* Reidenberg, *supra* note 34, Part IV.

67. The use of a "trusted" system can also preclude the exchange of any information to the destination site prior to the negotiation of the treatment of personal information. *See generally* Mark Stefik, *Trusted Systems*, SCI. AM., Mar. 1997, at 78-81 (discussing trusted systems and the challenge-response technique).

68. In essence, this means that the European Union might be able to avoid confrontation with foreign countries over the legal standards in the foreign country. The European Union can define a set of PICS compliant rating terms, approve a set of preferences for those rating terms that meet the "adequacy" standard, and accredit auditors to certify the accuracy of rating labels. Trusted servers filtering European approved preferences against rating labels certified by the accredited auditors provide assurance that "adequacy" is satisfied. The pronouncement by European data protection commissioners on rating terms, preferences, and auditor accreditation is both politically and practically easier than selectively judging foreign law. *See* Reidenberg, *supra* note 34 (discussing accrediting rating terms).

69. *See* WHITE PAPER, *supra* note 10, at 10 (discussing the needs for and problems with international intellectual property coordination and protection). Various foreign government reports

intellectual property laws may be a noninfringing use of the underlying protected work or may be an unauthorized copying;[70] the answer is unlikely to be uniform across national borders. In addition, works that are globally distributed or accessed internationally on networks face serious impediments to the enforcement of legal protection.[71] Digital multimedia works highlight the difficulties of protecting intellectual property in network environments.[72] The works can be manipulated, changed, or retransmitted by the recipient, often with little possibility of the owner's discovery.[73] Finding infringements and enforcing rights in distant locations is not easy. Even if these scope and enforcement problems were resolved, that technological developments outpace the rate of legal change poses another particular problem for intellectual property rights; the law always lags behind the technology.

2. The Technical Response.—In this context, technical solutions also become an instrument for the management of intellectual property rights and offer some policy solutions.[74] Technical standards can enable intellectual property producers to choose the type of protection they want. For example, technical copy protection can reverse the copyright law's fair use doctrine. If software is distributed in a copy protected form, the acquirer will not be able to make backup copies even though the law may permit

---

identify similar problems. *See* European Comm'n, *Green Paper on Copyright and Related Rights in the Information Society*, *reprinted in* 43 J. COPYRIGHT SOC'Y 53-54 (1995) (arguing that European intellectual property rights need to be enhanced and harmonized for the digital environment); *Preparing Canada for a Digital World: Final Report of the Information Highway Advisory Council*, Ch. 5 (visited Sept. 9, 1996) <http://strategis.ic.gc.ca/SSG/ih01643e.html> (Canadian report) (emphasizing the need to ensure that intellectual property-right protections continue to be adequate in a digital age); *see also* Pamela Samuelson, Consequences of Differences in Scope of Copyright Protection on an International Scale, Proceedings of "Information, National Policy and the Information Infrastructure," John F. Kennedy School of Government/Harvard Law School (Jan. 28-30, 1996), *available in* <http://ksgwww.harvard.edu/iip/>.

70. *See* Cyberspace Law Institute, *Copyright Law on the Internet: The Special Problem of Caching and Copyright Protection* (visited Aug. 29, 1997) <http://www.cli.org/Caching.html> (arguing that the subtleties should distinguish protected and nonprotected cache copying).

71. *See* WHITE PAPER, *supra* note 10, at 130-55 (articulating the challenges facing policymakers as they attempt to protect intellectual property rights in materials that are distributed electronically over international networks).

72. For an overview of the problem, see generally the excellent collection of papers contained in THE FUTURE OF COPYRIGHT IN A DIGITAL ENVIRONMENT (P. Bernt Hugenholtz ed., 1996) (discussing the applicability of copyright regimes to information on the Internet).

73. Netscape 3.01, for example, allows a user to save another person's web page—including images—and then manipulate or modify both the text and image in an editor mode. *See* Navigator Gold Authoring Guide (visited Nov. 15, 1997) <http://home.netscape.com/eng/mozilla/3.0/handbook/authoring/navgold.htm>; *cf.* Cohen, *supra* note 10, at 985 (discussing copyright owners' desire to prevent unauthorized reproduction by developing copyright management systems that track manipulations of digital works).

74. *See, e.g.*, Charles Clark, *The Answer to the Machine Is in the Machine*, *in* THE FUTURE OF COPYRIGHT IN A DIGITAL ENVIRONMENT 139, 143-44 (1996) (discussing technical protections as a means to control the use of electronic documents).

it.[75] The technology prevents the acquirer of the software to make duplications by establishing a read-only format; the law, in contrast, may have adopted a default rule permitting certain copying.[76] Technical mechanisms will also allow information policies such as web file caching to become negotiable.[77] Web caching occurs when world wide web pages on remote servers that are visited by users are copied into the user's local memory. Internet sites or browser software, like Microsoft Explorer or Netscape Navigator, typically perform web caching for quick and easy repeat access or manipulation.[78] The provider of the original web page does not presently participate in the caching decisions; the visitor's system determines when to save a copy in a cache. Technical architectures such as labelling and the interposition of middleware, however, can offer capabilities for web sites to refuse remote system caching.[79] Labelling web pages in the transmission protocol can allow web-page developers to express their rules for dissemination of the page.[80] Proxies or intermediaries that sit between the transmission and the user's system could then read the affixed labels and either allow the caching or require that access to the page pass through a secure viewing mechanism that does not permit transfers of accessed information.[81] These capabilities allow for self-enforcement of the choices desired by owners of intellectual property. Copy protection also employs self-executing protection analogous to the proxy or intermediary option for the customization of file caching.

---

75. *See* 17 U.S.C. § 117 (1994) (allowing copying of a copyrighted computer program for archival purposes). Surprisingly, the United States government has argued for criminal penalties against those trying to circumvent technical protections that might discourage even lawful copying. *See* WHITE PAPER, *supra* note 10, at 230 (recommending that the Copyright Act prohibit mechanisms that defeat technical protections even if such circumvention might constitute permissible "fair use"). Professor Cohen has argued persuasively, however, that legal mechanisms criminalizing tampering with technical protections may be unconstitutional if applied to prevent an individual from viewing information anonymously. *See* Cohen, *supra* note 10, at 1019-31. Nevertheless, such a constitutional restriction would only shorten the time window for commercial exploitation because the electronic lock is bound to be picked, eventually rendering the information insecure.

76. *See, e.g.*, Sega Enterprises, Ltd. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1992) (holding that a defendant's copying of the plaintiff's software with the mere purpose of studying the functional requirements of compatibility was a "legitimate, nonexploitive purpose" that did not violate the copyright laws).

77. *See generally* Rohit Khare & Joseph Reagle, *Rights Management, Copy Detection, and Access Control* (Proceedings of NRC/CSTB/Information Systems Trustworthiness Project) (visited Sept. 21, 1997) <http://www.w3.org/IPR/work/NRC-v1.htm> (describing the possibility of meta-data formats that would allow intellectual-property-rights negotiation).

78. For example, Netscape Navigator 3.01 typically stores web pages from visited sites in the Netscape directory within a subdirectory named "cache." The size of the cache file may be specified by the user through network preferences in the options menu. *See* How Does Document Caching Work in Netscape Navigator? (last modified May 24, 1996) <http://help.netscape.com/kb/client/960514-44.html>.

79. *See* Khare & Reagle, *supra* note 77, §§ 2.1.1, 2.3.2.

80. *See id.* §§ 2.1.2, 2.3.1.

81. *See id.* § 2.3.2.

Similarly, technical solutions can enable network-based enforcement of other intellectual property rights. Technical systems can automate permissions and payment for use of protected works.[82] Secure viewers may be implemented to assure that an owner's choice of restrictions are self-executing.[83] Alternatively, trusted systems may be used to enforce a property owner's rules on a computer that is outside the actual control of the property owner.[84] The trusted system acts as an intermediary between the property owner and user to assure that conditions for use and access are respected.[85] In effect, technology provides network-based instruments that enable owners to manage intellectual property in ways that legal regulation finds problematic.

