

CYBERSPACE TECHNOLOGICAL STANDARDIZATION: AN INSTITUTIONAL THEORY RETROSPECTIVE

By Daniel Benoliel[†]

ABSTRACT

Acknowledging the value of standard-setting, the Clinton administration originally made “industry self-regulation” the guiding principle for standardizing the Internet. The succeeding administration continues to use this approach. Nonetheless, historical analysis of the last two decades shows that industry self-regulation has not always been a coherent policy. Rather, it has become a rhetorical device used to legitimize the government’s agendas, particularly the mandated design of cyberspace’s architecture and infrastructure. To date, there are still too many inconsistencies in the government’s formal standardization policies. For example, the government’s policy of centralizing early infrastructure standards to mandate cyberspace’s architecture is in tension with its actions aimed at privatizing the Internet’s funding and governance. These contrasting policies demonstrate that “industry self-regulation” of cyberspace has actually included a large measure of government intervention.

This paper is a historical and conceptual assessment of the government’s standardization policies using a comparative institutional theory approach. After assessing standardization policies, this study considers the unique, multi-layered architecture of cyberspace to identify which institutional body should standardize the Internet. To do so, this study identifies a distinctive production process for cyber standards that distinguishes between the standardization of early infrastructure and the standardization of complementary applications.

© 2003 Daniel Benoliel

[†] J.S.D. candidate, University of California at Berkeley, School of Law (Boalt Hall). A version of this paper won first prize in the 30th Telecommunications Policy Research Conference (“TPRC”) Graduate Student Article Competition and was later presented at that conference and at the John M. Olin Law and Economics Workshop Seminar, at Boalt Hall. For their most helpful comments and support, I am indebted to Mark Lemley, Pamela Samuelson, Edward Rubin, David Post, Stuart Benjamin, Hal Varian, Bob Cooter, Jesse Fried, Dan Hunter, Polk Wagner, Jane Winn, and the participants at both fora. I am also grateful for the generous advice I received from Carl Cargill and Roger Martin from Sun Microsystems, Inc. Any inaccuracy in this paper is my own responsibility. For further questions or comments, please contact me at: Daniel_b@boalhall.berkeley.edu.

This study concludes with a set of policy rules. These rules are proposed with a caveat: cyberspace's present successful institutional regulative reality might not be preserved into future technological generations unless distinctive policies are maintained both sequentially in compliance with the technological standardization lifecycle, and contextually in compliance with the different categories of standards.

TABLE OF CONTENTS

I.	INTRODUCTION	1261
II.	THE TECHNOLOGICAL TRIPLE SCRUTINY ANALYSIS: TIME, SPACE, AND INSTITUTIONAL IDENTITY	1266
	A. IT Standards: The Methodological Framework.....	1266
	B. The Technological Lifecycle: The Criterion of "Time"	1267
	C. Cyberspace's Architectural Edifice: The Criterion of "Space"	1272
	1. <i>The Normative Framework</i>	1272
	2. <i>Infrastructure Standards</i>	1276
	3. <i>Application Standards</i>	1279
	D. Standard-Setting Institutions: The Criterion of "Institutional Identity"	1280
III.	THE INFRASTRUCTURE DEVELOPMENT PHASE: A POLITICAL INSTITUTIONAL INEVITABILITY	1285
	A. Infrastructure Telecommunications Services: The Collective Choice Analysis.....	1285
	B. Infrastructure Standardization: The Cost-Benefit Analysis.....	1293
	1. <i>Administrative Costs</i>	1295
	a) Quality Standardization Costs	1295
	b) Development Costs.....	1298
	c) Information Costs	1299
	2. <i>Compliance Costs</i>	1301
	a) Variety Reduction Costs.....	1301
	b) Coordination Costs	1305
	3. <i>Indirect Costs</i>	1308
IV.	THE MODIFICATION PHASE: THE COMMERCIALIZATION OF CYBER STANDARDS .	1309
V.	THE IMPLEMENTATION PHASE: THE RISE OF AUTONOMOUS INSTITUTIONS.....	1313
	A. Application Standardization: The Cost-Benefit Analysis.....	1314
	1. <i>Administrative Costs</i>	1315
	a) Eliminating Duplicative Efforts.....	1315
	b) Reducing Search Costs	1317
	2. <i>Compliance Costs</i>	1318
	3. <i>Indirect Costs</i>	1321
	B. Government Intervention	1323
	1. <i>Direct Intervention: The Problem of Efficiency</i>	1323
	2. <i>Indirect Intervention: Roles of Government Regulation</i>	1326
	a) Regulate Production Supervision Rules	1327
	b) Regulate the Process of Standardization.....	1329
	C. A Potential Deviation: The ICANN Case Study	1331
VI.	CONCLUSIONS	1336

I. INTRODUCTION

The regulative technique commonly known as technological standard-setting is one of the most effective ways to regulate cyberspace and shape its markets.¹ This regulative technique is too often seen as an overly technical discipline and has been neglected as a field of research on cyberspace regulation. Technological standard-setting has been given too little attention, both as an independent field of regulation theory and, more specifically, as a means of governing network environments such as the Internet.

As with other technological fields of mass media standardization,² cyberspace has reached the degree of comprehensiveness that makes it worthy of a wider perspective of comparative institutional analysis³ than has been given to it by the U.S. government. Notably, rather than conducting a principled analysis of the appropriate standardization approach to the Internet, the Federal Communications Commission ("FCC") has divided the network environments into incomplete legal categories by adopting the "basic" and "enhanced" service classifications prior to the widespread adoption of the Internet.

Overall, efforts to set standards in cyberspace have occasionally been ambiguous and inconsistent. The government's conflicting policies demonstrate this inconsistency. On one hand, government seeks to privatize the Internet's funding and governance particularly through the Internet Corporation for Assigned Names and Numbers ("ICANN") self-regulation

1. On the standardization discipline as an independent form of regulation, see STEPHEN BREYER, *REGULATION AND ITS REFORM* 96 (1982) (for an economic perspective); ANTHONY I. OGUS, *REGULATION: LEGAL FORM AND ECONOMIC THEORY* 150 (1994). See also CARL F. CARGILL, *OPEN SYSTEMS STANDARDIZATION: A BUSINESS APPROACH* 26-29, 137-38 (1st ed. 1997) (for an information technology ("IT") perspective); Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 EMORY L.J. 911, 918, 927-28 (1996) [hereinafter Reidenberg, *Governing Networks*] (concluding that standards in cyberspace embed policy choices, thus supplementing legal rules); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 570-72 (1998) [hereinafter Reidenberg, *Lex Informatica*] (for the cyberspace context).

2. For example, broadcast, cable and satellite, TV, and radio.

3. On the need for technological comprehensiveness for standard-setting, see, for example, MARTIN C. LIBICKI, *INFORMATION TECHNOLOGY STANDARDS: QUEST FOR THE COMMON BYTE* 16-18 (1995); Tineke M. Egyedi, *Institutional Dilemma in ICT Standardization: Coordinating the Diffusion of Technology*, in *INFORMATION TECHNOLOGY STANDARDS AND STANDARDIZATION: A GLOBAL PERSPECTIVE* 57 (Kai Jakobs ed., 1999); Ole Hanseth & Eric Monteiro, *Participatory Standardization of Information Infrastructure*, in *INTERNATIONAL PERSPECTIVES ON INFORMATION SYSTEMS: A SOCIAL AND ORGANISATIONAL DIMENSION* 174 (Savvas Katsikides & Graham Orange eds., 1998).

case study, while on the other, it still seeks to centralize and even monopolize the Internet's infrastructure standard-setting activities.

The commercialization, widespread use, and development of peripheral standardized software products for the Internet raise the question of who should standardize the Internet. One can answer this question by comparing the experience of analogous technological fields and retrospectively examining the experience of the Internet over the last two decades.⁴ This study undertakes this examination while confronting the unique progress of what is essentially a technological standardization process.

This study proceeds from Neil Komesar's comparative institutional theory insight. Komesar acknowledges that all standardization institutions are subject to both internal and external imperfections, and that only a comparative approach vis-à-vis the identical assignments should prevail.⁵ Accordingly, although an institution may function inefficiently, alternative institutions may function even worse. By the same token, even when the intrinsic worth of an institution might be apparent, alternative institutions may perform the same task more effectively.⁶ Thus, upon examining the market's ability to self-standardize cyberspace, the operative question is not how well the market functions, but whether political institutions, such as government branches and other autonomous institutions like industry standardization organizations, could produce a better outcome.

This study focuses predominantly on the relationship between institutional analysis and standardization *production* policy as an ex ante regulative mechanism.⁷ In addition, commercial implementation of a new technology with legal or technological standards can be viewed through the more general prism of regulation theory in cyberspace. Thus far, the ongo-

4. On the importance of precedents in designing standardization policies, see, for example, BREYER, *supra* note 1, at 99; JASON OXMAN, THE FCC AND THE UNREGULATION OF THE INTERNET (FCC OPP, Working Paper No. 31, 1999), available at http://www.fcc.gov/pub/Bureaus/OPP/working_papers/oppwp31.pdf (last visited Dec. 18, 2003); KEVIN WERBACH, DIGITAL TORNADO: THE INTERNET AND TELECOMMUNICATIONS POLICY (FCC OPP, Working Paper No. 29, 1997), available at http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp29.pdf (last visited Dec. 18, 2003). Werbach cautions that there is reason to believe that analogies to familiar services may not be appropriate for the Internet due to real "category" difficulties. Henceforth, any such analogy will derive from the proposition of contextual analysis, unless claimed otherwise.

5. NEIL K. KOMESAR, IMPERFECT ALTERNATIVES: CHOOSING INSTITUTIONS IN LAW, ECONOMICS, AND PUBLIC POLICY 3-10 (1996).

6. *Id.*

7. An alternative approach would be to look at telecommunications policy ex post by examining the implications of antitrust and intellectual property law.

ing debate has focused on application standards as a regulative constraint, and has overshadowed the separate debate concerning system-oriented infrastructure standards.⁸ In the latter forms of discourse, any institutional choice is mostly a reflection of an earlier pursued policy or defined “rights,” for example, both Lessig’s constitutional urge for reducing “code control” and Johnson and Post’s freedom for regulative multiplicity. Institutional choices are mostly a reflection of an earlier pursued policy of defined legal rights.⁹ As a result, current discourse on institutional choices places legal and other normative principles above the political *production* process and costs.

The Komesarian proposition, on the other hand, suggests that the mere reflection of any social goals and “rights” on institutional choices is largely insufficient because such goals tautologically embed institutional choices of their own.¹⁰ Accordingly, social policy should become relevant only upon consideration of the proper institutional constraint.¹¹ This study follows Komesar’s theory and suggests that any institutional choice should be seen as an integral part of the general technological goal and not merely as its reflection. Indeed, the structure of cyberspace’s regulative institutions profoundly affects the prevalence and form of information technology (“IT”) standards.

8. See, e.g., LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* 101-02 (1999) (explaining that his book and the present regulative discussion is and should be aimed at the standardized application layer); see also Llewellyn J. Gibbons, *No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace*, 6 CORNELL J.L. & PUB. POL’Y 475, 481-87 (1997) (using the term cyberspace “infrastructure” while focusing on “application” standards, like e-mail or the World Wide Web, instead); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1382-91 (1996) (examining standardized applications for example, copyright and trademark regimes as the point of reference in their regulative argument); Timothy Wu, *Application-Centered Internet Analysis*, 85 VA. L. REV. 1163, 1164 (1999) (“[T]he whole Internet is rarely an appropriate level on which to generalize. Instead, legal thinking can better focus on where the variation that is apparent to the user is actually found: the application layer above the Internet’s basic protocols.”). See generally Dan L. Burk, *Federalism in Cyberspace*, 28 CONN. L.R. 1095 (1996) (focusing on consumer protection applications and other public laws to police online behavior and commerce). For a skeptical view of this trend, see CARL SHAPIRO & HAL R. VARIAN, *INFORMATION RULES: A STRATEGIC GUIDE TO NETWORK ECONOMY* 317-18 (1999) [hereinafter SHAPIRO & VARIAN, *INFORMATION RULES*].

9. LESSIG, *supra* note 8; Johnson & Post, *supra* note 8.

10. KOMESAR, *supra* note 5, at 43 (arguing that “calling something a “right” is an institutional statement”).

11. *Id.* at 271.

Based on the proposition that any institutional choice should be seen as an integral part of the general technological goal rather than a reflection of a previously pursued static policy or right, this study introduces a multi-layered production process for technological standardization. This study thus offers an alternative synthesis to the existing top-bottom, bottom-up and industry standardization organization's single-layered regulation models.¹² In general, all of the existing approaches seem to fall short with respect to the critical factor of *timing* because they fail to properly acknowledge the evolving nature of technological environments.

Technological environments such as cyberspace have processional nature. This study echoes that procession by measuring the strengths and weaknesses of each of these single-layered regulatory models in each sequential phase. It does so by looking at variations in the types of standards located on different layers of technical architecture from one production stage to the next. Overall, the institutional selection of a standard setter for each phase will be only a transitory choice among highly imperfect alternatives. Lastly, this study confronts the distinctive costs of standardization. These costs are found outside the partial scope of its institutional participatory process. Thus, this study suggests that whenever strict legal process analysis falls short in supplying policy makers with a comprehensive result, any institutional choice should be subject to production costs that exist beyond the participatory process *per se*.¹³ This study also departs from the supported proposition that current law and economics may be seen to share a joint objective and importance in standardizing cyberspace. As a result, a preliminary cost-benefit analysis is outlined in Parts II-V.

12. *Id.* at 6 (suggesting that, originally, the available institutions are political institutions i.e., executive and legislative branches of government, market and the courts). However, the cyberspace technological environment includes, in practice, additional autonomous institutions such as industry, group consortia, etc., while minimizing the role of courts. See discussion *infra* Part II.D. See generally JOSEPH FARRELL & GARTH SOLANER, COMPETITION, COMPATIBILITY AND STANDARDS: THE ECONOMICS OF HORSES, PENGUINS AND LEMMINGS (Univ. of Cal. Berkeley Dep't of Econ., Working Paper No. 8610, 1986).

13. See Edward L. Rubin, *The New Legal Process, the Synthesis of Discourse, and the Microanalysis of Institutions*, 109 HARV. L. REV. 1393, 1394, 1411-13, 1425-37 (1996) (supporting a comprehensive synthesis to law and economics and the legal process movements for comparative institutional analysis); see also JAMES G. MARCH & JOHAN P. OLSEN, REDISCOVERING INSTITUTIONS 1-2, 16-19 (1989); PAUL J. DIMAGGIO & WALTER W. POWELL, *Introduction to THE NEW INSTITUTIONALISM IN ORGANIZATIONAL ANALYSIS* 11-15 (Paul J. DiMaggio & Walter W. Powell eds., 1991); Neil K. Komesar, *Exploring the Darkness: Law, Economics, and Institutional Choice*, WIS. L. REV. 465, 466-71 (1997).

To narrow the conceptual framework of this study, Part II opens by examining how an IT standard becomes defined. It continues by defining the three technological benchmark criteria of the standardization realm: time (referring to the processional technological lifecycle), space (referring to cyberspace architecture, established by different types of technological standards), and institutional identity (referring to which institution is best situated to define, implement, and maintain standards). This sets forth a triple scrutiny analysis for the appropriate institutional choice in each of cyberspace's distinctive standardization phases.

Part III begins with the first of three standardization phases: the *infrastructure development* phase. New platform technology is typically introduced in this early technological phase, beginning with its evolution from an idea to the development of a basic system product or process. This creates the content of the first standardized infrastructure technology. In this early phase, central political institutional control, in the form of mandated government intervention in infrastructure standardization, for example, is inevitable.

Part IV continues to the *modification* phase and explains how rapid innovative changes were made to cyber technology. These changes were followed by extensive bargaining and modifications to support commercial use of Internet technology. These changes are what led to the third, and current, commercial standardization phase of the technological generation.

Part V describes the concluding technological *implementation* phase. Whenever technology matures, the explosion of new markets for both early core Internet telecommunications services and markets for application and conforming standardized products evolve and should promote the rise of autonomous standard-setting institutions. Part V also presents four arguments in support of this paper's comparative institutional analysis. The four arguments touch upon 1) standardization's chilling effect on governmental intervention, 2) government's supposedly limited direct role in application standardization, 3) government's indirect regulatory and supervisory roles in standardization, and 4) the ICANN lesson.

Part VI enunciates several suggestions as policy rationales for future technological generations in cyberspace. The main conclusion is that the unprecedented development of cyberspace provides theoreticians and decision-makers alike with a feasible opportunity to develop a comprehensive, time- and context-based institutional standardization policy. Furthermore, choosing the optimal standardization institution for each technological phase has three-fold significance in cyberspace institutional theory. First, a rational standard setter should be able to predict efficiently the de-

gree of compliance of each such standardized technology by recognizing different phases of technological development and different standardization institutions. Second, the rise of different types of IT standards demands transitory regulatory conduct for the different technological phases. Third, a comprehensive institutional framework can be established for future technological generations in cyberspace.

II. THE TECHNOLOGICAL TRIPLE SCRUTINY ANALYSIS: TIME, SPACE, AND INSTITUTIONAL IDENTITY

A. IT Standards: The Methodological Framework

Typically, there are two technical criteria used to define IT standards, such as the standards used in regulating cyberspace. First, a technological standard is primarily viewed with respect to the degree of its technical maturity. That maturity is most commonly assessed through a technological standardization process.¹⁴ Second, an IT standard is quantified as a function of its acceptance by the relevant market.¹⁵ This measurement is assessed through the intensity and the breadth of the standard's recognition and its use by consumers. That estimate typically derives from the recognition that the specified protocol or service provides significant personal and social benefits to users and the market respectively.

14. See Scott O. Bradner, *The Internet Standards Process—Revision 3*, RFC 2026 (IETF Network Working Group, Harvard University Oct. 1996) [hereinafter Bradner, *Internet Standards Process*] (noting that “specifications that are intended to become Internet Standards evolve through a set of maturity levels known as the ‘standards track’”), at <http://www.ietf.org/rfc/rfc2026.txt> (last visited Dec. 18, 2003). Eventually, the Internet Engineering Task Force defined these maturity levels as: “Proposed Standard”, “Draft Standard”, and “Standard”. *Id.* at § 4; see also FLOYD WILDER, A GUIDE TO THE TCP/IP PROTOCOL SUITE 368-70 (2d ed. 1998); *Internet Official Protocol Standards*, RFC 1800 (John Postel ed., IETF Network Working Group & Internet Architecture Board) (providing an earlier description of the maturity levels), at <http://rfc.sunsite.dk/rfc/rfc1800.html> (last visited Dec. 18, 2003); William J. Clinton & Albert Gore Jr., *A Framework for Global Electronic Commerce* (1997) [hereinafter Clinton & Gore, *A Framework*] (concluding that “[p]remature standardization . . . can lock in outdated technology”), at <http://www.technology.gov/digeconomy/frameworkr.htm> (last visited Dec. 3, 2003); Egyedi, *supra* note 3, at 49 (offering a theoretical perspective).

15. See CARGILL, *supra* note 1, at 42 (providing a theoretical IT perspective); LIBICKI, *supra* note 3, at 18-19; Bradner, *Internet Standards Process*, *supra* note 14 (granting the strongest status, “Internet Standard”, only to those specifications that have already become widely adopted); cf. MARCH & OLSEN, *supra* note 13, at 50-52 (offering an institutional analysis perspective).

Not every technological specification meets both criteria.¹⁶ Technological developments placed on the standards track but that do not comply with both criteria are generally regarded as “non-standard” technology.¹⁷ Such non-standard technology usually lacks the minimum degree of acceptance.¹⁸ Another type of non-standard technology is found in specifications that had been previously defined as standards until they were superseded by an updated standard¹⁹ or otherwise fell into disuse.²⁰ In short, only specifications meeting both criteria are regarded as IT standards. As potentially cohesive and stable technologies, standardized specifications are the focus of cyberspace’s institutional policy planning.

B. The Technological Lifecycle: The Criterion of “Time”

The U.S. government’s formal standardization policy regarding the time constraint, either as a production investment restraint or as a function of a technological life cycle, was consistently ignored.²¹ The emerging investment literature already acknowledges that the ability of an investor to delay an irreversible investment may affect a decision on whether and

16. See Bradner, *Internet Standards Process*, *supra* note 14 (providing examples of standards which failed to attract wide acceptance, such as most of the ISO standards for data communications, and the IEEE 802.6 standard for Distributed Queue Dual-Bus data communications).

17. *Id.* §§ 4.2.1-4.2.4.

18. *Id.* § 4.2 (“Specifications that are not on the standards track are labeled with one of three ‘off-track’ maturity levels: ‘Experimental’, ‘Informational’, or ‘Historic.’”).

19. *Id.*

20. *Id.*

21. Initially, there are numerous questions regarding the timing constraint, such as the relationship between the optimal entry of infrastructure standards vis-à-vis application standards; the impact of regulatory delay in issuing first entry licenses from the diffusion of innovation to their standardization; the preemptive, immediate and long-term effects of additional entry licenses of innovations on standardization; the optimal time it takes to detect “early maturity,” the optimal time to publicly announce a standard; and the distinction between simultaneous versus sequential entry. These questions invite further research, and a reassessment of IT standardization policy at large. See generally Jay P. Choi & Marcel Thum, *Market Structure and the Timing of Technology Adoption with Network Externalities*, 42 EURO. ECON. REV. 225-44 (1998); Joseph Farrell & Garth Saloner, *Installed Base and Compatibility: Innovation Product Reannouncement and Predation*, 76 AM. ECON. REV. 940-55 (1986); Pierre Regibeau & Katherine E. Rockett, *The Timing of Product Introduction and the Creation of Compatibility Decisions*, 14 INT’L J. INDUS. ORG. 801-23 (1996). In system environments such as cyberspace, probably the most important concern regards the influence of time of entry of infrastructure standards vis-à-vis application standardization, as discussed herein.

when to invest.²² This central recognition is even more evident whenever dynamic IT standards are involved.

More specifically, in IT standardization theory and practice, it is well accepted that the technical absorption of highly technologically finished products or routine product improvement processes²³ into common usage is a progressive phenomenon. That is, the absorption of one standard or a more complex system²⁴ of standards²⁵ is neither immediate nor inclusive. Rather it is progressive and takes on different investment inputs.²⁶ Seen through a production stage model, there are three consecutive independent technological phases, in the establishment of a standardized system technology.²⁷ All three are part of what is also known as a technological life-cycle—a metaphor that typically describes the evolution of standardized technology from its emergence to technological maturity and inevitable decline.²⁸ In essence, a technological lifecycle interacts with the standardization process through the life of each standard or group of standards.²⁹

22. See Robert McDonald & Daniel R. Siegel, *The Value of Waiting to Invest*, 101 Q.J. ECON. 707 (1986); Robert S. Pindyck, *Irreversibility, Uncertainty and Investment*, 29 J. ECON. LITERATURE 1110 (1991).

23. For the difference between close-ended “product standards” and descriptive “process standards,” see CARGILL, *supra* note 1, 59-61; LOUIS G. TORNATZKY & MITCHELL FLEISCHER, *THE PROCESSES OF TECHNOLOGICAL INNOVATION* 20-22 (1990); Mark Blaug, *A Survey of the Theory of Process-Innovations*, 30 *ECONOMICA* 13-22 (1963) (commenting on the more wider context of “product innovation” and “process innovation”). Both of these IT definitions were finally adopted in The National Cooperative Production Amendments of 1993, 15 U.S.C. § 4301(a)(6)(D) (2000) (regarding the definition of a term “joint venture”) and accordingly in 15 U.S.C. § 4305(a)(3) (2000) (regarding the disclosure of the purpose of the joint venture).

24. Conceptually, systems are goods that consist of perfectly complementary components such as hardware and software. See Jeffrey Church & Neil Gandal, *Network Effects, Software Provision, and Standardization*, 40 J. INDUS. ECON. 85-103 (1992); Michael L. Katz & Carl Shapiro, *Systems Competition and Network Effects*, 4 J. ECON. PERSP. 8, 93-115 (1994).

25. See CARGILL, *supra* note 1, 142 (“Usually quite a few standards will be invoked at once.”); Andy Sloane, *The Standards Process: Tools and Methods for Standards Tracking and Implementation*, 22 *COMPUTER STANDARDS & INTERFACE* 5-12 (2000).

26. See FARRELL & SOLANER, *supra* note 12, at 3 (for the technological standardization perspective); TORNATZKY & FLEISCHER, *supra* note 23, 27-30 (for the wider technological innovation perspective); see also sources cited *infra* note 28.

27. In keeping with its public standardization production process perspective, this study will focus on a production stage model. Cf. TORNATZKY & FLEISCHER, *supra* note 23, at 28-29 (discussing a private user-oriented stage model and the interplay between both models).

28. In IT standardization literature, a variety of overlapping phases of this process were have been suggested. See, e.g., Michal J. Bonino & Michael B. Spring, *Standards as Change Agents in the Information Technology Market*, 12 *COMPUTER STANDARDS &*

For information systems like the Internet, this processional rationale is constituted in the dominant industry “performance standard”³⁰ known as the ISO/IEC 15288³¹ “Life Cycle Management—System Life Cycle Processes.”³² ISO/IEC 15288 establishes a common framework for describing the lifecycle of systems and a complete set of well-defined processes and associated terminology.³³ ISO/IEC 15288 is meant to be applicable to any type of system or system of systems, such as the Internet.³⁴ In fact, the

INTERFACES 97-107 (1991) [Weiss & Spring, *Standards as Change Agents*]; Egyedi, *supra* note 3, at 49 (suggesting developing, inventing, and diffusing phases); Robin Mansell & Richard Hawkins, *Old Roads and New Signposts: Trade Policy Objectives in Telecommunication Standards*, in TELECOMMUNICATION, NEW SIGNPOSTS TO OLD ROADS 45 (Franca Klaver & Paul Slaa eds., 1992) (suggesting planning, negotiation, and implementation phases); Martin B.H. Weiss & Michael B. Spring, *Selected Intellectual Property Issues in Standardization*, in INFORMATION TECHNOLOGY STANDARDS AND STANDARDIZATION: A GLOBAL PERSPECTIVE 63 (Kai Jakobs ed., 1999) [hereinafter Weiss & Spring, *Selected IP Issues*]. For a variety of five-phased processional descriptions, see, for example, Yesha Y. Sivan, *Knowledge Age Standards: A Brief Introduction to Their Dimensions*, in INFORMATION TECHNOLOGY STANDARDS AND STANDARDIZATION: A GLOBAL PERSPECTIVE 1 (Kai Jakobs ed., 1999) (suggesting missing, emerging, existing, declining, and dying phases). See also BREYER, *supra* note 1, at 101-09 (for an economic analysis upholding an analogous five-phased standardization process).

29. See CARGILL, *supra* note 1, at 142; Bengt Hogberg et al., *Innovation in Industrial Policy Sectors—The Cases of Remote Sensing and Bioenergy*, in ORGANIZING INDUSTRIAL DEVELOPMENT 160-62 (Rolf Wolf ed., 1986); Sloane, *supra* note 25, at 6-7.

30. “Performance standards” state requirements in terms of results with criteria for verifying compliance but without stating the methods for achieving those results. See FEDERAL PARTICIPATION IN THE DEVELOPMENT AND USE OF VOLUNTARY CONSENSUS STANDARDS AND IN CONFORMITY ASSESSMENT ACTIVITIES § 3(2) (Off. Mgmt. & Budget, Circular A-119, Feb. 10, 1998) [hereinafter OMB Circular No. A-119] (memorandum for heads of executive departments and agencies) (discussing federal participation in the development and use of voluntary consensus standards and in conformity assessment activities), at <http://www.whitehouse.gov/omb/circulars/a119/a119.html> (last visited Dec. 18, 2003).

31. “ISO” is the International Organization for Standardization. “IEC” is the International Electrotechnical Committee. See *ISO Website*, at <http://www.iso.ch/iso/en/ISOOnline.frontpage> (last visited Dec. 1, 2003).

32. Consequentially, ISO 15288 is designed to be in complete harmonization with the ISO 12207, or “Software Life Cycle Processes” standard, and the ISO 15504, or “Software Process Assessment” standard. See *ISO/IEC 15288 Website*, at <http://www.15288.com/> (last visited Dec. 18, 2003); see also *Software Productivity Consortium Website*, ISO/IEC 15288, at <http://www.software.org/quagmire/descriptions/iso-iec15288.asp> (last visited Dec. 1, 2003).

33. See *ISO/IEC 19760—System Engineering—A Guide for the Application of ISO/IEC 15288 System Life Cycle Processes*, ISO/IEC 15288 Website (Oct. 2002), at http://www.15288.com/about_15288.htm (last visited Dec. 1, 2003).

34. *Id.*

ISO/IEC 15288 system lifecycle definition is the first ISO standard to deal aggregately with system lifecycle process in the context of hardware, software and human interfaces.³⁵ Without a precise understanding of the consecutive relations between infrastructure and applications, both types of activities can be wrongly assumed to be taking place simultaneously. This assumption ignores the existence of distinct system technologies, such as encryption or security standards, thereby failing to acknowledge their distinct standards and unique standardization activities. Alternatively, with a different policy approach, a sequential institutional choice should be made to account for the differences between infrastructure and applications.

The first lifecycle phase, the infrastructure development phase, begins with idea generation and ends with the development of a basic product or process. The introduction of a new technological innovation creates the content of the core infrastructure standards. In the infrastructure development phase, standards begin to be specified in their public form.³⁶ This phase is technologically-oriented, thus any consumer-oriented price-based competition of technological knowledge is usually both technically premature and economically inefficient.³⁷ Thus, very little price-based competition transpires in this phase. In this infrastructure development phase,

35. Some definitions of an “information system life cycle” potentially include both infrastructure and applications. See U.S. Dep’t of Agric., Natural Res. Conservation Serv., *Part 511—Information System Life Cycle Oversight and Evaluation* § 511.3 (“An information system contains the components developed and maintained during its lifecycle, including hardware and software configurations, application architecture, technical architecture, custom software components, application built packages, databases, project plans, test plans, implementation and migration plans, system documentation, and user documentation.”), at http://policy.nrcs.usda.gov/scripts/lpsiis.dll/M/M_270_511.htm (last visited Dec. 1, 2003); see also Hogberg et al., *supra* note 29, at 160-62 (“[T]he life cycle concept can be applied to different levels of analysis, i.e., to a technology, a product, or a branch of industry.”).