III. Network Technology as a Distinct Source of Information Flow Rule-Making: Distinguishing Lex Informatica from Legal Rules

The technical responses and solutions to policy conflicts show new ways to establish information flow rules. Policymakers typically, though, associate rule-making with the elaboration of law through the political process within and among states. Rules established in this fashion form a legal regulatory regime. In the context of information flows on networks, the technical solutions begin to illustrate that network technology itself imposes rules for the access to and use of information. Technological architectures may prohibit certain actions on the network, such as access without security clearances, or may impose certain flows, such as mandatory address routing data for electronic messages. Technology may also offer policymakers a choice of information flow rules through configuration decisions. In effect, this set of impositions on information flows through technological defaults and system configurations offers two types of substantive rules: immutable policies embedded in the technology standards that cannot be altered and flexible policies embedded in the technical architecture that allow variations on default settings. Lex Informatica has a number of distinguishing features that are analogous to a legal regulatory

---

82. The Copyright Clearance Center is, for example, beginning to use an on-line clearing system for granting permissions for the use of copyrighted works and for collecting royalty payment. *See, e.g.*, *CCC Statement of Mission* (visited Oct. 7, 1997) <http://www.copyright.com/ccc_frames.html>. Legal mechanisms for tracking access to on-line works may, however, pose significant constitutional hurdles. *See* Cohen, *supra* note 10, at 1024-30 (discussing how the government's interest in antitampering mechanisms may violate the First Amendment).

83. A secure viewer acts as a sort of "embassy on the Net." It enables "extraterritorial" enforcement of a data provider's access restrictions. Data is distributed encrypted and can only be accessed or managed through the secure viewer controlled by the information distributor. This is known as a "trusted system." *See generally* Stefik, *supra* note 67 (explaining the technologies of secure access and trusted systems).

84. *See id.* at 81.

85. For example, a file downloaded in Adobe PDF format and read using Acroread.exe cannot be printed. Folio Views software similarly allows the owner to specify user permissions.

regime and support its role as an important system of rules for an Information Society. In essence, policy choices are available either through technology itself, through laws that cause technology to exclude possible options, or through laws that cause users to restrict certain actions.[86] Specific information policy technologies that set information flow rules show the significance of Lex Informatica as a parallel rule system.

A. Features of Lex Informatica

Table 1—Rule Regimes

	Legal Regulation	Lex Informatica
Framework	Law	Architecture standards
Jurisdiction	Physical Territory	Network
Content	Statutory/Court Expression	Technical Capabilities Customary Practice
Source	State	Technologists
Customized Rules	Contract	Configuration
Customization Process	Low Cost Moderate cost standard form High cost negotiation	Off-the-shelf configuration Installable configuration User choice
Primary Enforcement	Court	Automated, Self-execution

As illustrated in Table 1, Lex Informatica has analogs for the key elements of a legal regime. The basic building block or framework for

86. Professor Lessig has argued a similar point from the perspective of interpreting the United States Constitution for cyberspace. *See* Lessig, *supra* note 5, at 871 (discussing the traditional legal and technological constraints on state regulatory power).

legal regulation is law. For Lex Informatica, architectural standards are an analogous set of building blocks. Architectural standards such as HTTP[87] define the basic structure and defaults of information flows on a communications network. Jurisdictionally, the legal regime and Lex Informatica provide overlapping rule systems. Jurisdiction for legal regulation is primarily based on territory. Legal rules apply only in a well-defined place where the sovereign can exert its power.[88] In contrast, the jurisdictional lines for Lex Informatica do not depend on territorial borders. Instead, the jurisdiction of Lex Informatica is the network itself because the default rules apply to information flows in network spheres rather than physical places. Legal rules, consequently, can apply to each constituent part of the network that is located in a particular physical jurisdiction.

The substantive content of the rules in a legal regime derives from statutory language, government interpretation, and court decisions. Lex Informatica also contains substantive content defined through technical capabilities and customary practices. For example, the protocol for sending electronic mail, SMTP,[89] sets a substantive policy default rule for the circulation of identifying information which is an immutable rule of communications transmission. The standard message format contains a required data field labelled "FROM" to identify the sender, and the customary practice of electronic mail servers establishes that the data in the "FROM" field pertains to the actual person sending the message.[90] Similarly, digital telecommunications signaling capabilities establish a default policy rule for the circulation of caller information.[91] This rule allows flexibility and customization of the information flow. Compared to earlier analog switches, digital signaling provides more options for the stream of transaction information. With digital signaling, call identification information may be transmitted or blocked, and unidentified calls may be rejected by recipients. Actual practices give great control to network users.[92] Thus, these technological capabilities and practices set default rules for the circulation of all information.

---

87. HTTP is an acronym for "Hypertext Transfer Protocol," which is the transmission structure for exchanging information on the World Wide Web. *See* RICHARD W. WIGGINS, THE INTERNET FOR EVERYONE 268 (1995).

88. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 402 (1987).

89. SMTP is an acronym for the "Simple Mail Transfer Protocol." *See* JOHN R. LEVINE & CAROL BAROUDI, THE INTERNET FOR DUMMIES 69 (1993).

90. Nevertheless, anonymous or forged senders are also technically possible and illustrate the case of a deviation from the customary default expectation. This immutable rule may thus be bypassed with the customization of information policy for the particular message.

91. *See* Reidenberg, *Rules of the Road*, *supra* note 5, at 300 n.53.

92. *See* Glen Chatmas Smith, *We've Got Your Number! (Is It Constitutional To Give It Out?): Caller Identification Technology and the Right to Informational Privacy*, 37 UCLA L. REV. 145, 149 (1989) (describing the technology and services available).

The source of default rules for a legal regime is typically the state. The political-governance process ordinarily establishes the substantive law of the land. For Lex Informatica, however, the primary source of default rule-making is the technology developer and the social process by which customary uses evolve.[93] Technologists design the basic infrastructure features that create and implement information policy defaults. Although states may influence the decisions made by technologists through legal restraints on policy choices,[94] the technologists otherwise "enact" or make the technical standards, and the users adopt precise interpretations through practices.

In the legal regulatory regime, private contractual arrangements can be used both to deviate from the law's default rules and to customize the relationship between the parties.[95] Such deviations are only available if the law permits freedom of contract and does not preclude the participants' actions; circumstances exist in which the law may not permit customization.[96] For example, public policy generally rejects contractual waivers of liability for intentional or reckless harms inflicted on others.[97] Like a legal regime, Lex Informatica offers both customization of rules and inalienable rules. Customization for Lex Informatica occurs through technological configurations. For example, Internet browsers such as Netscape contain log files that record the user's web traffic patterns.[98] This protocol establishes a default rule for the collection of personal data that a user can override by altering file attributes or by disabling the log feature.[99] As with legal regulation, these customizations through reconfigurations are only possible if the architectural standards support the deviations. In the

93. *See* Lessig, *supra* note 5, at 897 ("With respect to the architecture of cyberspace, and the worlds it allows, we are God.").

94. *See infra* section V(B)(2).

95. *See* Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87, 87 (1989) (observing that parties are sometimes free to contract around the default rules); Randy E. Barnett, *The Sound of Silence: Default Rules and Contractual Consent*, 78 VA. L. REV. 821, 824 (1992) (analogizing default rules to word-processing programs that set margins in the absence of the user expressly changing the setting).

96. *See* E. ALAN FARNSWORTH, CONTRACTS § 5.2, at 353 (2d ed. 1990) (providing examples of agreements that courts will not enforce because they contravene public policy).

97. *See id.*

98. *See* Netscape Communications Corp., *Persistent Client State HTTP Cookies* (visited Aug. 29, 1997) <http://home.netscape.com/newsref/std/cookie_spec.html> (explaining that cookies can be used to store information about a user on the user's computer, which is then accessed by the server visited on subsequent visits).

99. The data storage files may be attributed "Read-only" status, which prevents the Netscape from recording the information on the hard drive. For example, a user of Windows 95 may do this using the Windows Explorer Software packaged with Windows 95. At the File Menu, Properties Sub-menu, General Tab, and Attributes Selection, the user may impose "Read-only" attributes on the selected file. Netscape Version 3.0 offers users the option to disable the log file, but neither informs of nor explains the existence of "cookies" tracking.

case of log files for Internet use, reconfigurations can only be effective if the logging feature is designed to collect and store the data on a user's local disk drive. If the information is collected and stored directly by the Internet service provider, the user will not have the capability to override the default rule. Lex Informatica can thus have substantive inalienable rules as a result of architectural decisions.

The customization process shows a number of significant differences between the legal regime and Lex Informatica. Law allows customization either through high cost, individualized contract negotiations, or through the moderate-cost use of standardized forms.[100] Lex Informatica offers a wider range of options. Off-the-shelf configurations, like those contained in software packages bundled with equipment, are a relatively low-cost customization of rules.[101] Manufacturers determine these configurations or customizations, such as the routine packaging of Windows 95 with Texas Instrument laptop computers.[102] User installable configurations, such as printer fonts, are a slightly more expensive method of customization.[103] Users must invest time and effort for the selection and installation of the configuration, but these are nevertheless available. And, analogous to the costly negotiation process for contractual arrangements, users may individually select configurations to achieve rule customization. For example, users may deviate from the default configuration by selecting customized color schemes for the appearance of the Windows operating system.[104]

Finally, Lex Informatica has distinct enforcement properties. Legal regulation depends primarily on judicial authorities for rule enforcement. Rule violations are pursued on an *ex post* basis before the courts.[105] Lex Informatica, however, allows for automated and self-executing rule enforcement.[106] Technological standards may be designed to prevent actions from taking place without the proper permissions or authority.[107]

---

100. *See, e.g.*, Ayres & Gertner, *supra* note 95, at 90-92.

101. For example, the Internet Wizard on Windows 95 contains a pre-programmed set of configurations for the use of Internet Explorer and the MSN network.

102. For example, the Texas Instruments Extensa 650CDT sold in December 1996 gave the buyer a one-time choice of a Windows 95 installation or a Windows for Workgroups installation. *See* Texas Instruments, *Notebook Product Information—Extensa 650CDT Notebook* (visited Mar. 28, 1997) <http://www.ti.com/notebook/docs/ext650t.htm>.

103. These configurations require an investment of time and skill by users.

104. The display options in Windows 95 allow users to choose alternate color patterns or to custom design their own if they wish to spend the time and effort.

105. Lawsuits to enforce rules ordinarily occur after the alleged violation has taken place. *See, e.g.*, EDWARD YORIO, CONTRACT ENFORCEMENT: SPECIFIC PERFORMANCE AND INJUNCTIONS § 1.2.2, at 8-9 (1989). Injunctions to prevent violations *ex ante* are still enforced by *ex post* contempt actions. *Id.* § 4.5.2, at 96.

106. Technology may, however, prevent an action that violates the rule from occurring at all.

107. *See* Lessig, *supra* note 5, at 896 (noting that software code can control access to information).

For example, PolicyMaker, a cryptographically based trust management mechanism, illustrates this attribute.[108] PolicyMaker is a language for sophisticated trust management that can certify permissions for both users and actions.[109] PolicyMaker will block the execution of transactions if credentials are not appropriately verified. PolicyMaker checks the authenticity of a cryptographic key (usually that of a particular person) and, before allowing the transaction to proceed, verifies that the keyholder meets a set of criteria required for the transaction.[110] For instance, PolicyMaker can check the validity of a password for an electronic payment order and verify that the password is held by a corporate officer entitled to issue such payment orders.[111] If either the password is fraudulent or the holder does not have the rank permitting payment orders, PolicyMaker blocks execution. This *ex ante* enforcement is implemented automatically using information processing capabilities.

B. Setting Information Flow Rules with Technology

Table 2—Policy Rules and Technologies

Information Flows	Default	Customization	Policy Technology
Content Transmission	Public Identified	Private Anonymous	Cryptography Remailers
Payment Transaction	Identified	Anonymous	E-cash
Web Surfing	Anonymous Identified	Identified Anonymous	Web Browser Masking Sites
Information Distribution	Unrestricted	Pre-screened	PICS Label Filters

108. *See* Matt Blaze et al., *Decentralized Trust Management, in* PROCEEDINGS OF THE IEEE CONFERENCE ON SECURITY AND PRIVACY (Oakland, Cal.) (May 1996).

109. *See id.*

110. *See id.*

111. PolicyMaker, in this example, would authenticate the password of the corporate officer and verify that the officer was authorized to issue a payment order for the amount required by the transaction.

As demonstrated in Table 2, technologies designed expressly for information policy already exist and demonstrate the capabilities and existence of flexible as well as immutable substantive rule features of Lex Informatica. Technologists have specifically designed "privacy enhancing technologies"[112] to customized particular information flow rules. In addition, new policy technologies are under development or are available to facilitate the customized management of information rights in the face of existing technological default rules.

Privacy-enhancing technologies focus on the preservation of confidentiality in the transmission of messages. Many networks, like the Internet, have architectural designs and standards that implement the default rule of open information access. Public key cryptography is a classic example of a privacy-enhancing technology. This technology allows the contents of information to be secured against unauthorized access.[113] Because most network architectural designs do not preclude cryptography, network participants can use it to engage in private communications. Cryptographic choices override the default rule of public disclosure and form a customized rule for the particular users. This customized system configuration may be accomplished by off-the-shelf products such as PGP and RSA or by user-created mechanisms.[114] In any case, once the user chooses to encrypt information, the privacy protection applies throughout the network and is self-executing—ordinarily, only recipients with the proper keys will have access.[115]

Technologies of anonymity also exist to establish network privacy rules for message transmission, electronic transactions, and Internet web surfing.[116] Where network architecture and technical capabilities set the identification of users as a default mandatory transmission rule, participants may nevertheless desire to interact anonymously. Network architecture allows technologies of anonymity to override the standard practice of linking particular senders to messages and thus allows flexibility within the substantive rules governing information flows. For example, electronic

---

112. This terminology has been adopted by several government agencies. *See* INFORMATION AND PRIVACY COMMISSIONER, ONTARIO, CANADA & REGISTRATIEKAMER, THE NETHERLANDS PRIVACY-ENHANCING TECHNOLOGIES: THE PATH TO ANONYMITY (1995).

113. *See* OFFICE OF TECH. ASSESSMENT, U.S. CONGRESS, INFORMATION SECURITY AND PRIVACY IN NETWORK ENVIRONMENTS 113 (1994) [hereinafter INFORMATION SECURITY AND PRIVACY]. Public Key cryptography, or asymmetric cryptosystems, involves two keys: the first to encrypt and a second related key to decrypt. The first of the two keys is publicly distributed, but the second remains private and assures that only the keyholder can decrypt. *See id.* at 38-39.

114. *See id.* at 39. Users may also define their own cryptographic algorithm such as a simple code name to replace an actual identity or a complicated mathematical formula to cipher text. These may be more expensive than existing products.

115. This is not to say that cryptography is fail-safe. If the encryption algorithm is weak or if the keys are not safely stored, unauthorized access to the information may still take place.

116. *See generally* Froomkin, *supra* note 47.

mail messages may be routed through anonymous remailers to mask the identity of the message sender,[117] electronic payment transactions may similarly be structured to anonymize the payor,[118] and even anonymous credit cards can be created through communications networking techniques.[119] These configurations offer customized rules which deviate from the network norm. Like confidentiality technologies, those of anonymity may be used from off-the-shelf configurations or from more elaborately designed arrangements. For example, Internet surfers have a certain degree of "off-the-shelf" anonymity when they visit web sites because only the Server Internet Protocol address[120] is revealed to the site hosting the web page, not the individual user's name.[121] This level of anonymity is, nevertheless, often by-passed by browsers that are configured to reveal user identities.[122] Alternatively, web surfers may choose to surf through several layers of anonymizing sites to assure greater anonymity.[123] One of the Lex Informatica features of these technologies of anonymity is that they operate throughout the network. Anonymization may occur automatically, providing *ex ante* enforcement.

The development of "policy technologies" for information distribution also illustrates the rule-making features of Lex Informatica. These technologies create network-based rules which enhance the access, distribution, and use of information. The basic architecture of the Internet, for example, embodies the default rule of unrestricted information distribution. The PICS technical standard[124] creates a mechanism for pre-screening or modifying the default rule. The Internet architecture allows rating terms and rating labels based on the PICS format to be included in data

---

117. *See* Andre Bacard, *Anonymous Remailer FAQ* (last modified Mar. 27, 1995) <http://www.paranoia.com/drugs/kef/remailer-faq.html>; *see also* Ralph Levien, *Remailer List* (last modified Oct. 23, 1997) <http://www.cs.berkeley.edu/~raph/remailer-list.html> (listing of anonymous re-mailers). A similar technique may be used for anonymous web surfing. *See Your Anonymized Surf Starts Here* (visited Oct. 28, 1997) <http://www.anonymizer.com/open.html>.

118. *See* Froomkin, *supra* note 47, at ¶ 41.

119. *See, e.g.*, Steven H. Low & Nicholas F. Maxemchuk, *Anonymaus Credit Cards*, *in* PROCEEDINGS OF THE 2ND ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY (Fairfax, Va.) (Nov. 2-4, 1994).

120. The Internet Protocol (IP) address is a numeric address that identifies the message server rather than the individual user. IP addresses may also be assigned domain names such as "law.fordham.edu" for easy user recognition. For many users accessing the Internet from an Internet service provider such as America Online or CompuServe, the IP address will be different each time the user logs onto the Internet. This dynamic IP address provides a further degree of anonymity.