36. See JOHN E.S. PARKER, *THE ECONOMICS OF INNOVATION* tbl. 4.5 (1978). The dynamic correlation between the creation of innovations and standards is subject to a substantive change with the beginning of standards’ commercialization. See discussion *infra* Part IV.

37. See, e.g., J. Gregory Sidak, *An Antitrust Rule for Software Integration*, 18 YALE J. ON REG. 1, 27 (2001) (“[i]n such a market, consumer knowledge is accumulating, and product demand is still immature and unstable”); Michael Whinston, *Tying, Foreclosure, and Exclusion*, 80 AM. ECON. REV. 837, 855-56 (1990) (suggesting that lack of technologic maturity leads to unclear ex ante results and to ambiguous future welfare effects); Carl Shapiro, *Antitrust in Network Industries*, *Address to the American Law Institute and the American Bar Association on Antitrust/Intellectual Property Claims in High Technology Markets* (Jan. 25, 1996), at <http://www.usdoj.gov/atr/public/speeches/shapiro.htm> (last visited Dec. 1, 2003).

radical innovations develop entirely new core standards (“infrastructure standards”). As a whole, these core standards are oriented toward increased technological performance, rather than an immediate market need. As a general rule, core or infrastructure standards usually establish a necessary technical platform for future standardized applications as well as for other complementary standardized technologies.³⁸

The second lifecycle phase is the modification phase. In the modification phase, the technology accepted in the infrastructure development phase undergoes rapid innovative changes. Because of consumer demand for enhanced complementary application products, competitors begin to challenge each other, leading to extensive bargaining over modifications.³⁹ These bargaining result in modifications to the previous technical policies that are necessary for the emergence of new markets for core Internet telecommunications services. The modification phase also serves to enhance the creation of commercial products or processes that are later finalized in the last phase of the technological lifecycle, the implementation phase. Consequently, the technological modification phase does not generate any new standards of its own because it is a short and intermediate stage.

The implementation phase is the last of three standardization stages. Here, technology matures due to technological and market limitations. In cyberspace, this leads to the final creation of new markets for both core Internet telecommunications *services* and conforming standardized *products* and *applications*.⁴⁰ The creation of new markets typically propagates the unavoidable final decline of that same technology as it attempts to adhere to its own standards, followed by the emergence of new, competitive product generations that are standards-compliant to the extent necessary for consumer adoption.⁴¹ Seen as an evolutionary production process, each product generation would then suggest a more advanced and compatible technology with existing standards and the fast growing consumer demands. In this third and final phase, complementary application standards became largely oriented towards specific market needs of improving exist-

38. This technological incentive is particularly effective when it creates entirely new markets for standards. The difficulty in maintaining this incentive after the development phase will be discussed in Part V.

39. See BREYER, *supra* note 1, at 107-08, 177-78 (describing such bargains in various industries).

40. See Sidak, *supra* note 37, at 27-28 (stating that “[i]n such a market, products are well-defined, both by the consumer demand that they satisfy and by the production technology through which firms supply them”).

41. See OMB Circular No. A-119, *supra* note 30.

ing technology and further standardizing newer applications and conforming standards (“application standards”).

C. Cyberspace’s Architectural Edifice: The Criterion of “Space”

In addition to institutionalizing the aspect of time, the technological lifecycle ultimately incorporates the creation of substantively different types of standards in each sequential phase. Infrastructure standards are created in the infrastructure development phase. This is followed by application and complementary technology standards, which are then replaced by new and improved standards.⁴² Accordingly, as a function of both technological and commercial needs, these *categories* of standards emerge as part of the overall technological standardization endeavor and, as such, serve as an additional independent regulatory constraint.

1. *The Normative Framework*

After evaluating the function of time, a rational policy planner should evaluate the long-established criterion of space, namely, types of standards by location.⁴³ In cyberspace, space is a function of architectural layer. With technological standards, the need for this criterion may be less obvious. On one hand, an overly strict definition of standards by type according to architectural layer may lead to technological rigidity, inhibiting potential standard setters from developing additional or cheaper alternative standards.⁴⁴ On the other hand, identification of standards by type may potentially lower administrative costs and thus diminish both technological and economic uncertainty.⁴⁵

Theoreticians and the FCC have tried to view setting standards according to architectural layer as a way to lower costs and diminish uncertainty. As early as 1966, the FCC commenced an inquiry (“First Computer Inquiry”) to study the interrelationship of computers and telecommunications technologies, and the use of computer-based services over telephone lines.⁴⁶ This inquiry partly influenced the Telecommunications Act of 1996 and certain of these orders are still in effect. The FCC Commission further observed that “the growing convergence of computers and communications has given rise to a number of regulatory and policy questions

42. See TORNATZKY & FLEISCHER, *supra* note 23, at 165.

43. See OGUS, *supra* note 1, at 165-68.

44. *Id.* at 167.

45. See *id.*; Shapiro, *supra* note 39, § III.B.2.

46. See *In re Regulatory & Policy Problems Presented by the Interdependence of Computer & Communication Serv. & Facilities*, 7 F.C.C.2d 11 ¶ 2 (1966) (addressing the apparent convergence between telecommunications and computing).

within the purview of the Communications Act.”⁴⁷ These policy concerns are as true today as they were more than three decades ago.⁴⁸

In its next inquiry (“Second Computer Inquiry”), the Commission reaffirmed its essential regulatory approach to the provision of computer data services, but improved its analysis.⁴⁹ By distinguishing regulated telecommunications services from unregulated data services, the Commission created the categories of *basic* services⁵⁰ (renamed “telecommunications services”) and *enhanced* services⁵¹ (renamed “information services”).⁵² The Commission also elaborated on the extent of structural separation required between the incumbent telephone provider and its enhanced services affiliate.⁵³

Understanding that the future would bring the convergence and interdependence of computers and communications, the Commission was aware of the difficulty of separating telecommunications services into two

47. *Id.* ¶ 1.

48. *Id.*

49. This distinction was then formally adopted. F.C.C., 103D CONG., REPORT IN RE FEDERAL-STATE JOINT BOARD ON UNIVERSAL SERVICE ¶ 33 (Apr. 10, 1998) [hereinafter *Second Computer Inquiry*] (stating that telecommunications services and information services are “separate, non-overlapping categories, so that information services do not constitute ‘telecommunications’ within the meaning of the 1996 Act”), at http://www.fcc.gov/Bureaus/Common_Carrier/Reports/fcc98067.pdf (last visited Dec. 1, 2003).

50. The Commission defined the term “basic” service, which referred to traditional common carrier telecommunications offerings as “the offering of transmission capacity for the movement of information.” See *In re Comsat Study*, 77 F.C.C.2d 584 ¶ 93 (1980).

51. The Commission defined “enhanced services” as “services, offered over common carrier transmission facilities used in interstate communications, which employ computer processing applications that act on the format, content, code, protocol, or similar aspects of the subscriber’s transmitted information; provide the subscriber additional, different or restructured information; or involve subscriber interaction with stored information” See 47 C.F.R. § 64.702(a) (2001).

52. The Telecommunications Act broadly defines an “information service”, specifically excluding “telecommunications services”, as

the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing, but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service.

47 U.S.C. § 153 (2000).

53. See *Comsat Study*, 77 F.C.C.2d ¶ 190-266. For a wider discussion about the three Computer Inquiries’ genealogy, see BARBARA ESBIN, INTERNET OVER CABLE: DEFINING THE FUTURE IN TERMS OF THE PAST 25-26 (FCC OPP, Working Paper No. 30, 1998), at http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp30.pdf (last visited Dec. 18, 2003).

discrete categories.⁵⁴ The Internet, in its contemporary form, did not exist at the time the FCC formed the basic/enhanced distinction and, as a result, the categories are subject to genuine interpretive ambiguities when applied to cyberspace. As the Commission acknowledged, “[p]lausible arguments can be tendered for drawing the line between the two services elsewhere. At the margin, some enhanced services are not dramatically dissimilar from basic services or dramatically different from communications as defined in the First Computer Inquiry.”⁵⁵ For example, appreciative data processing, computer memory or storage, and some advanced switching techniques typically identified as enhanced services can be components of a basic service if they are used solely to facilitate the movement of information.⁵⁶ A second interpretive ambiguity for cyberspace is that the FCC classification has focused entirely on the basic and enhanced services distinction from a telecommunications perspective with no adequate consideration of cable-based Internet services.⁵⁷ Instead, the Commission observed that because enhanced service was not explicitly referred to in the Telecommunications Act, there was no more reason to confront it with a specific traditional regulatory mechanism than there was for cable television’s formal elements of common carriage and broadcast television (then unregulated under the Act).⁵⁸

A third interpretive problem is that, even while upholding the Commission’s policy of regulating only the common carrier *basic* transmission service,⁵⁹ there is still little or no guidance about the question of how the Commission *should* act towards Internet-based services.⁶⁰ For standardiza-

54. See OXMAN, *supra* note 4, at 7; WERBACH, *supra* note 4, at 46.

55. See *Comsat Study*, 77 F.C.C.2d ¶ 434 (the Commission avoided re-drawing the line at this margin due to its concerns that such action could potentially subject the issue to constant adjudication over the status of individual services offerings. However, as such distinctions are crucial for any institutional standardization analysis, such adjudication is necessary, and will be upheld in this chapter hereinafter); see also ESBIN, *supra* note 53.

56. *Comsat Study*, 77 F.C.C.2d ¶ 419-20.

57. Traditionally, cable service has been regulated as an integrated video, information content, and conduit service under Title VI of the Telecommunications Act. See ESBIN, *supra* note 53, at 3, 83-90 (for an of integrated cable-based analysis of Internet access services); see also *Second Computer Inquiry*, *supra* note 49, at 98-167 n.140 (reserving consideration of the “regulatory classification of Internet services provided over cable television facilities”).

58. See *Comsat Study*, 77 F.C.C.2d ¶ 430.

59. See J. SCOTT MARCUS, THE POTENTIAL RELEVANCE TO THE UNITED STATES OF THE EUROPEAN UNION’S NEWLY ADOPTED REGULATORY FRAMEWORK FOR TELECOMMUNICATIONS 6 (FCC OPP, Working Paper No. 32, 2000), at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-224213A2.doc (last visited Dec. 18, 2003).

60. See, e.g., WERBACH, *supra* note 4, at 29.

tion purposes, there was thus no adequate distinction between the question of *regulating* existing enhanced services and standardizing their *production*. This lack of direction implicitly leaves both processes to the competitive “hands off” premise of Title II of the Telecommunications Act.⁶¹ To add to this confusion, the Commission noted that it retains regulative control over enhanced services under the ancillary jurisdiction of Title I, on the grounds that the enhanced services under consideration “constitute the electronic transmission of writing, signs, signals, pictures, etc., over the interstate telecommunications network.”⁶²

Notwithstanding these interpretive difficulties, these two dependent categories, basic and enhanced, give rise to two different types of standards in present day cyberspace.⁶³ The first type is standardized physical telephony infrastructure standards and layers, which are supported by the basic packet switching, transporting, addressing, and routing protocols that establish most of cyberspace’s infrastructure standards. Originally, in the *Report In re Federal-State Joint Board on Universal Service*⁶⁴ and subsequent orders, the Commission came to address the implications of packet-switching technologies for this regulatory framework.⁶⁵ It was admitted that the use of packet switching and error control techniques⁶⁶ “that facilitate the economical, reliable movement of [such] information [do] not alter the nature of the basic service.”⁶⁷

The second type of standards, computer software standards, establish most of cyberspace’s subsequent application standards and are to be found in the user-oriented “application” layer of cyberspace’s architecture. The application layer performs many of the Internet’s information processing functions, such as authentication, email storage and retrieval, Web page hosting, and domain name server lookups. These functions involve substantial computer processing and interaction with customer-supplied information, and therefore fall squarely within the definition of enhanced

61. See OXMAN, *supra* note 4, at 13, 21.

62. *Comsat Study*, 77 F.C.C.2d ¶ 432.

63. Cf. STUART MINOR BENJAMIN ET AL., TELECOMMUNICATIONS LAW AND POLICY, 867 (2001) (implying this analysis).

64. See *supra* note 49.

65. See WERBACH, *supra* note 4, at 31 (discussing the applicability of the distinction between basic and enhanced Internet telecommunications services).

66. *Comsat Study*, 77 F.C.C.2d ¶ 420.

67. For example, in subsequent decisions the Commission determined that packet-switched networks following X.25 protocols, and frame relay service offerings provide a basic transport service. See *Application of AT&T*, 94 F.C.C.2d 48, 55-57 (1983); see also WERBACH, *supra* note 4, at 32.

services.⁶⁸ Specific enhanced services include protocol processing and electronic publishing, as well as the provision of access to data networks such as commercial online services and the Internet.⁶⁹

Ultimately, both sets of standards and their associated services should pave the way for a more comprehensive and accurate multi-layered and standards-based understanding than the current one. The higher the layer and production phase, the more specific the purposes of their standards become. The key insight is that although data is transmitted vertically, each different layered protocol is programmed horizontally to become compatible with neighboring standards and should thus be subject to different production costs. Later, with clear categories of standards, it will be possible to finalize the Internet's institutional regulative policy as a whole.⁷⁰

2. *Infrastructure Standards*

Cyberspace, and more distinctively, the Internet are commonly defined by a unified architectural backbone structure and core protocols known together as the formal TCP/IP networking reference model of the Internet's four-layer architecture.⁷¹ TCP/IP's architectural hegemony began as early as 1983, when the TCP/IP networking reference model largely overtook the formal, seven layered, Open System Interconnection ("OSI") networking reference model. The TCP/IP model refers to a large number of protocols located in four main layers of standardized architecture that formally standardize both the Internet's core infrastructure and complementary application standards by their relevant layer location. Practically, although the TCP/IP reference model is not always strictly followed with respect to keeping related functions together in a well-defined layer, most telecommunications and information systems products make an attempt to describe their functions in relation to this model. At least informally, the Internet's architecture can be described methodologically in four layers. The first layer is the "network access" layer. In its basic physical foundation lays the North American architecture, in connection with Europe through the EBONE communication supporter, which consists of three autonomous managed levels of hierarchical architecture. Each of

68. WERBACH, *supra* note 4, at 32-33.

69. *Id.*

70. See discussion *infra* Parts III-V.

71. A "backbone" is a telecommunications line that links one or more locations together. See CRAIG HUNT, TCP/IP: NETWORK ADMINISTRATION 1-22 (2d ed. 1997); Hans-Wernes Braun & Kimberly C. Claffy, *Network Analysis for a Public Internet*, in PUBLIC ACCESS TO THE INTERNET 353-56 (Brian Kahin & James Keller eds., 1995).

these levels as a whole represent a function performed when data is transferred between cooperating applications across the network, in the following hierarchical order: National Backbones (for example, NSFNET) which are attached among themselves, through (inter-) national network interconnections facilities, and down the line also to mid-level networks (for example, Midnet), which are attached to local service providers (for example, UCSD).⁷²

The latter backbone level supports five additional infrastructure levels, beginning with different IP networks (for example, 132.204.m.n), which are attached to IP sub-networks (for example, 132.204.51.n), which are attached to IP Host/end-systems (for example, 132.204.51.6)⁷³, which are attached to end-users, which are attached to networked applications (for example, X-Windows).⁷⁴

Ultimately, the different layers also differ in their standardized system-oriented specifications. The three backbone levels, consisting of the “network access” layer, contain very few protocols, as they handle relatively uncomplicated network interactions. This layer defines the network hardware and device drivers.⁷⁵

72. The FCC refers to cyberspace’s lower physical telephony infrastructure through four physical categories and formally suggested an analogous definition: backbone, middle mile, last mile and last 100 feet. *See In re Inquiry Concerning the Deployment of Advanced Telecommunications*, 15 F.C.C.R. 20913 (2000).

73. A “host” is a computer directly connected to the Internet. Still, it does not accurately reflect the actual number of Internet users, and is usually shared by groups of users and is thus smaller than them in size.

74. *See* Braun & Claffy, *supra* note 71; *cf.* HUNT, *supra* note 71, at 1-22. Hunt provides a functional-based description of the TCP/IP networking reference model in four levels: 1) “network access” (referring to the three backbone network levels); 2) “Internet” (referring to the IP Networks and sub-networks levels, similar to the Open System Interconnection (“OSI”) “network” layer); 3) “host-to-host transport” (referring to the IP Host/end-systems, similar to the fourth layer in the OSI model); and finally 4) the “application” level (referring to the end-users and the networked applications levels, similar to layers 5-7 in the OSI model). HUNT, *supra* note 71, at 1-22. For an analogous four-layer description, containing the Link, Network, Transport and Application layers, see *ISO/OSI Network Model Description*, at http://www.uwsg.iu.edu/usail/network/nfs/network_layers.html (last visited Dec. 1, 2002). In order to simplify, I suggest to refer the hegemonic TCP/IP labels as layers, as suggested also by Hunt. Previously, the Federal Networking Council (“FNC”) has unanimously upheld the existence of a layered architecture, as part of the Internet’s definition. *See* Brian Carpenter, *Architectural Principles of the Internet*, RFC 1958, at <http://www.faqs.org/rfcs/rfc1958.html> (last visited Dec. 18, 2003).

75. As far as standardization matters, these “non-consumer-oriented” levels include technologies for network management (for example, the Simple Network Management Protocol (“SNMP”)), the Ethernet standard for local area networks, the Frame Relay

More infrastructure protocols exist at the next two levels—the IP networks and sub-network layers, or the “Internet” layer, where the IP protocol prevails. As a general matter, they are both responsible for routed data interchange between hosts and across network links, through addressing and fragmentation of packets (for example, the Internet Protocol Version 6 standard (“IPv6”).⁷⁶ The third and final infrastructure layer is the “transport” layer, referring to the IP Host/end-systems level. The function of this layer is to make the Internet more useful and accessible to its users. This layer includes standardized telecommunications and transport protocols (for example, the Transmission Control Protocol (“TCP”)),⁷⁷ and more general standards for providing sufficient quality of service.⁷⁸

The various infrastructure layers are breeding grounds for strict network or system-oriented (rather than user-oriented) physical telephony infrastructure standards, which together establish the Internet’s core infrastructure. Potentially seen as “basic” services according to the meaning established in the Computer Inquiries, they should also refer to traditional common carrier telecommunications offerings as “the offering of transmission capacity for the movement of information[.]”⁷⁹ As such, the three

packet-switched data communication service, and standardized management interfaces for various classes of equipment (for example, the Fiber Distributed Data Interface (“FDDI”) for the 100 Mbps local area networks, and other operations issues). See DOUGLAS E. COMER, *INTERWORKING WITH TCP/IP (PRINCIPLES, PROTOCOLS, AND ARCHITECTURE)* 32-33 (3d ed. 1995); WILDER, *supra* note 14 (describing the TCP/IP protocol suite).

76. WILDER, *supra* note 14, at 155-64.

77. See *id.* at 165-84 (discussing the transmission control protocol); Charles Hornig, Symbolics Cambridge Research Center, RFC 894—Standard for the transmission of IP Datagrams over Ethernet networks (Apr. 1984), at <http://www.faqs.org/rfcs/rfc894.html> (last visited Dec. 2, 2003); Information Sciences Institute, University of Southern California, RFC 791—Internet Protocol (Sept. 1981), at <http://www.faqs.org/rfcs/rfc791.html> (last visited Dec. 2, 2003); Information Sciences Institute, University of Southern California, RFC 793—Transmission Control Protocol (Sept. 1981), at <http://www.faqs.org/rfcs/rfc793.html> (last visited Dec. 2, 2003); P. Mockapetris, Information Sciences Institute, University of Southern California, RFC 882—Domain names: Concepts and facilities (Nov. 1983) [hereinafter RFC 882], at <http://www.faqs.org/rfcs/rfc882.html> (last visited Dec. 2, 2003).

78. This layer is generally dominated by two different protocols, YCP and UDP, which are responsible for negotiating the flow of data between any two network hosts. See COMER, *supra* note 75, at 179-90; WILDER, *supra* note 14, at 163-64. See also Clinton & Gore, *A Framework*, *supra* note 14, § 9 (providing a U.S. governmental perspective); *Active IETF Working Group Website* (a list of working groups in these areas), at <http://ietf.org/html.charters/wg-dir.html> (last visited Dec. 18, 2003); IETF Internal Division Website (providing an industry perspective on these layers), at <http://www.ietf.org> (last visited Dec. 18, 2003).

79. *In re Comsat Study*, 77 F.C.C.2d 584 ¶ 93 (1980).

infrastructure layers are subject to separate standardization costs and a different institutional choice.

3. *Application Standards*

The “application” layer sits on top of the infrastructure layers and refers to the end-user and the networked application levels of the Internet. Application layer standards serve two major functions. First, as TCP/IP-compatible standards, they facilitate the operation of the infrastructure standards. The most familiar among these application standards are the standardized network application protocols (for example, HTTP, FTP and SMTP, NFS, DNS, arp, rlogin, talk, and ntp).⁸⁰ Functionally, application standards interact between clients (our personal computers) and servers (the relevant data storage units).⁸¹

Not all standardized technologies are directly related to earlier infrastructure technology and are not meant to facilitate operation. Thus, a second function of these standards, only indirectly related to infrastructure protocols, is as a source of innovation.⁸²

Overall, the emergence of new markets and sub-markets that the application layer has given rise to a variety of Internet software products such as browsers, encryption modules, contract infrastructures, electronic payment systems and security equipment (for example, the IP Security (“IP-Sec”) protocols⁸³ and XML Digital Signatures⁸⁴), X-Windows, Java, and

80. *See generally* WILDER, *supra* note 14, at 293-356.

81. Of central importance to this interaction are Hyper Text Transfer Protocol (“HTTP”), used to publish (and read) hypertext documents across the web; File Transfer Protocol (“FTP”), used to transfer files; and Simple Mail Transport Protocol (“SMTP”), used to transfer electronic mail. *See* COMER, *supra* note 75, at 299-304, 315-23, 344-47.

82. One example for this technological development can be examined through security technology, as it is embedded in both infrastructure and application standards. Thus, in its infrastructure lies the Secure Socket Layer (“SSL”) infrastructure protocol, which resides above the TCP layer and below application layer protocols. Examples include HTTP, LDAP, and IMAP. SSL is designed to make use of TCP to provide a reliable and end-to-end service. Because SSL is a channel security mechanism running on TCP, it can secure any protocol that can be carried by TCP. Thus, it was ideally suited for following secured applications such as SMTP, Telnet, and FTP, through independent commercial innovative software, such as NetStructure 7115 e-Commerce Accelerator (an SSL offload device) and SeeBeyond e*Xchange eBusiness Integration Suite (an interface for configuring security parameters). *See, e.g.*, Zeus Technology, *SSL Theory and Practice* (June 2000), at <http://itpapers.com/abstract.aspx?kw=ssl+&docid=25317> (last visited Dec. 2, 2003).

83. *Id.*

84. *See* W3C, *Extensible Markup Language (XML) 1.0* (2d ed. Oct. 10, 2000), at <http://www.w3.org/TR/2000/REC-xml-20001006> (last visited Dec. 2, 2003).

e-mail systems.⁸⁵ In essence, application standards are distinct from infrastructure standards in both specification and function. Potentially seen as “enhanced services” as defined by the Computer Inquiries these user-oriented standards seem to comply with the Commission’s definition of “enhanced services” as “services, offered over common carrier transmission facilities used in interstate communications, which employ computer processing applications that act on the format, content, code, protocol, or similar aspects of the subscriber’s transmitted information.” Like user-oriented standards, application standards also embed unique standardization costs and ultimately require a different institutional choice.

D. Standard-Setting Institutions: The Criterion of “Institutional Identity”

The final standard-setting criterion derives from the competing regulative regimes. Along with the criteria of time and space, this third criterion suggests a three-dimensional matrix of institutional choices for policy makers.

Institutions that regulate technological standards differ according to several variables. First, they differ by the degree of regulative formality, which indicates the degree of legality and influence of its legitimate elective legislators. Turning to comparative institutional theory, March and Olsen address this question, while questioning both the primacy of such action and its outcomes.⁸⁶ Accordingly, the core task of political institutions is to confirm the legitimacy of standardization choices by ensuring that relevant people are involved and that an appropriate control structure exists.⁸⁷ These same elements are also arguably evident in standardization ideology as they define the role of formal standards bodies as guardians of the process.⁸⁸ In all standardization bodies, specifications are merely a starting point. Functionally, standard setters also perform the role of checking the level of acceptance of their standards in relevant markets, through the breadth of their recognition and, ultimately, through actual exercise by users.

Measuring that acceptance typically requires determining whether the specified protocol or service provides significant benefit to the cyber

85. This same application layer lies exclusively (and, arguably, only for the time being) at the core of the ongoing debate regarding application software as a regulative constraint. See LESSIG, *supra* note 8, at 101-02; SHAPIRO & VARIAN, *supra* note 8; Gibbons, *supra* note 8; Johnson & Post, *supra* note 8; Wu, *supra* note 8.

86. MARCH & OLSEN, *supra* note 13, at 50-52.

87. *Id.*

88. See TORNATZKY & FLEISCHER, *supra* note 23, at 41-42.

community and market.⁸⁹ The second variable is the degree and type of monopolistic power over the right to supply, vis-à-vis the regulated status of all suppliers in a given market.⁹⁰ Third is the scope of the institution's legal status, evaluated in terms of its binding force and efficiency of enforcing a given standard.⁹¹ As a general matter, such performance is difficult to monitor for several reasons. For a start, there is no official legal means in the United States for ascertaining whether or not a standardization organization is a formal or informal standard developer.⁹² Moreover, this differentiation is empirically blurred since there have been no experiments on competitive self-regulation, no real market for the *control* of standard setters, and no easy option for principals (politicians and citizens) to dismiss ineffectual officials or market standard setters.⁹³

In one of the seminal articles on standardization, Farrell and Saloner identify five distinctive types of regimes, based on a function of their standardization endeavors.⁹⁴ The first, and least influential in cyberspace, is *de facto* standardization activity generated by internal decisions of

89. *See generally* MARCH & OLSEN, *supra* note 13.

90. *See id.*; TORNATZKY & FLEISCHER, *supra* note 23, at 41.

91. *Id.*

92. In the United States, alleged standards developers may request to be formally accredited by the American National Standards Institute ("ANSI"). *See* <http://www.ansi.org> (last visited Dec. 18, 2003). As part of a non-binding voluntary initiative, ANSI requires written procedures with strict requirements for openness, balance, consensus and other due process. Internationally, the situation is not substantively better, as alleged standards developers may be created by declaration of treaty agreements between cooperative nations, such as the International Telecommunication Union ("ITU") or by national policies which recognize a standards organization, such as the International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee ("ISO/IEC JTC 1"). *See Joint Technical Committee Website*, at <http://www.jtc1.org/> (last visited Dec. 2, 2003). Drafts of "international standards" adopted by the joint technical committee are circulated to national bodies for votes. Publication as an "international standard" requires approval by at least 75% of the national bodies casting a vote. *See also* CARGILL, *supra* note 1, at 200-04, 269-70 (discussing the activities of ISO/IEC JTC 1).

93. *See, e.g.*, FARRELL & SOLANER, *supra* note 12, at 5.

94. *Id.* at 2-5; *see also* OGUS, *supra* note 1, at 108-09; Mark A. Lemley, *Antitrust and the Internet Standardization Problem*, 28 CONN. L. REV. 1041 (1996) [hereinafter Lemley, *Antitrust*] (focusing on the government and industry players and *de facto* standards); Mark A. Lemley, *Standardizing Government Standard-Setting Policy for Electronic Commerce*, 14 BERKELEY TECH. L.J. 745, 747 (1999) [hereinafter Lemley, *Standard-Setting*]; Bob Toth, *Putting the U.S. standardization system into perspective*, 4 STANDARDVIEW 169, 169-78 (1999) (reviewing the presiding organizations inside the United States).

autonomous firms with a single vendor.⁹⁵ Closely related are standards emerging from a mutual agreement among several manufacturers, whether formal or informal, binding and/or voluntary—aimed at consolidating potentially different interests among the parties to the agreement.⁹⁶ Third, are ad hoc standards, consisting of market *de facto* and industry *gray* standards that are subsequently absorbed by consumers through accidental,⁹⁷ or strategic choice and then later adopted by the entire relevant market.⁹⁸ Standards designed by *de facto* standard setters are typically driven by self-interested profit maximizing implementers and tend to be both proprietary and closed sourced. Consequently, they are especially interesting from a legal perspective because they tend to raise a variety of issues concerning the proper scope of antitrust and intellectual property law in influencing market outcomes particularly in the implementation phase.

A fourth type of standardization institution is governmental, usually implemented through delegated regulatory agencies or organizations. Initially, governmental standards, in their meaning in section 12(d)(4) of the

95. Cf. FARRELL & SOLANER, *supra* note 12, at 2 (concluding, however, that a final analysis for both this regime and beyond is neither mutually exclusive nor independent, as it can be reflected in alternative *de facto* standard setters).

96. *Id.* (adding that this type of standard setter faces all the problems of autonomous firms, and more); see also SHAPIRO & VARIAN, *supra* note 8, at 236-37.

97. See Brian W. Arthur, *Competing Technologies and Lock-in by Historical Small Events: The Dynamics of Allocation Under Increasing Returns*, 99 ECON. J. 116-31 (1989) (modeling technological choice under increasing returns by consumers as a random process); Paul A. David, *Clio and the Economics of QWERTY*, 2 AM. ECON. REV. 75, 332-37 (explaining the development of the typewriter keyboard from this approach); Paul A. David, *Some New Standards for Economics of Standardization in the Information Age*, in ECONOMIC POLICY AND TECHNOLOGICAL PERFORMANCE 206 (Dasgupta & Stoneman eds., 1987) (confirming Arthur's study on historical lock-in under increasing returns).