121. There may, however, be instances when an IP address or domain name correspouds to an individual user and thus more completely reveals ideutity.

122. Netscape Navigator, for example, reveals the user's identity to web sites if the user has entered the information to the Netscape program.

123. Technological configurations can also be constructed to give the benefits of anonymity to users and the value of personal information to web sites.

124. For a general description of the PICS technology, see *supra* section II(A)(2).

transmissions throughout the network.[125] This technical capability enables individual network participants to set customized rules through filters for the type of information that each participant may receive, rather than forcing a unique restriction on the type of information disseminated throughout the network; and either "off-the-shelf" customizations or intensively designed policies can accomplish this rule-setting. For example, a parent-teacher association may distribute computer disks with suggested filters preconfigured, or parents may tailor their choice of rating terms and screening to their children and their family values.[126]

Similarly, the creation and distribution of rating terms and rating labels for the fair information practices of web sites allows users to set filters to warn of particular practices before disclosing personal information.[127] Combining PICS rating terms and rating labels with filtering software gives users the ability to judge others' use of personal information, customizing the network default policy of total web site control. In essence, filtering provides assurance that a user's information policy matches the policy at a remote site.[128] The PICS-based examples also illustrate the self-executing nature of Lex Informatica. The filtering-software technology performs the permission check prior to displaying content on the user's screen or warns the user of remote-site privacy standards in advance of certain information disclosures.[129]

IV. Applying Lex Informatica

The substantive norms and flexibility of Lex Informatica provide new and useful public-policy tools. Networks challenge traditional legal means to establish ground rules for information access and use. Global access and communications pose extraordinarily difficult jurisdictional dilemmas and choice of law problems.[130] Any particular activity may be subject to

---

125. *See* FTC Testimony, *supra* note 38 (statement of Paul Resnick, AT&T Research).

126. CyberPatrol, for example, offers off-the-shelf screening. *See* Microsystems Software, *Welcome to Cyberpatrol* (visited Sept. 19, 1997) <http://www.cyberpatrol.com/>; *see also* Weinberg, *supra* note 24, at 454-55 (noting that, although a common language for Internet rating systems makes it easier to create ratings and therefore easier for parents to block access, there are drawbacks).

127. Such a label-and-filter mechanism employs the paradigm established by PICS for content-access control. *See supra* notes 26-38 and accompanying text.

128. Additional infrastructure mechanisms, such as independent certification of rating labels, are prerequisites to effective participation by the user in actual information practices. *See* Reidenberg, *supra* note 34.

129. In the case of information privacy, some transaction information will be received by the host web site in order to implement the PICS-based customization. Nonetheless, the use of trusted third-party sites may be used to assure anonymity of this information. *See* Reidenberg, *supra* note 34, Part III.

130. Network actors and activities may be difficult to localize, thus challenging concepts of in personam jurisdiction and applicable law. *See generally* Burk, *supra* note 3 (discussing the jurisdictional problem in the context of United States law); David R. Johnson & David Post, *Law and*

varying national legal standards, and the decentralization of networks creates opportunities to circumvent national laws and evade state enforcement powers. Alternatively, decentralization may impose the most restrictive laws on all global activities. At the same time, harmonization of legal standards is not a realistic solution for global information issues.[131] A legal regulatory regime lacks an important degree of flexibility that the Information Society requires.[132] By contrast, Lex Informatica has a series of valuable characteristics that may flexibly advance information policy goals. The formulation of customized Lex Informatica rules may, to an important degree, avoid many significant difficulties inherent in legal solutions, such as conflict and uncertainty. For example, Lex Informatica offers a new means to deal with the difficult problems that the legal regime faces with Internet content regulation, circulation and abuse of personal information, and preservation of intellectual property interests on global networks.

A. *Advantages of Lex Informatica*

Lex Informatica has three sets of characteristics that are particularly valuable for establishing information policy and rule-making in an Information Society. First, technological rules do not rely on national borders.[133] Second, Lex Informatica allows easy customization of rules with a variety of technical mechanisms.[134] Finally, technological rules may also benefit from built-in self-enforcement and compliance-monitoring capabilities.

1. Jurisdictional Advantages.—The Information Society poses important jurisdictional issues. Network activities may take place on a

---

Borders—The Rise of Law in Cyberspace, 48 STAN. L. REV. 1367 (1996) (distinguishing Cyberspace regulation from other areas of law that are geographically based and arguing that Cyberspace has its own jurisdiction); Symeon C. Symeonides, *Choice of Law in the American Courts in 1995: A Year in Review*, 44 AM. J. COMP. L. 181 (1996) (discussing the complexities of court decisions in the choice-of-law area).

131. The Uruguay Round of GATT negotiations illustrated the difficulty of coordinating international regulation. *See* Final Act Embodying the Results of the Uruguay Round of Multilateral Trade Negotiations, Apr. 15, 1994, 33 I.L.M. 1143 (1994); Agreement Establishing the World Trade Organization, Apr. 15, 1994, 33 I.L.M. 1144 (1994). The negotiations took eight years to complete and still did not resolve thorny issues for international services. Similarly, the TRIPS accord, a major achievement regarding intellectual property that emerged from the Uruguay Round, does not address key questions of the scope of protection for intellectual property. *See* Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Agreement Establishing the World Trade Organization, Annex 1C, 33 I.L.M. 1197 (1994).

132. The Information Society has dynamic and complex characteristics that are at odds with standard regulatory approaches. *See, e.g.*, Reidenberg, *supra* note 2, at 926-30.

133. *See* Reidenberg, *supra* note 2, at 917 (suggesting that national borders are being replaced by network borders).

134. *See infra* section IV(A)(2).

transnational basis. For the legal regime, various national authorities and policymakers may make legitimate claims to regulate users and information flows.[135] However, the very nature of network behavior makes these claims subject to complex choice of law decisions. States are generally reluctant to impose their laws on activities taking place in foreign jurisdictions.[136] Consequently, jurisdiction becomes a critical threshold obstacle to sensible information policymaking.

In contrast, the jurisdiction of Lex Informatica is the network itself. Technologically implemented rules apply throughout the relevant network. As such, Lex Informatica reaches across borders and does not face the same jurisdictional, choice of law problem that legal regimes encounter when networks cross territorial or state jurisdictional lines. Lex Informatica faces conflict of rules at the gateways between networks. If technological standards on both sides of the gateway are interoperable, information flows can cross the gateway without difficulty. When the standards are not compatible, the flows will be impeded by the difference in technical specifications. For example, software modules written for one computer operating system cannot usually function on another operating system. However, the legal regime's choice of law problem forces a selection of one governing law, while both sets of technical rules may be applicable through the use of translations and conversions. In the example of operating systems, software programs exist to translate standards between computer operating systems.[137] This duality feature allows flexibility in accommodating many information policy rule choices simultaneously.

Technical rule formulations for information access may also avoid the risk of liability imposed by conflicting legal rules and may offer solutions for the problem of self-censorship that conflicting content regulation encourages. Policy technologies offer substantive rules in Lex Informatica that shift the issue from censorship, or blocking distribution, to filtering the reception of information.[138] This shift allows different rules to apply to different recipients. Policy decisions about information reception can be made at various levels. Recipients themselves can have the power to make

---

135. The state where access or use occurs, the state where processing takes place, or the state where the server is located may all try to claim jurisdiction.

136. *See, e.g.*, Update Art, Inc. v. Modiin Publ'g, Ltd., 843 F.2d 67, 73 (2d Cir. 1988) (stating that United States copyright law cannot generally be applied abroad); Burk, *supra* note 3, at 1107-32 (recognizing the due process and dormant Commerce Clause limitations on states' ability to regulate activities outside their borders).

137. *See* Computer Assocs. Int'l, Inc. v. Altai, Inc., 982 F.2d 693, 698 (2d Cir. 1992) (describing the program in controversy as an "operating system compatibility component" that translates between operating systems).

138. *See supra* section II(A)(2) (describing PICS filtering technology).

informed decisions about information content.[139] A particular computer may be configured with its own filtering rule. A local area network may have a network-wide policy rule, while an information service provider may adopt a particular rule system-wide. All ISPs in a given country may even have the same filter policy. This flexibility and emphasis on reception means that a unique rule is unnecessary for global distribution of information because distributors in one jurisdiction need not contravene the norms of another jurisdiction.