98. See Michael L. Katz & Carl Shapiro, *Network Externalities, Competition and Compatibility*, 75 AM. ECON. REV. 424 (1985); Michael L. Katz & Carl Shapiro, *Product Compatibility Choice in a Market with Technological Progress*, 38 OXFORD ECON. PAPERS 145-65 (1986) (formalizing Arthur's notion into a theoretical model describing consumer's choice of technological products as a strategic consideration). These standards are possible after such a standard achieves a predominant market share over potential competitors. These three formats are commonly known as informal standards, and share the characteristic of being produced by non-legally binding autonomous market forces (*de facto*) or even particular groups (for example, non-profit organizations) or consortia (*gray*) standardizing autonomously. In some cases, companies may operate outside the established standard-setting organizations in consortia to form standards. See Roy Rada, *Consensus versus Speed*, in INFORMATION TECHNOLOGY STANDARDS AND STANDARDIZATION: A GLOBAL PERSPECTIVE 19, 30-31 (Kai Jakobs ed., 2000) (providing preliminary description of consortia); see also Egyedi, *supra* note 3, at 54-55 (describing grey standardization institutions).

National Technology Transfer and Advancement Act of 1995,⁹⁹ are developed by the government for its own uses.¹⁰⁰ As such, they are produced and made to serve, and thus penetrate, an entire industry. Finally, standards are introduced by intra-national, and more so, international standardization organizations operating jointly, through special agencies.¹⁰¹

These last two regimes, and the parties creating them, are commonly known as formal (“*de jure*”) standards and standard setters. They are processed by traditional political standard development organizations, such as the International Organization for Standardization (“ISO”), Internet Engineering Task Force (“IETF”), scientific or professional societies, trade associations or other types of industrial standard organizations, which may operate in accordance with official formal regulative bodies. Standards designed by *de jure* standard setters are typically driven by technologically-oriented implementers and tend to be both non-proprietary and open sourced. Historically, in other fields of media, standardization used to be the prefecture of international industry standardization organizations for example, the ITU, ISO, and the International Electrotechnical Commission (“IEC”). With time, standardization activity expanded to *de facto* and governmental standardization bodies.¹⁰² As in the telecommunications field, cyberspace is also subjected to all three, albeit not necessarily in that evolutionary order, as will be described in the following parts.

To conclude, the absorption of high technology, through one or more standards, into ordinary usage is sequential. Generally, there are three consecutive independent technological phases in the establishment of a standardized technology, beginning with the emergence of the technology in the development phase and ending in a full technological life-cycle. The creation of such standards varies in space, with the partition of cyberspace’s standardized architecture into four layers. Broadly, one can draw a clear distinction between the first three network or system-oriented layers,

99. National Technology Transfer and Advancement Act of 1995, Pub. L. No. 104-113, § 12(d)(4), 110 Stat. 775 (1996) (codified as amended at 15 U.S.C. 272(b) (2000)).

100. *Id.*

101. See FARRELL & SOLANER, *supra* note 12, at 4; see also FORMAL METHODS IN STANDARDS: A REPORT FROM THE BRITISH COMPUTER SOCIETY (BCS) WORKING GROUP 7-8 (C.L.N. Ruggles ed., 1990) (describing the various early European and American-based International standardization organizations); KELLEY LEE, GLOBAL TELECOMMUNICATIONS REGULATION: A POLITICAL ECONOMY PERSPECTIVE 121-22 (1995) (describing the telecommunications field main precedents: the International Telecommunications User Group (“INTUG”), Intelsat or Eutelsat).

102. Petri Mähönen, *The Standardization Process in IT—Too Slow or Too Fast?*, in INFORMATION TECHNOLOGY STANDARDS AND STANDARDIZATION: A GLOBAL PERSPECTIVE 35, 37 (Kai Jakobs ed., 2000).

and the fourth user-oriented layer. These two groups of layers consist of substantively different technological standards, and therefore create different regulative costs and concerns. First, the three lower layers imbed infrastructure standards that are intended to maintain expensive lines,¹⁰³ data networking equipment,¹⁰⁴ Internet backbone telecommunications, and cable services.¹⁰⁵ These types of standards are most common to the early development phase. The application layer involves substantively different types of standards. These application standards establish most of cyberspace's computer software products. These standards are created primarily in the implementation phase of IT standardization. In essence, although data is transmitted vertically through each layer, each functional layer is programmed horizontally and should be subject to different production costs. Ultimately, different production costs may then lead to different institutional choices, as will be discussed later.

In addition to the criteria of time and space, different types of standardization regimes can be characterized by the identity of the institution that creates them. Standards designed by *de facto* standard setters are typically driven by self-interested profit maximizing implementers and tend to be both proprietary and closed. In contrast, standards designed by *de jure* standard setters are typically driven by technologically-oriented implementers and tend to be both non-proprietary and open sourced. Conceptually different phases of technological development lead to different technological standards. With that recognition, a rational policy-maker should be able to predict efficiently the degree of regulative compliance of each such standardized technology with typical price-based Kaldor-Hicksian efficiency,¹⁰⁶ and thereby establish a comprehensive regulative policy. Therefore, any optimal institutional choice will have to consider the following three technological phases, and their distinctive standardization activities.

103. But lots of cheap routers manage a limited number of these expensive lines. *See, e.g.*, Jeffrey K. MacKie-Mason & Hal R. Varian, *Pricing the Internet*, in PUBLIC ACCESS TO THE INTERNET 269, 273 (Brian Kahin & James Keller eds., 1995) (estimating that this conclusion is reflected in the rapid decline from expensive routers to expensive transmission links).

104. Both of which are oriented at clients (modem, ISDN, cable) and servers (routers, modem pools, and call aggregators).

105. These services include, for example, hybrid fiber-coax to cable and digital cable for higher-speed PC Internet connections.

106. According to the Kaldor-Hicksian notion of efficiency, whenever at least one person is better off and at least one is worse off, gainers should compensate losers. *See* ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 43-44 (3d ed. 2000).

III. THE INFRASTRUCTURE DEVELOPMENT PHASE: A POLITICAL INSTITUTIONAL INEVITABILITY

The technological infrastructure development phase introduces new innovations, beginning with idea generation to the development of a basic product or process. The infrastructure development phase results in the creation of core infrastructure standards. As a whole, these infrastructure standards are oriented toward increased technological performance rather than an immediate market need. As a general rule in cyberspace, infrastructure standards establish a necessary technical platform for future standardized applications as well as for other complementary standardized technologies. This part evaluates cyberspace's infrastructure endeavor of the early 1990s in light of this technological standardization phase with a further view toward infrastructure standardization for future technological generations. Official U.S. policy regarding cyberspace standard-setting never dealt appropriately with such infrastructure standards or the difference between setting infrastructure and application standards.¹⁰⁷ It has even largely ignored the existence of the technological professional constraint on standardization itself. Instead, the United States has largely focused its standardization policy on application standard-setting. The following will provide separate analysis for the Internet architecture establishment, the separate development of infrastructure standards and the backbone transit services of cyberspace.

A. Infrastructure Telecommunications Services: The Collective Choice Analysis

Between 1986 and 1992, Internet infrastructure governance evolved from an institutional hybrid of Department of Defense ("DoD") and government-supported academic research institutions, with the DoD controlling the funding and governance of the latter.¹⁰⁸ The Internet started as a U.S. government military project. It was later transferred to the National Science Foundation ("NSF"), which operated it for another decade.¹⁰⁹ The

107. In fact, the U.S. government applied its policy broadly, and made no distinction between infrastructure standards, such as "high-speed network technologies" and application standards, such as "electronic copyright management systems," in their meaning. See Clinton & Gore, *A Framework*, *supra* note 14, § 9.

108. See Anthony M. Rutkowski, *Factors Shaping Internet Self-Governance*, in COORDINATING THE INTERNET 92, 93-94 (Brian Kahin & James H. Keller eds., 1997).

109. See Steve Bickerstaff, *Shackles on the Giant: How the Federal Government Created Microsoft, Personal Computers, and the Internet*, 78 TEXAS L. REV. 1 (1999) (describing the major developments in these years while concluding that today's Internet market exists as a result of that government intervention rather than early free market competition).

NSF officially started the process that led to the comprehensive standardization of the current cyberspace technological generation. Following the experience of other telecommunications industries, the NSF realized the need for a unified wide-area infrastructure to support the early NSFNet.¹¹⁰ That realization immediately led to the adoption of two main *regulatory standardization* policies. The first was the 1985 decision to unify the TCP/IP set of protocols as a worldwide mandatory infrastructure for the NSFNet program at large.¹¹¹ Over time, that decision marginalized the other competitive computer network protocols and heralded the dominance of the addressing IP system.¹¹² Second, the NSF decided to support DARPA's existing Internet organizational infrastructure hierarchy, assembled by the previous Internet Activities Board ("IAB") in the decision known as the "Request for Internet Gateways" RFC 985.¹¹³

Having successfully dominated over DARPA and NSF's interoperable infrastructures, the federal government was ready to enlist the telecommunications and cable industries to further build out the Internet's infrastructure and promote private investment.¹¹⁴ The ultimate purpose of that initia-

110. See CARGILL, *supra* note 1, at 64-65 (discussing coordinating mandatory policies, as regulatory standardization).

111. Cf. Toru Komatsu, *The history and motivation of the Internet* (Feb. 29, 2000) [hereinafter Komatsu, *History*] (describing the transition of the ARPANET host protocol from Network Control Protocol ("NCP") to TCP/IP as of Jan. 1, 1983, which required all hosts to convert simultaneously or be left having to communicate via ad-hoc mechanisms, and stating that "[t]his transition was carefully planned within the community over several years before it actually took place and went surprisingly smoothly"), at <http://www.sju.edu/~tk098681/csc5235/history.htm> (last visited Dec. 3, 2003). But it resulted in a distribution of buttons saying "I survived the TCP/IP transition." Richard W. Wiggins, *The Internet Marks Its 20th Anniversary* (Dec. 30, 2002), at <http://www.infotoday.com/newsbreaks/nb021230-1.htm> (last visited Dec. 3, 2003).

112. See Komatsu, *supra* note 110.

113. Network Technical Advisory Group, *RFC 985—Requirements for Internet Gateways* (IETF Network Working Group, May 1986), at <http://www.faqs.org/rfcs/rfc985.html>; V. Cerf, *RFC 1160 – Internet Activities Board* (IETF Network Working Group, May 1990) (defining the areas of responsibility of the Internet Activities Board), at <http://www.armware.dk/RFC/rfc/rfc1160.html> (last visited Dec. 3, 2003); see also WILDER, *supra* note 14, at 6, 366 app. A.

114. See, e.g., Mähönen, *supra* note 102, at 42 (agreeing that a "firm standard is needed for ensuring interoperability . . . before large investments are made"); see also U.S. DEP'T OF COM., THE NATIONAL INFORMATION INFRASTRUCTURE: AGENDA FOR ACTION (Dec. 21, 1993) [hereinafter AGENDA FOR ACTION] (discussing U.S. policy concerns), at <http://metalab.unc.edu/nii/NII-Agenda-for-Action.html> (last visited Dec. 18, 2003). The U.S. administration's National Information Infrastructure ("NII") initiative intends to improve access to essential services, while encouraging private sector investment in the net's development through tax and regulatory policies that encourage innovation and promote long-term investment. See discussion *infra* Part V.1.

tive was to develop an independent network, away from direct federal funding or governance.

Following the successful effort to unify infrastructure standards, the NSF went on to gradually privatize the Internet backbone providers.¹¹⁵ It began with the local and regional networks and then expanded upon successful preservation of the compatible standardized infrastructure. Its efforts eventually turned into the complete privatization of the Internet's transit infrastructure, through the final privatization of the national backbone pipes and the creation of simple economies of scale in the provision of a standardized transit service.¹¹⁶ One of the main indications of this privatization policy initiative came with the December 23, 1992 announcement by the NSF regarding the cessation of funding to the ANS T3 Internet backbone.¹¹⁷ This announcement catalyzed the transition from the government-funded engineering-oriented Internet to the commercial Internet run by private providers of telecommunications services and business.

In the beginning of this process, these efforts were aimed solely at the local and regional networks. Through its "Acceptable Use Policy" ("AUP") the NSF prohibited backbone usage for purposes "not in support of research and education," intending to encourage commercial network traffic at the local and regional levels, while temporarily denying access to the national scale transportation facilities.¹¹⁸ It was only in 1995 that the NSF finally decides to reinstitute funding of the NSFNET backbone, thus allowing the full recovery of costs through competition on buying national-scale Internet telecommunications services by private networks.¹¹⁹

With the decision to privatize these services the government also committed part of its effort to setting up and facilitating the interconnection of different future private networks to exchange traffic via Network Access Points ("NAPs").¹²⁰ This decision was meant to further encourage diverse infrastructure equipment providers, such as data networking and

115. See Jay P. Kesan & Rajiv C. Shah, *Fool Us Once Shame on You—Fool Us Twice Shame on Us: What We Can Learn From the Privatizations of the Internet Backbone Network and the Domain Name System*, 79 WASH. U. L.Q. 89, 111-17 & n.6 (2001) (describing the privatization process of the NSFNET and providing a bibliographic list of short histories that discuss the privatization of the net).

116. *Id.* at 117.

117. See MacKie-Mason & Varian, *supra* note 103, at 274.

118. Barry M. Leiner et al., *A Brief History of the Internet, version 3.31* (Internet Society) [hereinafter Leiner, *Brief History*], at <http://www.isoc.org/internet/history/brief.shtml> (last modified Dec. 4, 2000).

119. *Id.*

120. Constance K. Robinson, *Network Effects in Telecommunications Mergers MCI Worldcom Merger: Protecting the future of the Internet*, 1192 PLI/CORP 517, 530 (2000).

telecommunications equipment providers and cable operators, to participate. Any company that wished to exchange traffic at a NAP, did so after negotiating the terms and conditions of that inter-exchange through bilateral agreements.¹²¹

With the enormous growth of Internet traffic followed by a new problem of congestion of the NAPs emerged the first signs of a free ride problem. That congestion came in the form of a bottleneck of connection speed across the Internet, followed by the typical telecommunications' loss of data and quality.¹²² Acting as interest groups, the larger networks responded to this problem by investing in private dedicated connection points over which they had a monopoly (provided earlier by the government). That initiative was responsible for partly restoring faster and more accurate connections.¹²³

As individual networks grew, more actions were needed to combat free ride failure in the nationwide backbone providers' extensive network investment. As a result, larger network providers began to create policies to restrict potential peer-to-peer arrangements between small and regional ISPs that had not invested in growing their networks.¹²⁴ These individual-to-individual peering agreements were then replaced by seller-customer transit agreements, where the national backbones charged the small networks or ISPs "transit fees" for carrying and terminating their traffic, while further maintaining their inter-connectivity services monopoly.¹²⁵

The ultimate establishment of public goods in users' access rights in the Internet backbone telecommunications services, and the minimization of the free ride failure were eventually achieved as usage became essentially free to all authorized end users. While most users were connected to a backbone through a "pipe" for which a fixed access fee is charged, the user's organization nearly always started covering the access fee as over-

121. *Id.* at 531.

122. *Id.*

123. *Id.* at 532.

124. MICHAEL KENDE, THE DIGITAL HANDSHAKE: CONNECTING INTERNET BACKBONES 4-9 (FCC OPP, Working Paper No. 32, 2000) (describing the analogy between the Internet transit and peering arrangements and the bill-and-keep and sender-keeps-all arrangements in traditional telephony interconnection arrangements, respectively), available at http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp32.pdf (last visited Dec. 18, 2003).

125. BENJAMIN ET AL., *supra* note 63; KENDE, *supra* note 124. In contrast, telecommunications carriers interconnecting with one another for the exchange of telecommunications traffic, still do it pursuant to Title II of the Telecommunications Act of 1996, which obliges all carriers to interconnect pursuant to reasonable terms and conditions. See 47 U.S.C. § 251 (2000).

head without any direct charge to the user. As a result, most users of the NSFNET backbone do not pay any pipeline fee to the service provider, but instead pay in order to get connected to their regional or mid-level network, and then are granted a connection to the NSFNET.¹²⁶

In essence, this provision of infrastructure backbone transit services as public goods was achieved based on a governmental policy aimed at minimizing only the negative affect of uncoordinated multiple infrastructure standardization efforts. Conceptually, this policy can be identified as a *positive default approach* to standardization. This is, in contrast to a *negative default approach*, in which not even negative externalities such as a technological arms race in infrastructure transit services are handled ex ante. For the infrastructure development phase, when a unified infrastructure is presumed to be efficient, this latter extreme approach does not seem justified, even by those who identify cyberspace as a state-free sphere complying only with alternative regimes under full consumer sovereignty.¹²⁷

In time, the creation of these first suspected monopolies by primary interest groups resulted in their vast control over access to the Internet's telecommunications services.¹²⁸ Because such vast monopoly powers

126. MacKie-Mason & Varian, *supra* note 103, at 269 n.1 (estimating that this conclusion is reflected in the rapid decline from expensive routers to expensive transmission links). For two additional secondary reasons why most Internet end-users do not pay usage charges: (1) residential local service tends to be flat-rated, and ISPs have located their POPs to maximize the number of subscribers who can reach them with a local call; and (2) ISPs typically connect to Local Exchange Carriers ("LECs") networks through business lines that have no usage charges for receiving calls. *See* WERBACH, *supra* note 4, at 50.

127. This regulative doctrine is analogous to Cyberanarchism referred to by Neil Netanel. *See* Neil Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 CALIF. L. REV. 395, 433-35 (2000); *see also* WERBACH, *supra* note 4, at 29.

128. *See* Kesan & Shah, *supra* note 115, at 148-59 (arguing that large backbone providers unfairly benefit from the lack of an interconnection policy, which penalizes smaller networks unjustly and limits new competitors). This situation typically happens when the largest backbone providers obtain the ability to dominate other backbones by threatening disconnection, degrading interconnection services, or charging monopoly prices for interconnection. *See also* Bickerstaff, *supra* note 109, at 101 ("[I]f left to market forces, many of the subsidies that are critical to public use of the Internet would disappear as [Independent Local Exchange Companies] would drive interconnection charges toward cost through usage-sensitive [sic] rates.").

would become almost inevitable, they would later demand counter-antitrust measures.¹²⁹

Conceptually, this governmental use of higher-quality telecommunications interest group participation conforms remarkably well to Olson's widely accepted collective choice theory.¹³⁰ According to this theory, smaller, influential, self-interested groups will be better able to organize collectively and combine their resources and minimize the free ride problem.¹³¹ This holds true for early high technology research and development ("R&D") standardization activities.¹³² To achieve access to broad dispersed public goods in cyberspace, namely users' access rights to telecommunications services in the Internet backbone networks, the standardization efforts were dominated by small influential groups of individuals or firms that were seeking to benefit themselves by establishing the Internet's infrastructure.¹³³ In practice, as in theory, then, these influential groups were small groups in the form of pre-organized homogenous telecommunications transit providers, with high per-capita stakes, rather than large heterogeneous potential customer groups with relatively small per capita stakes in the form of dispersed customers.¹³⁴ However, unlike in the earlier telephone industry, the researchers working on the ARPA's Internet working program in the early 1970s did not follow the model of the telephone system with its tightly integrated multiple networks into a centrally managed system, instead building a loose confederation of inde-

129. Lemley, *Antitrust*, *supra* note 94, at 1042; see I. DE SOLA POOL, *TECHNOLOGIES OF FREEDOM* 245 (1983); Ronald Hirshhorn, *Regulating Quality in Product Markets*, in *THE REGULATION OF QUALITY* 77 (Donald N. Dewees ed., 1983).

130. See MANCUR OLSON, *THE LOGIC OF COLLECTIVE ACTION* (2d ed. 1971). Mancur Olson's analysis of formalized models of institutional theory is one that has profoundly shaped the debate, and will be used henceforth as a theoretical point of reference.

131. See generally DANIEL FARBER & PHILIP P. FRICKEY, *LAW AND PUBLIC CHOICE* 23 (1991); Jonathan R. Macey, *Promoting Public-Regarding Legislation Through Statutory Interpretation: An Interest Group Model*, 86 COLUM. L. REV. 223, 231 (1986).

132. See, e.g., William J. Baumol & Janusz A. Ordover, *Antitrust: Source of Dynamic and Static Inefficiencies?*, in *ANTITRUST, INNOVATION, AND COMPETITIVENESS* 89 (Thomas M. Jorde & David J. Teece eds., 1992).

133. See OLSON, *supra* note 130, at 132-34, 162.

134. See Roger G. Noll, *Economic Perspectives on the Politics of Regulation*, in *HANDBOOK OF INDUSTRIAL ORGANIZATION* 1265 (Richard Schmalensee & Robert Willig eds., 1989); see also Hanseth & Monterio, *supra* note 3, at 173-74 (adding that the uniquely complex technological "invisibility" of the Internet infrastructure serves, in fact, as a negative incentive for participation by private users); Mähönen, *supra* note 102, at 40.

pendently managed networks.¹³⁵ Even so, ARPA assumed that such large-scale producers would be able to organize better than diffused consumers with lesser ability to reach a stable coordinated consensus needed for such new industry.¹³⁶

As a result, potential future consumers, such as the emerging Internet user community, would have found counter-organizing over-costly and substantively inefficient.¹³⁷ Accordingly, in the infrastructure development phase, legislators are generally biased in favor of these narrow economic interests at the expense of the general public.¹³⁸ Therefore, at this stage the government should have allowed and acknowledged an additional degree of monopoly power.¹³⁹

Thus, not surprisingly, the interest groups enrolled in this political action came from the leading telecommunications and cable service carriers such as AT&T, WorldCom, and Sprint.¹⁴⁰ The government's goal that only previously efficient, organized groups should be part of this preliminary commercial effort was realized.¹⁴¹ The rationale behind that policy was imported from previous experiences. The government determined that organized groups that had already paid the fixed costs of formation would have an advantage over their counterparts.¹⁴² This was especially important due to the anticipated susceptibility of these organized groups to the free ride failure. This free ride failure occurs when efficient interest groups

135. See Sharon Eisner Gillett & Mitchell Kapor, *The Self-Governing Internet: Coordination by Design*, in COORDINATING THE INTERNET 3-7 (Brian Kahin & James H. Keller eds., 1997).

136. For the theoretical perspective, see Olson, *supra* note 130, at 29; Noll, *supra* note 134, at 1264-65; see also Netanel, *supra* note 127, at 437, n.161.

137. See generally FARBER & FRICKEY, *supra* note 131, at 19 (discussing the theoretical framework); Netanel, *supra* note 127, at 438 (discussing cyberspace's application); Susan Rose-Ackerman, *Progressive Law and Economics—and the New Administrative Law*, 98 YALE L.J. 341 (1988) (same); Cass R. Sunstein, *Interest Groups in American Public Law*, 38 STAN. L. REV. 29 (1985) (same).

138. See KAY SCHLOZMAN & JOHN TIERNEY, ORGANIZED INTERESTS AND AMERICAN DEMOCRACY 317 (1986); Frank B. Cross, *Public Choice and the Judiciary*, 50 HASTINGS L.J. 355, 357 (1999); Frank H. Easterbrook, *Forward: The Court and the Economic System*, 98 HARV. L. REV. 4, 15 (1985).

139. POOL, *supra* note 129, at 245 (suggesting that “[u]nder these circumstances the best solution seemed to be to define a monopoly’s turf narrowly”).

140. Kesan & Shah, *supra* note 115, at 144 (suggesting that although thousands of companies provide Internet connectivity, they are all dependent upon MCI WorldCom, Genuity (formerly GTE), AT&T, Sprint, and Cable & Wireless); see also Neil Weinberg, *Backbone Bullies*, FORBES, Jun. 12, 2000, at 236.

141. See, e.g., Cooney et al., *Internet surge strains already shaky structure*, NETWORK WORLD, Apr. 3, 1995, at 1.

142. OLSON, *supra* note 130, at 28; cf. Noll, *supra* note 134, at 1265.

achieve an efficient outcome but have no ability to limit the benefits to its members, who originally had to confront additional, sometimes fatal, costs of formation.¹⁴³

In essence, in the infrastructure development phase of the Internet, the government took a dual regulative attitude towards what were two main purposes. The first was to coordinate a unified core standardized infrastructure, namely both the worldwide domination of the TCP/IP set of protocols, and the adoption of the hierarchical multi-layered architecture. Institutionally, research institutions were very cleverly effected in a way that allowed governmental governance of all the key aspects of TCP/IP and hierarchical multi-layered architecture adoption, while at the same time encouraging open and highly active research and academic collaboration.¹⁴⁴ Only with the success of this early regulatory goal did the government continue on to its second, substantively different goal. This second goal was the transfer of power over the Internet infrastructure to new market agents, namely, the telecommunications and cable industries. To achieve the second purpose, the government relegated itself to an indirect monitoring role, gradually pushing these interest groups to seize control over increasingly larger backbone levels. By giving away much of its power over the market for basic backbone transit *services*, the government deliberately avoided giving up hegemony over cyberspace's standardized *infrastructure*. It retained worldwide domination of the TCP/IP protocols,

143. See Noll, *supra* note 134 (suggesting that costs of formation are central to the ability to dominate the market); see also Julie E. Cohen, *Lochner in Cyberspace: The New Economic Orthodoxy of "Rights Management"*, 97 MICH. L. REV. 462, 522 (1998). A key insight of Olson that goes even further than Noll's is that such organization costs (as initial fixed costs) required to realize collective benefits, are an increasing function of the size of the group. See OLSON, *supra* note 130, at 53-57. To date, there is still no sufficient empirical evidence to apply Olson's claim to cyberspace. Furthermore, the costs of organizing groups that span international boundaries (i.e., cyberspace) are said to be decreasing in some respects due to communication technology and the Internet's radical ability to lower the significant costs associated with reproducing information and transmitting it over distance. Thus, even when Olson's application may have not yet been upheld adequately, the predictions of his theory can still serve as an early indicator in measuring cyberspace's institutional costs of formation. In fact, practice shows that earlier than 1995, private companies were merely overseen by the NSF in developing early TCP/IP hardware and software products, for example, private companies' participation in the advisory panel of scientists and engineers from academia and industry, including those involved in Computer Scientists Net ("CSNET"), to assist the Division of Networking and Communications Research and Infrastructure ("NCRI") staff in designing the first TCP/IP products. See Livinginternet.com, *NSFNET*, at http://livinginternet.com/ii_nsfnet.htm (last visited Dec. 3, 2003).

144. See Rutkowski, *supra* note 108, at 94.

and control over the root zone.¹⁴⁵ Whether this infrastructure production policy was institutionally justified will be the central question answered by the cost-benefit analysis of infrastructure standardization discussed below.

B. Infrastructure Standardization: The Cost-Benefit Analysis

Reflecting the specific costs of infrastructure standard-setting, the optimally efficient institutional choice of the infrastructure development phase was justifiably an *ex ante* governmental standard initiative propagated by federal agencies and governmentally-monitored research institutions.¹⁴⁶ Left to market agents alone, a pre-commoditized infrastructure environment bears too high a cost (and thus too high a risk of failure) to produce optimal core standards.¹⁴⁷ For the infrastructure development phase, a rationale planner should avoid any independent *de facto* or gray standardization coordination initiatives. Instead, coordination of infrastructure standardization should be entrusted to government standardization hegemony. As suggested earlier, this policy rule should be regarded as a positive default approach for minimizing the main negative externalities deriving from multi-standardization of core infrastructure. To achieve this goal, it is critical to identify the most efficient standard-setting institution.

In an early seminal work on regulation, Stephen Breyer suggests the basic theoretical framework for assessing the efficiency of such standard-setting activity.¹⁴⁸ As Breyer suggests, a rational standard setter, operating with broad statutory authority, would first define the adverse effect he seeks to control.¹⁴⁹ The standard setter would then use a preliminary rough cost-benefit analysis to identify the specific part of the general problem he intends to minimize, while obtaining the greatest improvement at the lowest cost. On balance, the standardization plan must be set at the level at which the total benefits exceed the total costs by the greatest comparative

145. See A. Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution*, 50 DUKE L.J. 17, 169 (2000) (suggesting that possessing control over the root zone the U.S. government had, in fact, only quasi-privatized the control over root server services); Mähönen, *supra* note 102, at 36-37.

146. See CARGILL, *supra* note 1, at 176; Hanseth & Monteiro, *supra* note 3, at 175.

147. As a general rule, that would also mean that in a few marginal cases, uniquely weak *de jure* infrastructure standards might be overcome by stronger self-regulated standards. One such example was the development of the TCP/IP infrastructure standardized set of protocols, which, jointly, quickly gained dominance over the OSI layer architecture. However, due to the coordinated hegemonic role taken by the U.S. government in that case, only a unified TCP/IP was adopted. See, e.g., Mähönen, *supra* note 102, at 43.

148. See BREYER, *supra* note 1, at 96-119.

149. *Id.* at 98.

amount and at which the marginal standardization benefits are equal to the marginal standardization costs.

Next, the standard setter would obtain information and design a standard, which would most efficiently reduce the targeted adverse effects to an economically reasonable degree.¹⁵⁰ Later, he would operate to enforce that standard through developed means that ensure compliance.¹⁵¹ Finally, he would monitor enforcement, while evaluating the standard's effectiveness, through occasional revisions.¹⁵²

After identifying the fundamental lack of interoperability in constructing cyber infrastructure products as public goods, a rational planner would then continue to categorize the preliminary rough benefit-cost analysis for each specific parts of the general problem (for example, the need for transferring, addressing and routing standards), which he wishes to minimize through possible standardization. Yet, bearing in mind the technological maturity of the TCP/IP suite of protocols, a more general cost-benefit analysis could be made for its various protocols. In providing a reasonable view of the adverse effect at issue such as the lack of interoperability and the inevitable expansion of early fragmentation of the Internet's architecture—such evolution would implicitly include the specific ingredients of the adverse problem for example, the lack of addressing, routing and transferring of this former broader framework.

Scholars have initially subdivided the costs associated with technical standardization into three types of costs. These are administrative costs, compliance costs and indirect costs.¹⁵³ *Administrative costs* are generally created by the standard setters through several subsidiary activities. The first part of the administrative costs comes from the costs of quality standardization while overcoming numerous anticompetitive concerns of the infrastructure development phase. The second part is the cost of R&D activity for standard development. The third part is the information cost or the cost of conveying information about infrastructure standard formulation. *Compliance costs* arise from the need to coordinate standard interoperability (or compatibility) and espouse technological convergence with the three general constituents of media: mass media (broadcast, cable and satellite TV, and radio), telephony (wired and wireless), and interactive computer services. Accordingly, compliance costs also include transaction

150. *Id.*

151. *Id.*

152. *Id.*

153. See OGUS, *supra* note 1, at 155-56; cf. Lemley, *Antitrust*, *supra* note 94, at 1045-51; Marcus Maher, *An Analysis of Internet Standardization*, 3 VA. J.L. & TECH. 5, 12-23 (1998).

costs and the need to reduce inefficient variety. *Indirect costs* consist of productive inefficiencies where resources are not allocated most efficiently. All these concerns still require further economic modeling, and for the purpose of this study will be broadly outlined, as follows.