2. *Customization Advantages.*—Flexibility and customization of information policy are critical for an Information Society. Because activities conducted on global networks may be transnational, network participants need certainty in the rules applicable to their relationships and need to accommodate potentially varying national laws. Legal regimes typically allow for these objectives to be met through freedom of contract.[140] However, freedom of contract is neither absolute nor always an efficient means to deal with network issues. Public-order rights may not be waivable,[141] and the negotiation process for developing an appropriate international contract will either be complex or unlikely to give any choice to individual participants.[142]

Lex Informatica allows customized rules to suit particular network situations and preserve choices for individual participants.[143] Lex Informatica can provide for this flexibility and customization through the adoption of technological standards and configurations that may tailor rules to the precise circumstances or that may empower individual participants to make their own decisions. System-wide configurations may be specified to follow different rules in different national jurisdictions. For example, automatic data purges may be set for European data to comply with data

---

139. *See supra* section II(A)(2).

140. *See* FARNSWORTH, *supra* note 96, § 1.7, at 20-24 (discussing freedom of contract as a historical way of promoting economic activity in the United States).

141. *See id.* § 5.1, at 345-50 (listing reasons why courts will sometimes refuse to enforce contracts based on public policy grounds).

142. On-line service provider contracts, for example, are presented to users on a take-it or leave-it basis. As providers adopt standardized contracts for transnational services, users will encounter fewer choices in their "freedom to contract." Mark A. Lemley, *Shrinkwraps in Cyberspace*, 35 JURIMETRICS J. 311, 321 (1995) (noting that uniform contracts for on-line services would not allow bargaining).

143. Arguably, this advantage may be mitigated by pressures for product standardization that would reduce the desirability of extensive choices. *See, e.g.*, Mark A. Lemley, *Antitrust and the Internet Standardization Problem*, 28 CONN. L. REV. 1041, 1043-54 (1996) (suggesting that network externalities, the advantages of compatibility, and resource commitments all push the Internet toward standardization). However, Lex Informatica customization does not refute product standardization. Lex Informatica customization only requires that the underlying base standard not preclude configuration choices. The desirable product standardization would take the form of default configurations that might nevertheless be modified.

privacy laws[144] but not set in parts of the network where laws do not require it. Alternatively, technological choices may be made to give individuals various configuration options such as PICS-based content screening.[145] Similarly, technological standards may be used to customize rules for transnetwork differences. Protocols exist, for example, to connect on-line service providers such as America Online (AOL) to the Internet.[146] At the same time, technical choices may be developed to accommodate differences in network and national information policy rules. If rules for content evolve differently in various states, users may receive differentiated access.[147] Lex Informatica offers a panoply of opportunities in configuration choice and frequently allows users to override standard system configurations.

Lex Informatica is also distinct from legal regulation because its mechanisms may implement customizations with minimal effort. Technological "filters," for example, assure that a particular rule is applied to information wherever the information goes. Security filters are a paradigmatic illustration such as the use of passwords to access data no matter where the user or data are located. Similarly, technological "translators" provide a significant mechanism to facilitate customization. Translation converts either a rule or a data set from one system to another for execution. For example, one set of PICS content rating labels may be translated into another group's rating scheme.[148] Other translation mechanisms include anonymization of data, use of an anonymous remailer, or encryption-decryption operations.

3. Enforcement Advantages.—For the legal regime, the enforcement capability of rights-holders or states is a serious issue. Legal regulation relies on *ex post* actions against rule violators. However, because of the fluid and global nature of network activities, rule violators will increasingly be difficult to identify, find, and ultimately prosecute. Self-help measures may be available for private parties, such as requiring security bonds or full payment in advance of service or delivery, but these measures can be cumbersome and risky.

---

144. *See* European Privacy Directive, *supra* note 9, at Art. 6 (establishing a limitation on the duration of data storage for personal information).

145. *See supra* section II(A)(2).

146. On-line service providers such as AOL, MSN, and CompuServe all offer Internet access to their subscribers, though the terms of Internet use may be different among the providers. For example, AOL's Internet connection does not give unrestricted access to Newsgroups.

147. Although today the Internet may allow circumvention of access limitations based on geography because a user could log onto the Internet from an unrestricted site, one should not assume that future architectural decisions preclude network segmentation.

148. *Cf.* Stefik, *supra* note 67, at 79 (describing current attempts to develop a formal language for conveying fee information that could then be translated by individual users).

Lex Informatica offers two particularly valuable enforcement advantages. First, technological devices can be readily developed to monitor compliance with both information policy rules and legal norms and to enforce specific policy choices.[149] Technology allows automated monitoring of information access and use, through techniques such as data tagging to identify the applicable rules,[150] data sniffers[151] and search engines, such as AltaVista[152] or Yahoo!,[153] to locate data users or use, and public or accredited private organizations to verify system compliance. Other technologies such as secure viewers and encrypted data provide self-executing enforcement of an information distributor's own data-use restrictions. And second, in contrast to the *ex post* enforcement of legal rules, Lex Informatica relies typically on *ex ante* measures of self-execution. Filters and translations, for example, apply to block information flows that violate the information policy rules. If a PICS-based filter is applied to screen the content of a web page, those pages rated inappropriate for the user will simply not be displayed—only permissible viewing will take place.[154] Likewise, translations such as decryption will only allow execution of actions permissible under the applicable information policy rule. In essence, Lex Informatica has efficient self-help characteristics.

B. *Implications*

The advantages of Lex Informatica give it strength as a policy instrument. Technological configurations allow security wrappers to be placed firmly around information wherever it travels on the network. PolicyMaker, for example, can be used to assure that information is only used by authorized individuals for permitted uses.[155] Technological mechanisms even allow data sources to specify information policies that impose restrictions on the manipulations of information at remote sites.

---

149. Such monitoring would, of course, raise significant privacy concerns.

150. *See About the DOI* (visited Oct. 26, 1997) <http://www.doi.org/about_the_doi.html> (promoting the Digital Object Identifier (DOI) as "a way to link users of the [digital] materials to the rights holders themselves to facilitate automated digital commerce in the new digital environment").

151. *See Sniffer FAQ Version 3.00* (visited Nov. 20, 1997) <http://www.iss.net/vd/sniff.html>. Although packet sniffing is usually conceived as a security threat, the technique may also be used to search for specific data; *see, e.g.*, *Field Exercise Using Snoop*, (visited Nov. 13, 1997) <http://www.vuse.vanderbilt.edu/~apon/courses/cs283s97/assignments/sniffing.html> (class exercise for CS283 course at Vanderbilt University, Spring 1997).

152. *See* Digital Equip. Corp., *AltaVista: Main Page* (visited Sept. 6, 1997) <http://www.altavista.digital.com/>.

153. *See* Yahoo! Inc., *Yahoo!* (visited Sept. 6, 1997) <http://www.yahoo.com/>.

154. *See* FTC Testimony, *supra* note 38 (statement of Paul Resnick).

155. *See supra* note 107. PolicyMaker does not, however, assure "downstream" activities; it only verifies the authority of particular users to perform permitted actions.

Encrypted data may be provided only with a secure viewer, giving the source control over access to "secure" data even at the remote location.[156] These mechanisms are part of the everyday concerns and experiences of technologists; technologists have expertise in designing these systems. With these security features, Lex Informatica offers the possibility of designing enforceable information policy rules on a customized basis throughout networks.[157]

The nuances of Lex Informatica require its use to be a careful exercise. For example, information policy rules located deep within the architecture of networks, such as those built into the transmission protocols, will have greater force than those located at a higher level on servers or user PCs. The higher-level choices, in general, provide more flexibility and greater opportunity to customize information flow policies than rules designed for all network transmissions. However, the flexibility of technological configurations also means that these technologically mediated rules can be circumvented. If configuration choices establishing rules are located on a user's hard drive, users may be able to by-pass the configuration and establish a different rule. For example, a teenager could install a new version of Internet browsing software in order to by-pass parental restrictions installed on the family PC. However, if a technological rule is built into the network software, the possibilities for circumvention may be eliminated. For example, a network protocol could require that content codes be included on all data strings—only information with selected codings would be transmitted to the same teenager who knew how to by-pass the local content filter. The teenager in this instance would not be able to circumvent the network rule.

The power of Lex Informatica to embed nonderogable, public-order rules in network systems is not benign. Once a technical rule is established at the network level, the information policy rule is both costly and difficult to change. All participants in the network must adopt and implement any new rule. At the higher, local level, changes in information policy are easier and likely to be less expensive to modify. Yet pressure will exist for

156. *See* Stefik, *supra* note 67, at 79-81 (describing new techniques and technology that allow publishers to distribute encrypted work that only "trusted" users can view or print). JavaApplets, for example, are programming modules that operate remotely through web browsing software. A data source could package information with a JavaApplet to preserve the source's control of the data at remote locations.