1. *Administrative Costs*

a) Quality Standardization Costs

In previous telecommunications infrastructure standardization, primacy was given to technical performance-based efficiency over price-based efficiency.¹⁵⁴ This imperative quality rationale is true for any IT standardization activity, but is even more acute for infrastructure standardization to the degree that it implies a centralized and unified vision of the future of that technology.¹⁵⁵ Infrastructure quality assurances should be coordinated through delegated formal standard setters and monitored research institutions. This policy rule is based on several grounds.

First and foremost, under the alternative paradigm of price competition based on varying consumer demand,¹⁵⁶ the motivation of *de facto* standard

154. See, e.g., THE REQUEST FOR COMMENTS REFERENCE GUIDE 2 (Joyce Reynolds & Jay Postel eds., IETF Network Working Group, Aug. 1987) (giving a historical account of that policy in designing core infrastructure standards between the years 1969-1987), <http://www.ietf.org/rfc/rfc1000.txt> (last visited Dec. 3, 2003). Such policy was also embedded in the ITU rules and policies, regarding mobile telephony, HDTV, Radio Frequency Spectrum, etc. From the restructuring of the ITU in 1947 through the commercialization of telecommunications information in the 1980s, a separate federal structure was created for the “technical” organs, including the Administrative Radio Conferences (“ARC”) and International Frequency Registration Board (“IFRB”). These institutions preside next to the more “political” Plenipotentiary Conference (“PC”) and Administrative Council (“AC”), which came to maintain that technological qualitative primacy. See LEE, *supra* note 101, at 131-33; cf. THOMAS M. JORDE & DAVID J. TEECE, PRODUCT MARKET DEFINITION IN THE CONTEXT OF INNOVATION: AN EXPLANATION 236-37 (1987) (suggesting that competition in early technological phases of production is insensitive to price changes, but very sensitive to product feature changes and emphasizing that limiting new technology can bring an innovative development to an end, harming quality).

155. See, e.g., CARGILL, *supra* note 1, at 64 (justifying the central “regulatory style,” “where quality programs mandate a single procedure in order to fabricate a product that must meet stringent quality standards”).

156. See, e.g., ALAN O. SYKES, PRODUCT STANDARDS FOR INTERNATIONALLY INTEGRATED GOODS MARKETS 38 (1995) (adding that, in general, not all potential customers will be willing to pay the same for particular attributes in quality due to differences in underlying tastes or to differences in wealth). In its recent report, the National Telecommunications and Information Administration (“NTIA”) of the Department of Commerce concluded that the use of computers and the Internet varies significantly according to income, race, and ethnicity, and that the gap is increasing for certain demographic categories. See U.S. DEP’T OF COMMERCE, FALLING THROUGH THE NET:

setters would be to reduce marginal development costs. Firms will ultimately end up reducing relatively high undervalued costs of socially desirable R&D quality benefits.¹⁵⁷ Moreover, the focus on quality assurances is not only intrinsic to the development process, but would also be guaranteed if a long-term unified infrastructure production were to be preserved. In conclusion, hegemony of *de facto* standard setters in infrastructure design may not only decrease quality assurance, but may accordingly create a technologically inefficient standard market. Such market may be overcostly to maintain as seen with the formal OSI networking reference model of the Internet's architecture, developed by representatives of major computer and telecommunication companies beginning in 1983, and later overtaken by the TCP/IP networking reference model and set of protocols.¹⁵⁸

DEFINING THE DIGITAL DIVIDE § IIE, at <http://www.ntia.doc.gov/ntiahome/fttn99/contents.html> (last visited Dec. 3, 2003).

157. This core argument, limited here to the context of IT standardization, is part of a larger one, upheld by neoclassical economists, according to which average market agents tend to under-supply R&D activity (and thus benefits), resulting in these players' lack of incentive to explore different technological paths compared to their relatively lower worth. Eventually, market agents, left alone, will not generate a sufficient degree of variety of high-quality standards. See KENNETH ARROW, ECONOMIC WELFARE AND ALLOCATION OF RESOURCES FOR INVENTIONS: THE RATE AND DIRECTION OF INVENTION ACTIVITY 609-25 (1962); Richard R. Nelson, *Recent Evolutionary Theorizing about Economic Change*, 33 J. ECON. LITERATURE 48, 48-90 (1995). Nevertheless, to date, there is still no theoretical or empirical consensus that reduced competition leads to less R&D and fewer new products. Economic theory is ambiguous on this point and only industry-specific findings, for example, Internet infrastructure standardization, are relevant. See OLIVER E. WILLIAMSON, MARKETS AND HIERARCHIES: ANALYSIS AND ANTITRUST IMPLICATIONS 180 (1975) (stating that "the technological potential to innovate differs greatly across industries"); see also *F.T.C. Hearings on Global and Innovation-Based Competition*, 102d Cong. (1995) (statement of Dennis A. Yao), <http://www.ftc.gov/opp/global/yaotest.htm> (last visited Dec. 1, 2002); JOHN LIPCZYNSKI & JOHN WILSON, INDUSTRIAL ORGANIZATION: AN ANALYSIS OF COMPETITIVE MARKETS 249 (2001); CARGILL, *supra* note 1, at 37; Thomas M. Jorde & David J. Teece, *Rule Of Reason Analysis Of Horizontal Arrangements: Agreements Designed To Advance Innovation And Commercialize Technology* (1998), <http://www.ftc.gov/opp/global/jorde2.htm#5> (last visited Dec. 3, 2003).

158. Probably one of the main reasons for the final collapse of OSI was the fact that its vendors undervalued R&D investment and declined to invest in test suites for both quality assurances and compatibility. Interview with Carl Cargill, Director of Corporate Standards, Sun Microsystems, Inc. (Mar. 2003) [hereinafter Cargill Interview]. It should be added that there were other, related, reasons for the collapse of the OSI network model such as greater cost, lower efficiency and lateness to market. See *infra* note 178.

Second, the desire to propagate technology widely should also lower potential price-based competition in developing a unified infrastructure.¹⁵⁹ Initially, infrastructure standards as opposed to serial product applications such as operating systems or browsers might not be effectively exposed to premature price competition where infrastructure (and thus market) boundaries are pre-defined.¹⁶⁰ Alternatively, any inducement for premature product interchangeability and cross elasticity of demand between its substitutes will not lead to the clear differentiation of such outer boundaries.¹⁶¹ Essentially, such early price competition comes at the expense of the quality assurance that is needed in the early infrastructure development phase.¹⁶² Thus, lack of technological maturity optimally requires mandated centralized coordination.¹⁶³

Third, absence of consumer qualitative judgment is most acute with technological infrastructure because potential customers tend to overvalue the exterior *interface* of a standard at the expense of interior assurances and solid development.¹⁶⁴ In part, this is what led the U.S. government to lower its independent coordination role of *de facto* standard setters in the infrastructure development phase while continuing to monitor *de facto* standard setters' development activity.

Fourth, the combination of Akerlof's "market of lemons" insight,¹⁶⁵ with the realization that architecture and protocol designing imbed future

159. See discussion *infra* Part III.B.2.b.

160. Andrew C. Hruska, Note, *A Broad Market Approach to Product Market Definition in Innovative Industries*, 102 YALE L.J. 305, 316 (1992). In essence, this use of the potential competition doctrine in the market for infrastructure standards might apply to application standards that do not now exist but will most likely exist in the future. See generally U.S. DEP'T OF JUSTICE & F.T.C., HORIZONTAL MERGER GUIDELINES (1992) (defining market boundaries based on price competition), <http://www.ftc.gov/bc/docs/horizmer.htm> (last modified Apr. 8, 1997).

161. See ANTITRUST, INNOVATION AND COMPETITIVENESS 9 (Thomas M. Jorde & David J. Teece eds., 1992); Hruska, *supra* note 160, at 310 (noting that because product development begins years before the commercialization that would allow enforcing agencies to test claims of market power empirically, market definitions remain elusive).

162. Michael J. Trebilcock, *Regulating Service Quality in Professional Markets*, in THE REGULATION OF QUALITY 86-87 (Donald N. Dewees ed., 1983) (emphasizing that consumer ignorance of serious risks embedded in the wrong choice may call for prescribed quality standards irrespective of the price or the access affects of such standards). Later, in the implementation phase, quality standardization will serve to benefit price competition. See discussion *infra* Part V.B.

163. See Gillett & Kapor, *supra* note 135, at 18.

164. See CARGILL, *supra* note 1, at 36-37 (providing this unique technological rationale).

165. George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q. J. ECON. 488 (1970) (arguing that because quality is usually

market preferences,¹⁶⁶ leads to the conclusion that high-quality infrastructure standardization aimed at facilitating future transferability of information will eventually lower the anticipated informing and advertising costs of application standards that would potentially be demanded by *de facto* standard setters in the implementation phase.¹⁶⁷ Acknowledging the role of core technology in establishing future consumer preferences, it may also minimize tendencies of producers and consumers to settle for lower quality, lower-price products in the subsequent implementation phase.¹⁶⁸ This argument is relevant to any standardization activity¹⁶⁹ but it is more acute for infrastructure standardization where future market boundaries and motivations of *de facto* standard-setting are imbedded in infrastructure definitions. In that regard, *de jure* standard-setting should facilitate future competition and lower these costs.¹⁷⁰

b) Development Costs

Central governments most efficiently bear the cost of funding R&D activity and monitoring its successful performance by setting standards for

costly to produce, poor-quality products can outcompete high-quality products and the market equilibrium may entail the future production of suboptimally low-quality products exclusively, thus increasing informing and advertising costs).

166. Niva Elkin-Koren, *Copyright in Cyberspace—Rights Without Laws?*, 73 CHI-KENT L. REV. 1155, 1186 (1998); Lawrence Lessig, *Constitution and Code*, 27 CUMB. L. REV. 1, 14-15 (1997) (observing that “the architecture is the product of private interests”—whether the relatively open Internet Engineering Task Force or the absolutely closed Microsoft Corporation—and “code is political . . . the architectures that are established in cyberspace have normative significance, and . . . choices can be made about the values that this architecture will embed”); Lawrence Lessig, *The Constitution of Code: Limitations on Choice-Based Critiques of Cyberspace Regulation*, 5 COMM.LAW CONSPICUOUS 181, 184 (1997); 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*].

167. Cf. Akerlof, *supra* note 165.

168. *Id.*

169. See, e.g., CARGILL, *supra* note 1 (discussing potential competition in future standardized technologies); James J. Anton & Dennis A. Yao, *Standard-Setting Consortia, Antitrust, and High-Technology Industries*, 64 ANTITRUST L.J. 247, 264 (1995) (“Because standard-setting is forward looking, it may involve a competitively sensitive information exchange about future technologies and products.”); David A. Balto, *Standard Setting in a Network Economy* §§ I-II (Feb. 17, 2000) (“Competition may be affected in complementary goods, or even in next generation goods.”), http://www.ftc.gov/speeches/other/standardsetting.htm#N_40_ (last visited Dec. 3, 2003); Shapiro, *supra* note 37 (describing the components of the technological arms-race competition as including anticipating user needs and foreseeing and exploiting further hardware improvements).

170. Hruska, *supra* note 160, at 316.

research institutions. As with all other types of standards, infrastructure standards tend to freeze existing technology.¹⁷¹ However, infrastructure standards tend to freeze technology for longer periods. Thus, whenever *de facto* standard setters develop infrastructure they risk losing potential long-term market revenues. Ultimately, such risks are typically reflected in the lack of sufficient firm funding for development efforts.

Therefore, deciding who should develop infrastructure standards depends upon determining which institution can most efficiently fund the development of infrastructure standards. Because infrastructure standards are necessary long-run guides, mistakes made in setting them involve high risk of future harm.¹⁷² In any defective form, infrastructure standards would have to be reviewed and modified, if they are to become functional. This development and review process in itself would impose additional development cost on standard setters, thus increasing that same risk of error. To prevent these negative side effects, there is a need for central governments to play a central role in standard-setting activity and monitor its successful performance by autonomous standard setters such as research institutions.¹⁷³ On balance, because the small-to-medium enterprise (“SMEs”) of new applications in cyberspace is usually technically excused from a pre-commitment to build infrastructure, more entrepreneurs can finance and design more applications.

c) Information Costs

Formal industry standard setters can usually better internalize information costs and risks embodied in infrastructure standardization. Nevertheless, obtaining accurate information about prospective standards is likely the most costly activity for political institutions.¹⁷⁴ Moreover, conveying

171. See BREYER, *supra* note 1, at 105-06, 115-16; Mähönen, *supra* note 102, at 39.

172. See, e.g., Gillett & Kapor, *supra* note 135 (upholding the opposite conclusion for application standardization errors); see also LIPCZYNSKI & WILSON, *supra* note 157, at 225.

173. See AGENDA FOR ACTION, *supra* note 114 (presenting U.S. government support of this policy); RESEARCH CHALLENGES FOR THE NEXT GENERATION INTERNET 5 (Jean E. Smith & Fred W. Weingarten eds., Computing Research Ass’n, May 12-14, 1997), http://www.cra.org/Policy/NGI/research_chall.pdf (last visited Dec. 3, 2003) [hereinafter NEXT GENERATION INTERNET]; SHAPIRO & VARIAN, *supra* note 8, at 314.

174. BREYER, *supra* note 1, at 103, 109, 112 (describing information collection as the main cost in standard-setting); Eric J. Iversen, *Standardization and Intellectual Property Rights: Conflicts between innovation and diffusion in new telecommunications systems*, in INFORMATION TECHNOLOGY STANDARDIZATION AND STANDARDIZATION: A GLOBAL PERSPECTIVE 85-86 (Kai Jakobs ed., 1999) (suggesting that cost-structure of manufacturers of IT standards involves high investments risks, i.e., R&D costs, regularly in excess of 10% of turnover, with low variable costs); Tim Sloane et al., *Efficient Business-to-*

information about performance-based infrastructure standards is even harder, as such information is primarily quality-based rather than price-based.¹⁷⁵ Designers of infrastructure standards have varying preferences regarding quality and other value measurements (for example, price and service) of these standards.¹⁷⁶ Theoretically, central intervention would be unnecessary whenever *de facto* standard setters 1) have perfect information on the characteristics of infrastructure; 2) behave rationally in accordance with their preferences; and 3) have not generated externalities or monopolistic control on R&D information as a result of internal R&D decisions. Unfortunately, in cyberspace, this has been far from the case. Instead, *de facto* standard setters tended to keep their standards proprietary and closed sourced. Furthermore, even when sufficient information on the quality of infrastructure standards is made available, making decisions with the necessary degree of internalized social costs is difficult and expensive to coordinate among diverse, self-interested *de facto* standard setters.