157. One interesting consequence pointed out by Professor Mark Lemley is that different policy rules could, thus, apply to the same conduct by the same person depending on whether the person acted on-line or off-line. *See* Lemley, *supra* note 142, at 318-19. Nevertheless, this is not a cyberspace phenomenon because actions by the same person in different legal jurisdictions might have different applicable legal standards. In contrast, however, technical rules can provide a means to avoid the risk of inadvertently contravening information policies.

standardization to provide convenience and to minimize user confusion. In any case, this decision will rest with local users. However, the cost of change at the local level will be imposed directly on individual users, while change at the network level will be borne directly by network operators. In addition, implementation will affect the success or failure of embedded policy rules.[158] Software bugs and design defects are weak links in Lex Informatica. The deeper these occur in network architecture, the more problematic they are because of the greater difficulty in modifying lower level architecture. The location decision for an information policy configuration is thus significant in many respects.

C. *The Relationship Between Lex Informatica and Legal Rules*

The advantages and implications of Lex Informatica reflect an intersecting relationship between Lex Informatica and law. Lex Informatica may constrain law's ability to deal with a problem. As seen with the present Internet architecture and the very existence of the world wide web, infrastructure decisions that enable multiple paths of communication diminish the territorial authority to address social policy choices unilaterally. Lex Informatica may also substitute for law when technological rules are better able to resolve policy issues.[159] Lex Informatica can, for example, offer content filtering rather than distribution censorship.[160]

Law, nonetheless, has an important place in the elaboration of Lex Informatica. Law may encourage the development of Lex Informatica by imposing liability on various network actors, and law may provide immunity or safe harbors for implementation of technical rules. For instance, in the case of personal information and international privacy rules,[161] a web site that erroneously reports its practices should be subject to both criminal and civil fraud claims, but a web site that is labelled and certified by an accredited third party may enjoy the presumption of satisfying international standards.[162] Similarly, law may sanction the evasion of Lex Informatica. If an embedded information policy is circumvented, then law may intersect to redress this problem by allocating liability for evasions. For example, computer tampering laws can deal

158. For example, Microsoft Internet Explorer 3.0 implements PICS technology, while Netscape Navigator 3.0 does not. This means that PICS technology will be limited by the market share of Internet Explorer 3.0.

159. *See* Lessig, *supra* note 5, at 885 ("Congress's power is contingent upon the available technologies of regulation.").

160. *See* Resnick, *supra* note 31, at 62 (observing that filtering systems such as PICS allow individual users to specify safety and content requirements).

161. *See supra* subpart II(B).

162. *See supra* note 68 and accompanying text.

with the problem of third parties setting up mechanisms to corrupt filtering mechanisms built into web browsers.[163]

In the controversial case of content selection,[164] laws similar to the Communications Decency Act (CDA) in the United States and the recent communications law in France might have also provided this encouragement function in an unexpected fashion. Although initially rejected by their respective national courts, these laws allocated liability to Internet service providers, among others, who distributed indecent material to minors. Opponents of these measures believed them to be unacceptable restrictions on free speech. The United States Supreme Court, in a landmark decision, found the statute overly broad and denounced its restraint of speech on the Internet.[165] In France, the strong rejection of the liability provisions emphasized separation of powers but also reflected concern for speech on the Net.[166] Ironically, the long-term effect of these broadly worded court decisions may be counterproductive for accommodating robust speech and democratic values. While counter-intuitive to ardent supporters of free speech, provisions imposing liability would be unlikely to have a significant censorship effect if they were coupled with a safe harbor for those instituting configuration-choice mechanisms such as PICS-based filtering.[167] Such laws would more likely force a change in the Net's structure, rather than impose serious censorship on the Net's content.[168] Justice O'Connor, in her concurrence, even suggested that the existence of technological tools would give Congress greater regulatory latitude.[169] Because the entire philosophy and present design of the Net is nevertheless geared to maximize information flow, the

---

163. Note that the computer tampering laws would apply to nonauthorized system users. *See* 18 U.S.C. § 1030 (1994); Scott Charney & Kent Alexander, *Computer Crime*, 45 EMORY L.J. 931, 950-53 (1996). If, for example, evasion of NetNanny or SurfWatch filtering mechanisms takes place by the family's twelve-year-old, then the problem should belong to the parents. If a hacker changed the filter mechanism, then the law should sanction the hacker. One should recognize, nevertheless, that the technology must exist before society can say that the parents bear responsibility to prevent their child from replacing the Parent Teacher Association's browser with the Penthouse browser.

164. *See supra* section II(A)(1).

165. *See* Reno v. ACLU, 117 S. Ct. 2329, 2347, 2350 (1997) (proclaiming that the "wholly unprecedented" breadth of the CDA's coverage placed an "unacceptably heavy burden on protected speech").

166. *See* Cons. const., Décision No. 96-378 DC July 23, 1996, *available in* LEXIS, Public Library, consti File, *and in* <http://www.conseil-constitutionnel.fr/decisions/96/96-378.doc>.

167. Though neither the CDA nor the French law provided this type of safe harbor, the scope of the respective court's rejections makes consideration of such an approach extremely difficult as a practical matter.

168. *Cf.* Lessig, *supra* note 5, at 888 (claiming that the current cyberspace arehitecture could be changed to limit access if society desired such change). *But see* Weinberg, *supra* note 24, at 2 (arguing that blocking software might lead to censorship by intermediaries such as employers and librarians).

169. *See Reno*, 117 S. Ct. at 2354 (O'Connor, J., concurring) (suggesting that the availability of technology could offer less restrictive means to address the content problem).

resulting change due to this type of liability measure would most likely be a widespread implementation of Lex Informatica solutions to the pornography issue.[170] Technical solutions would put decisions in the hands of individual citizens—the network users—because the Net community would seek ways to customize the legal allocations of liability.

In any case, the CDA and the French law also illustrate that liability rules do not offer an easy legal solution. Public interest must be significant and, even then, appropriately tailored legislation will be difficult given the variety and fluidity of the Net.[171] Drafting a well-defined liability law will generally pose an extraordinary problem, given that networks create complex situations which tend to necessitate customized rules. To this extent, governments may have no choice but to acquiesce to Lex Informatica solutions.

Despite the initial judicial rejections of the CDA and the French statute, law can still successfully embed an immutable rule in the infrastructure when society has a fundamental principle at stake. The United States's Communications Assistance for Law Enforcement Act of 1994,[172] for example, mandates that new telecommunications switching equipment be wiretap ready.[173] The political process in the United States determined that the police have a fundamental need to obtain access to communications. Responsibility for this information flow policy was allocated to telecommunications companies that in turn had to adopt a Lex Informatica rule at a very low level in their networks. Likewise in France, the Constitutional Court let stand a provision in the telecommunications act requiring service providers to offer technical means to filter access to certain services.[174]

In essence, Lex Informatica and legal rules both parallel and overlap one another. This relationship means that policymakers must add Lex Informatica to their set of policy instruments and should pursue Lex

---

170. PICS, for example, owes much of its existence to Senator Exon and his early draft of the CDA. *See* Resnick, *supra* note 31, at 62 (identifying the impetus of PICS as regulatory avoidance); *PICS Statement of Principles* (visited Oct. 23, 1997) <http://www.w3.org/PICS/principles.html> (adopted in August 1995, before the enactment of the CDA).

171. To the extent that constitutionality may depend on available technologies, statutory legitimacy will be a moving target. *See* Lessig, *supra* note 5, at 888-89 (describing the changing nature of cyberspace); *see also Reno*, 117 S. Ct. at 2349 (suggesting that Congress should have considered technological feasibility).

172. 47 U.S.C. §§ 1001-1010 (1994).

173. *See id.* § 1002 ("[A] telecommunications carrier shall ensure that its equipment . . . [is] capable of . . . enabling the government . . . to intercept . . . all wire and electronic communications . . . ."). Unlike the features of analog conversations transiting copper wires, digitally switched communications over fiber optic cables did not readily offer the capability to monitor particular conversations.

174. Law No. 96-659 of July 26, 1996, art. 15, J.O., July 27, 1996, p. 11384, 11395.

Informatica norms as an effective substitute for law where self-executing, customized rules are desirable.

V. Redirecting Public Policy Strategies

Policymakers should accept and take advantage of the distinguishing features of Lex Informatica and its usefulness for controlling information flows on global networks. Lex Informatica gives policymakers new tools to use in the development of information policy; without these new tools, information flows will marginalize national policymaking authorities. Moreover, working with Lex Informatica places policymakers at the center rather than the periphery of solutions. Lex Informatica must be seen as a distinct source of policy action. Effective channeling of Lex Informatica requires a shift in the focus of government action away from direct regulation and toward indirect influence. The shift can, nevertheless, still preserve strong attributes of public oversight.

A. The Sources of Action

Policymakers are accustomed to traditional avenues for establishing rules through legal regulation. However, legal regulation confronts three tendencies which increasingly marginalize its effectiveness. First, technological developments outpace the rate of legal evolution. Consequently, today's regulations may easily pertain to yesterday's technologies. Second, today's technology may limit the ability of government to regulate. For example, digital networks can no longer be wiretapped like analog phone systems.[175] And finally, information flows may be impervious to the actions of a single government. As pundits have observed, the United States Constitution may just be a "speed bump on the Information Superhighway."[176]

Lex Informatica has very different avenues for rule formation. Lex Informatica's action takes place in standards organizations and in the market place. Standards determine basic architectural features for information policy.[177] Yet, several different processes can result in the adoption of standards.[178] There are formal standards organizations such

175. *See* INFORMATION SECURITY AND PRIVACY, *supra* note 113, at 97 (describing how digital information differs from traditional information in that digital information is "inaccessible to the user without hardware and software tools for retrieval, decoding, and navigation").

176. *See* Mark Lemley, *Romantic Authorship and the Rhetoric of Property*, 75 TEXAS L. REV. 873, 874 (1997) (book review) (referring to the "horrible" metaphors used to describe the information infrastructures and obstacles to information flows).

177. *See supra* subpart III(A).

178. *See* Lemley, *supra* note 143, at 1054-59, 1079 (noting how standards can result from a single firm's success in a competitive market or from a collaborative industry accord to utilize one standard).

as those in Europe[179] as well as important industry consortia such as Committee T1 in the United States.[180] Market forces influence the acceptance of configuration standards, and pressure from both industry representatives and consumers can affect the direction of standards-setting.[181]

B. Shifting Focus

With the technical arena serving as a critical source of information policy through Lex Informatica rule-making, government policymakers must shift their focus if they wish to contribute effectively. The promotion of technical standards must become a key goal. Because technical designs and choices are made by technologists, government policymakers should play an important role as public policy advocates promoting policy objectives. This involves a shift in goals, instrumentalities, and institutions for policymakers.

1. Goal Shift.—Lex Informatica should shift the focus of policymakers away from specific policy-rule content and toward greater flexibility. In general, flexibility is only undesirable when fundamental public interests are at stake and the public interest requires rules that individual participants in the network might not choose themselves.[182] Policymakers should thus become advocates for flexible standards that allow for individual policy choices through customization of configurations. By promoting flexible standards, policymakers advance the capability to establish information policy rules rather than attempt a specific exercise of government power to impose a particular substantive decision. Policymakers must be involved early in the development phases of new technologies to assure that options and flexibility are maximized.[183] This

---

179. *See* Commission of the European Communities, Communication from the Commission to the Council and the European Parliament: On "Standardization and the Global Information Society: The European Approach," COM(96)359 (final) at 4 ("Formal standards organi[z]ations in Europe, recogni[z]ed by law at [the] European level . . . are CEN, CENELEC, and ETSI." (citation omitted)), *available in Standardization and the Global Information Society* (visited Nov. 14, 1997) <http://www.ispo.cec.be/infosoc/legreg/docs/96359.html>.

180. T1, a privately sponsored organization accredited by the American National Standards Institute, "develops technical standards and reports regarding interconnection and interoperability of telecommunications networks at interfaces with end-user systems, carriers, information and enhanced-service providers, and customer premises equipment." Standards Comm., T1 Telecomm., *T1 Overview* (visited Sept. 14, 1997) <http://www.t1.org/html/intro.html>.

181. *See* Lemley, *supra* note 143, at 1055 ("[I]f companies competing to set an industry standard are offering different technology, this competition may serve a temporary market-disciplining purpose, allowing consumers to choose the best technical standard on a one-time basis.").

182. Essentially this means that flexibility does not work when the public interest would otherwise prohibit freedom of contract.

183. If policymakers arrive late in the development phase, the inertia and committed interests of the developers may seriously hamper any significant changes.

involvement does not entail policymakers' seeking to control the design of new technologies, but this involvement does mean that they instead should become partners in the development of system capabilities.[184]

Policymakers must emphasize the creation of an incentive structure both that encourages new developers to design technologies with information flow flexibility and that offers incentives for the implementation of technologically mediated information policy rules.[185] For example, new choices in privacy-enhancing technologies are likely to come from entrepreneurial developers. PICS-based filtering will only become a robust instrument in the context of information privacy if authors emerge to write rating terms, services emerge to assign rating labels, and an infrastructure is established that would support the rating terms and rating labels on the Internet.[186] Similarly, confidence in PICS filtering for information privacy will rely on the creation of certifying agents. Government can create both positive and negative incentives to stimulate such technology development and implementation. Threats of liability tend to be an effective negative stimulus for industry, while favorable tax treatment or publicity often act as positive incentives.[187] Government may also begin to look more carefully at accreditation as a way to both channel technological developments toward public policy goals and to reward developers.

2. *Instrumentality Shift.*—Policymakers have six significant approaches to influence the development of technical designs: (1) the bully pulpit, (2) participation, (3) funding, (4) procurement, (5) regulated behavior, and (6) regulated standards. For the development of Lex Informatica information policy rules, policymakers must use strategies and mechanisms that are different from traditional regulatory approaches.

Government can use the bully pulpit approach to threaten and cajole industry to develop technical rules. For example, in the context of

184. I am indebted to Professor Lessig for pointing out that such indirect regulation raises normative issues regarding the exercise of government power. The appropriate role of democratic government in a technologically mediated society is beyond the scope of this Article, but an important subject of future work.

185. This point does not suggest that governments must abdicate responsibility to others, but rather that this instrumentality—the creation of incentives for technical choices—may be far more effective in achieving desired policy results than a difficult to draft and hard to enforee piece of legislation such as the Communications Decency Act. *See supra* note 165.

186. Professor Weinberg nevertheless argues that any PICS-based rating system will be skewed against the distribution of information. *See* Weinberg, *supra* note 24, at 477 (explaining how blocking software can block desirable information). He ascribes an implicit illegitimacy to all rating labels because of an inherent subjective element. If arguably there is such an illegitimacy, it should become irrelevant when a user freely chooses to adopt the particular rating terms, preferences, and rating labels with knowledge of their meaning and creation.

187. A company will seek to avoid liability or shift its risk while striving to take advantage or qualify for favorable tax treatment.

children's programming, the Senate sought to encourage video games producers to restrain the dissemination of violent programming to children.[188] Hearings resulted in an industry decision to create and adopt the RSAC[189] and ESRB[190] systems—two competing rating systems that allow parents to restrict their children's access to inappropriate material. The government's bully pulpit resulted in a flexible mechanism that can provide an information policy rule customized by network participants rather than an immutable architectural rule. The resulting rating systems can let parents choose filtering rules without prohibitions on the network's dissemination of particular content.

The participation approach requires government to work with standards bodies to help develop technical rules. The Canadian Standards Association Code for the Protection of Personal Information reflects this approach.[191] The Canadian Standards Association worked with stakeholders from government, industry, and consumer groups to define the standard that was ultimately adopted as a Canadian standard.[192] Representatives from all sides participated in the actual negotiations.[193]

Policymakers often have significant influence through public funding decisions. The power of the purse can encourage the development of particular technological capabilities. For example, the present Internet routing structure owes its birth to the specifications established by the U.S. Defense Department. Funding for ARPANET, the precursor to today's Internet, sought a network that would preserve communications in the event of local disruptions or a nuclear attack on the United States.[194] The network thus automatically routes around problems and bottlenecks.

Government can also use its power to make the public interest voice heard through public sector procurement. The government's massive purchasing power can adopt particular standards. For example, the U.S. government adopted as a federal standard the Data Encryption Standard

---

188. *See* Laura Evenson, *Video Game Makers Pledge to Set Up Ratings System*, S.F. CHRON., Dec. 10, 1993, at B1.

189. *See* Recreational Software Advisory Council on the Internet (visited Sept. 14, 1997) <http://www.rsac.org/> (describing the RSAC's mission as the empowerment of "the public, especially parents[,] to make informed decisions" about electronic media).

190. *See* Entertainment Software Rating Bd., *ESRB—Parent's Gaide* (visited Sept. 14, 1997) <http://www.esrb.org/parent.html> (illustrating the ESRB's goal to inform parents about the "high-tech environment of the nineties").

191. CAN/CSA-Q830-1996, Model Code for the Protection of Personal Information (Mar. 1996) <http://www.csa.ca/83000-g.htm> [hereinafter CSA Code]; *see also* Colin Bennett, *Privacy Codes, Privacy Standards and Privacy Laws: The Instruments for Data Protection and What They Can Achieve*, *in* VISIONS FOR PRIVACY IN THE 21ST CENTURY (Colin Bennett ed., forthcoming 1998).

192. *See* CSA Code, *supra* note 191.

193. *See id.*

194. *See* Andrew Zimmerman, *The Evolution of the Internet*, TELECOMMUNICATIONS, June 1997, at 39, 40, *available in* LEXIS, Nexis Library, CURNWS File.

(the famous "DES") originally developed by IBM.[195] As a result, if the government needed encryption, the products it used had to incorporate the DES. This adoption had an important ripple effect on the private sector. The government's reliance on the standard gave a certain imprimatur to the DES, and the private sector consequently adopted it as a security standard.[196]

The regulated-behavior approach provides an indirect but significant stimulus to Lex Informatica norm-construction. Here the government can require or prohibit particular activities like the distribution of pornography[197] or the unauthorized electronic transfer of money.[198] Behavior regulation leads to a search for the means to assure conforming practices. Technical rules can become a cornerstone of that assurance.

Finally, policymakers may regulate particular technical standards. For example, both the Communications Assistance for Law Enforcement Act's (known as the Digital Telephony Act)[199] mandate of wiretap-ready capabilities for telecommunications switching equipment and the Clinton Administration's unsuccessful attempt to impose the Clipper Chip[200] for access to private communications have looked to set immutable rules in the basic network architecture. By forcing the technical rule lower in the network protocol, policymakers can reduce the possibilities of circumvention of the Lex Informatica default.

The six different mechanisms for policymakers to influence Lex Informatica each present different attributes. A traditional regulatory solution, like government mandated standards, will be the hardest to accomplish because it requires the government imposition of an immutable rule in the network infrastructure. In contrast, the bully pulpit approach and the regulated behavior approach provide greater leeway for network-driven solutions. Other approaches, such as funding, procurement, or especially participation, encourage the incorporation of public policy objectives in the heart of system design and market adoption. In situations in which public goals call for mandatory rules, policymakers may use combinations of the various approaches to increase their effectiveness. For example, if the policy goal is to incorporate an intellectual property rights management system that is difficult to evade, the system must be

195. *See* OFFICE OF TECHNOLOGY ASSESSMENT, *supra* note 113, at 121-22 (noting the adoption of DES as a federal encryption standard).

196. *See id.* (noting that the banking industry adopted the DES standard).

197. *Reno v. ACLU*, 117 S. Ct. 2329 (1997), did not strike down the portions of the Communications Decency Act relating to obscenity.

198. *See* 15 U.S.C. §§ 1693g-1693h (1994).

199. 47 U.S.C. § 1001 (1994).

200. Clipper Chip is a proposed encryption tool for electronic communications that would allow access to information content by law enforcement.

incorporated with sufficient security at various places in the network. Government participation in the standards-creation process can assist the development of a technical standard accepted by all network actors—one that adopts, for example, mandatory rather than optional data fields for rating labels.[201] Governmental influence may be supported by behavior regulation, namely the imposition of liability if technical means are not adopted to manage intellectual property rights.[202]

3. The Institutional Shift.—The shift in focus toward technical standards as a source of policy rules emphasizes technical fora whose institutions are not normally associated with governance. The Internet Engineering Task Force,[203] the Internet Society,[204] the World Wide Web Consortium,[205] and traditional standards organizations like ISO,[206] ETSI,[207] and committees like T1[208] are the real political centers of

---

201. This would mean that transmission could not occur without a rating label and would facilitate widespread implementation of a particular Lex Informatica rule.

202. This means that users or distributors of browsers might be liable for infringement if the browser does not recognize management codes for intellectual property rights. It does not mean that users should be prohibited from anonymous browsing or fair uses of copyright protected material.

203. The Internet Engineering Task Force is a self-selected organization that is the "protocol engineering and development arm of the Internet" composed of network designers, operators, vendors, and researchers. *See* Internet Eng'g Task Force, *Glossary* (visited Aug. 30, 1997) <http://www.ietf.org/glossary.htm#IESG>; Internet Eng'g Task Force, *Overview of the IETF* (visited Aug. 30, 1997) <http://www.ietf.org/overview.html>. The IETF engages in the development of new Internet technical standards.

204. The Internet Society, ISOC, is a non-governmental international organization that seeks to coordinate internetworking technologies and applications for the Internet. *See* Internet Soc'y, *What Is the Internet Society?* (visited Sept. 14, 1997) <http://www.isoc.org/whatis/index.html>. ISOC promulgates voluntary standards for the Internet that have been developed by the Internet Engineering Task Force and approved by the Internet Engineering Steering Group (or, in disputed cases, the Internet Arehitecture Board). *See* Internet Soc'y, *Internet Society Standards Page Index* (visited Sept. 14, 1997) <http://www.isoc.org/standards/index.html>.

205. The World Wide Web Consortium (W3C) is an international industry consortium run jointly by the MIT Laboratory for Computer Science in the United States and the Institut national de recherche en informatique et en automatique in France that seeks to promote standards for the evolution of the Web and interoperability between WWW products. *See* World Wide Web Consortium, *About the World Wide Web Consortium [W3C]* (visited Sept. 14, 1997) <http://www.w3c.org/Consortium/>. W3C produces specifications and reference software. *See id.*

206. The International Organization for Standardization (ISO) in Geneva is a world wide federation of national standards bodies from approximately one hundred countries. Its objective is "to promote the development of standardization and related activities in the world with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological and economic activity." International Org. for Standardization, *Introduction to ISO: What Is ISO?* (visited Sept. 14, 1997) <http://www.iso.ch/infoe/intro.html>. ISO's work results in international agreements which are published as standards. *See id.*

207. The European Telecommunications Standards Institute sets voluntary telecommunications standards for Europe and cooperates with the European Broadcasting Union and CEN/CENELEC for broadcasting and office information technology standards. *See* European Telecommunications Standards Inst., *ETSI Statutes* (last modified Sept. 10, 1997) <http://www.esti.fr/adm/rules/statute.htm>.

208. *See supra* note 180.

Lex Informatica. Yet these groups are generally not governmental organizations. Rather, they tend to be consortia of interested persons and companies.[209]

For the moment, standards bodies tend to be loosely organized and have few, if any, universal requirements for membership other than enough money to attend the various meetings. The organizations generally make decisions by consensus. When the network community was small and homogeneous, this process worked well. However, it is unlikely that the consensus model will persist to function effectively because global networks now reflect more diverse interests. The commercial politics that drove standards organizations will be succeeded by far more politicized social politics. This evolution is likely to make the technical tasks of standards bodies more difficult to accomplish. The technical community, willingly or not, now has become a policy community, and with policy influence comes public responsibility. Policymakers by necessity must pay closer attention to the activities of these organizations, and they must participate more aggressively if they wish to push technical developments in a direction responsive to public goals and the need for customization capabilities. Policymakers should argue for particular technical capabilities and functions that will incorporate public objectives (*i.e.*, what the network can and should do), while leaving the specifics of the protocols to the engineers (*i.e.*, how the infrastructure will provide the capabilities and functions). This task will not be easy because the policy and technical communities have very different cultures.

Finally, in addition to formal standards organizations, technical decisions can be effectively influenced by ideas generated outside of the organization structures. Culturally, engineers start designing when presented with particular goals. Engineers therefore tend to be receptive to presentations that state the public goal as a design objective. For this reason, policymakers can and must engage and participate in nontraditional fora. Conference speeches, workshops, and interest group meetings thus become key tools of influence impacting the direction of Lex Informatica development. In essence, the dynamics of Lex Informatica change the types of activities in which government should be engaged.

VI. Conclusion

Lex Informatica is an existing complex source of information policy rules on global networks. Lex Informatica provides useful tools to formulate rules customized for particular situations. Lex Informatica

209. The membership of these organizations by and large reflects domination of industry representatives.

allows the coexistence of varying information policies in a heterogeneous environment. The pursuit of technological rules that embody flexibility for information flows maximizes public policy options; at the same time, the ability to embed an immutable rule in system architecture allows for the preservation of public-order values. These tools can lessen a number of problems that traditional legal solutions face in regulating the Information Society. Yet a shift in public policy planning must occur in order for Lex Informatica to develop as an effective source of information policy rules. The new institutions and mechanisms will not be those of traditional government regulation. Policymakers must begin to look to Lex Informatica to effectively formulate information policy rules.