Alternatively, dominant and competitively neutral formal industry standard setters, as repeat players (as opposed to governmental one-time players), typically hold a systematic advantage with regard to conveying information about infrastructure standard-setting activity.¹⁷⁷ Thus they should be supported by a government monitoring mechanism, as seen in the development of cyberspace.¹⁷⁸ Overall, even with lesser commercial know-how than *de facto* agents,¹⁷⁹ formal industry standard setters can

Business Relationships: How Analytics and XML Can Help, at <http://www.webtechniques.com/archives/2000/11/sloane/> (last visited Dec. 1, 2002); Michel B. Spring & Martin B.H. Weiss, *Financing the Standards Development Process*, in STANDARDS DEVELOPMENT AND INFORMATION INFRASTRUCTURE 289 (Brian Kahin ed., 1994)

175. Jorde & Teece, *supra* note 154, at 9 (stating that performance changes are more difficult to measure than price changes, because performance is multidimensional and may require various criteria of measurements).

176. *Id.*

177. CARGILL, *supra* note 1, at 37 (describing the industry consensus standardization process as a means of promoting innovative market neutrality); Sloane et al., *supra* note 174 (stating that “[t]o obtain the information required to make these decisions, it’s crucial for companies to evaluate B2B operations through vendor- and market-neutral analytics”).

178. Vendors have created consortia, for example, X/OPEN, hoping not to repeat the mistakes that damaged the implementations of OSI in the development phase and encouraged by the U.S. government. To develop standards, these consortia focused on collecting information and testing the implementations of the POSIX 1003.0 standard (ISO/IEC JTC 1 9945) (Test methods ISO/IEC JTC 1 13210, et al.) and other UNIX-like commands. See CARGILL, *supra* note 1, at 76, 221-22.

179. See Anton & Yao, *supra* note 169, at 254 (suggesting that exchange of commercial know-how may not require the exchange of much marketing information). Gillett &

usually better internalize information costs and risks embodied in infrastructure standardization.¹⁸⁰

2. Compliance Costs

Standardization coordinates technological developments efficiently.¹⁸¹ The ultimate technological goal of infrastructure standardization is to achieve complete integration while minimizing congestion among various elements of a technology, such as infrastructure and application standards. At the same time, the main economic difficulty to overcome is the motivation of *de facto* standard setters to bargain among themselves, to deal with their own potential incompatibility. Still, coordinating infrastructure is a complicated process, one that requires a great deal of interaction among the different phases of any comprehensive technology. Therefore, compliance costs arise out of the need to reduce inefficient variety, coordinate standard compatibility in a scarce environment, create technological convergence with other media, and accounting for existing transaction costs, as will be elaborated hereinafter.

a) Variety Reduction Costs

One of the important costs standardization derives from inefficient variability of products. Standardization policy attempts to prevent the adoption of standards viewed as “wrong” from a social point of view whenever such variety results in too many standards.¹⁸² Theoretically, in network environments, standard setters tend to prefer a small number of

Kapor further justify that early business environment in two ways. First, unlike commercial protocols developed recently, such as IBM's SNA, Digital's DECNET, and Xerox's XNS, infrastructure standard setters did not have the marketing resources of a large company behind them; second, nor was their design oriented toward any particular vendor's hardware. See Gillett & Kapor, *supra* note 135. Consequently, in most cases, such marketing will probably not involve personnel with much knowledge or authority in the marketing area. See Anton & Yao, *supra* note 169.

180. The funding mechanism will be described *infra* Part V.B.2.a.

181. See SUZANNE K. SCHMIDT & RAYMUND WERLE, COORDINATING TECHNOLOGY: STUDIES IN THE INTERNATIONAL STANDARDIZATION OF TELECOMMUNICATION (1998); Joseph Farrell & Garth Solaner, *Installed Base and Compatibility: Innovation, Product Preannouncements, and Predation*, 76 AM. ECON. REV. 940, 942 (1986) [hereinafter Farrell & Solaner, *Installed Base and Compatibility*].

182. See Carl Shapiro & Hal R. Varian, *The Art of Standard Wars*, CAL. MGMT. REV. 41, 8-32 (1999) [hereinafter Shapiro & Varian, *Standards Wars*]; see also SHAPIRO & VARIAN, INFORMATION RULES, *supra* note 8; W. Brian Arthur, *Competing technologies: An Overview*, in TECHNICAL CHANGE AND ECONOMIC THEORY (Giovani Dosi et al. eds., 1988).

largely dispersed standards in order to exploit network benefits.¹⁸³ Thus, compared to standards markets without network effects, network markets tend to have lower variety, which is socially desirable. Therefore, when standard setters choose a standard, they take into account the benefits from expected network size. Such markets may be characterized by a “tipping” effect where only one standard survives.¹⁸⁴ All the same, there remains a tradeoff between a network’s size and its standard variety. In practice, there is no guarantee that standard setters’ optimal solution to this tradeoff implements the socially optimal outcome.¹⁸⁵ Standard setters may adopt the wrong standard, from a social point of view, resulting in too many or too few standards.¹⁸⁶ In such cases, corrective intervention might be socially desirable. More notably, such a scenario could lead to a gravely inefficient outcome in the infrastructure development phase. Instead, infrastructure standardization homogeneity, best achieved by central policy planning, is typically more efficient.¹⁸⁷ One key way to achieve a reduction in inefficient variety was manifested in the Domain Name System (“DNS”)—the naming hierarchy that tells connected computers where to find particular web sites.¹⁸⁸ The need for such homogeneity is a direct consequence of the scarcity constraint on the production of infrastructure standards to which the DNS is subject. In regulation analysis, any definition of a regulative realm as scarce has meaningful consequences. In cyberspace, such scarcity intensifies the need to reduce inefficient variety of infrastructure standards.

To begin with, uncertainty in the future growth of users and demand for IP addresses, combined with uncertain user adoption of technical changes makes it difficult to predict how many addresses would be re-

183. See Shapiro & Varian, *Standards Wars*, *supra* note 182; SHAPIRO & VARIAN, INFORMATION RULES, *supra* note 8.

184. SHAPIRO & VARIAN, INFORMATION RULES, *supra* note 8.

185. *Id.*

186. *Id.*

187. See Gillett & Kapor, *supra* note 135.

188. The importance of DNS stability is widely agreed by different institutions. See M. Kaat, *Overview of 1999 IAB Network Layer Workshop 10* (IETF Network Working Group Oct. 2000) (providing a formal industry view), at <ftp://ftp.ietf.org/rfc/rfc2956.txt> (last visited Dec. 3, 2003); see also Management of Internet Names and Addresses, 63 Fed. Reg. 31,741 (1998) [hereinafter White Paper], available at http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm (last visited Dec. 3, 2003); Internationalized Domain Names Committee, *Discussion Paper on Non-ASCII Top-Level Domain Policy Issues* (ICANN Apr. 16, 2002) (providing ICANN’s view—warning that “the sudden introduction of a massive number of new TLDs would be a bad idea”), <http://www.icann.org/committees/idn/non-ascii-tld-paper.htm> (last visited Dec. 3, 2003).

quired to satisfy this demand.¹⁸⁹ As a practical matter, successful address allocation requires administrators with strong technical skills, not just political or legal expertise.¹⁹⁰ For example, administrators must have technical knowledge to preserve Internet transparency.¹⁹¹ Regrettably, much of this traditional end-to-end infrastructure transparency has been lost in the current Internet.¹⁹² This leads to complexity in application design and inhibits the deployment of new standard applications.¹⁹³ There are multiple causes for this loss of transparency, such as the deployment of network address translation devices and the use of private addresses, firewalls and application level gateways, proxies and caches.¹⁹⁴ These mechanisms increase fragmentation of the network layer, which causes operational irregularities for many applications on the Internet. Bearing in mind that some of the mechanisms have an intrinsic value (for example firewalls) any substantive regulative intervention on the matter may be controversial, may make end-to-end transparency unreasonably costly to restore.¹⁹⁵ Thus, preferably only competitively neutral formal standard setters, as suggested above, should coordinate such technical preferences.

Secondly, the current address allocation mechanism relies on voluntary trust between the competitive allocation authorities and consumers. Both compete based on their provision of an accurate and honest assessment of their requirements, so that appropriate amounts of address space are allocated.¹⁹⁶ At the same time, the requesters must trust the allocation authorities to be fair and impartial.¹⁹⁷ A user who wants to add a network to the Internet must first obtain a guaranteed-unique IP address. This IP address is allocated to a new network through Internet connectivity providers that typically have a block of addresses allocated to them by Regional Internet Registries (“RIRs”). From time to time, the Internet As-

189. See Gillett & Kapor, *supra* note 135, at 23.

190. See also David Randy Conrad, *Administrative Infrastructure for IP Address Allocation* (Aldea Communications, Feb. 2, 1996), at <http://aldea.com/cix/randy.html> (last visited Dec. 3, 2003).

191. The concept of a single universal logical addressing scheme and the mechanisms by which packets may flow from source to destination essentially unaltered.

192. Kaat, *supra* note 188, at 2 (“[S]pecifically the assumption that IPv4 addresses are globally unique or invariant is no longer true.”).

193. *Id.* at 3 (“It was however concluded that end to end transparency is desirable and is an important issue to pursue.”).

194. *Id.*

195. *Id.*

196. ICANN Address Supporting Organization, *Memorandum of Understanding* § 1 [hereinafter MOU], at <http://www.aso.icann.org/docs/aso-mou.html> (last visited Dec. 3, 2003).

197. See Conrad, *supra* note 190.

signed Numbers Authority (“IANA”) allocates large portions of address space to suballocate to providers as the RIRs see fit. Presently, four RIRs, operating in large geopolitical regions, are signatories to the voluntary Memorandum of Understanding executed on October 18, 1999.¹⁹⁸ This geopolitical tension is likely to remain into the future, as the number of RIRs is expected to remain relatively small.¹⁹⁹ Consequently, DNS allocation is already subject to two types of centralized policies. First, based on past growth rate estimates; registries feel compelled to allocate remaining Internet Protocol version 4 (“IPv4”) address space conservatively.²⁰⁰ Second, allocation authorities are attempting to simplify the Internet routing system by allocating larger continuous blocks of addresses.²⁰¹ Conversely, with the growing dominance of self-interested commercial networks on the Internet, the trust model for resource allocation is under severe multi-institutional pressure.²⁰²

In essence, IANA’s consensual decision-making mechanism may not clearly survive challenges to its legitimacy. As long as Internet service providers and IANA or Regional Internet Registries (“RIRs”) can cooperate, such multi-institutional pressure could be resisted.²⁰³ Should the historical cooperation between these two sets of organizations break down, the ISPs, again working in concert, could conceivably create a joint self-made RIR, allocating new addresses from the unused pool without regard to IANA/RIR policies.²⁰⁴ The third reason that DNS scarcity increases variety reduction costs is procedural. Due to the clear need for consensus on infrastructure adoption, any change, as valuable as it would be, would be too slow and thus expensive to achieve.²⁰⁵ On balance, as long as DNS is subject to the present pre-designed scarcity policy, that stability will be best achieved within the non-competitive technically oriented institutional framework of formal standardization. The latter would then serve to block

198. See MOU, *supra* note 196.

199. Thus, service areas will be of continental dimensions. See K. Hubbard et al., *Internet registry IP Allocation Guidelines* § 1, RFC 2050, (IETF Network Working Group Nov. 1996), at <http://www.ietf.org/rfc/rfc2050.txt> (last visited Dec. 3, 2003).

200. See Gillett & Kapor, *supra* note 135, at 24.

201. *Id.*

202. *Id.*; David Post, *Governing Cyberspace: Where is James Madison when we need him?* (ICANNWatch 1999) [hereinafter Post, *Governing Cyberspace*], at http://www.icannwatch.org/archive/governing_cyberspace.htm (“Any entity exercising control over the DNS will be subject to immense pressure to do more than mere ‘technical management.’”).

203. Conrad, *supra* note 190, at 23.

204. *Id.*

205. See Gillett & Kapor, *supra* note 135, at 23.

the temptation to create alternative unstable, inefficient infrastructure storage of Internet names and addresses.

b) Coordination Costs

In network environments, computer communications require complete and rigid compliance with basic interface specifications.²⁰⁶ More specifically, in cyberspace, unified specifications are critical to designing both cheaper core protocols of computer communications and achieving interoperability among its hierarchical layers.²⁰⁷ Coordination costs also arise whenever standards are revised. When a network industry settles on a single standard, it may be expensive to move toward a new, superior technology even when all users would theoretically be better off doing so. These switching costs fall into four categories.

To begin with, there is the cost of identifying, and then settling on, a specific infrastructure standard.²⁰⁸ Left to strategically dominant *de facto* agents, any non-binding attempt would face competing claims from self-interested commercial stakeholders, or worse, from different national or international standard-setting agencies. This emphasizes the need to assess future technological risks, such as fragmentation of the network layer and the ultimate risk of root splitting.²⁰⁹ Since standard-setting is often a “one-shot game” (thus, non-repetitive), in coordinating such consensus infrastructure standard setters might undesirably stick to an established inferior network technology (exhibiting excess inertia) or agents might undesirably switch to a new emerging one (exhibiting excess momentum).²¹⁰ With dif-

206. See FARRELL & SOLANER, *supra* note 12, at 1; Carl Shapiro & Robert Willig, *On the Antitrust Treatment of Production Joint Ventures*, 4 J. ECON. PERSP. 113, 114 (1990) (upholding the traditional rationale for joint ventures as a form of enterprise that can enable firms to attain economies of scale or scope that they could not otherwise achieve cheaply).

207. See, e.g., A. Lyman Chapin, *The Internet standards process*, RFC 1310, (IETF Network Working Group, Mar. 1992) (suggesting that in 1992, “[m]ost IETF members agree that the greatest benefit for all members of the Internet community results from cooperative development of technically superior protocols and services”), <http://rfc.sunsite.dk/rfc/rfc1310.html> (last visited Dec. 18, 2003); David R. Johnson & David G. Post, *And How Shall the Net Be Governed?: A Meditation on the Relative Virtues of Decentralized, Emergent Law*, in COORDINATING THE INTERNET 68-69 (Brian Kahin & James H. Keller eds., 1997) (upholding that conclusion for the larger regulative perspective in cyberspace).

208. See Gillett & Kapor, *supra* note 135, at 18.

209. This “Split DNS” (or “two faced DNS”), is also a corollary of this same fragmentation, followed by the loss in communication between a particular FQDN and an IPv4 address, whenever it ceases to be universal and steady.

210. See Farrell & Solaner, *supra* note 181 (for a sequential game model suggesting that both excess inertia and excess momentum can occur. With excess inertia, new tech-

ferent parties having simultaneous moves, the nature of the problem may be equivalent to coordination games, such as the prisoner's dilemma, where no efficient incentive to cooperate prevails, and parties prefer to act strategically. Left alone, self-interested *de facto* standard setters for example, RIRs, and even nations, would have an incentive to benefit their own customers for example, regional and local ISPs and their users, at the expense of the overall DNS stability at large.²¹¹ In contrast, when parties make sequential moves, such as when several infrastructure standards are competing a "battle of the sexes" game model prevails, and the lack of incentive to cooperate is not merely strategic, but results from the existence of alternative preferences and would, once again, justify central coordination of the prevailing infrastructure standards.

In addition, in the infrastructure development phase, switching costs between technological ingredients among standard setters are typically slower to overcome and often high.²¹² Seen through the perspective of standard setters, this once again results from the purposely-low level of effective price competition.²¹³ Also, once defective but potentially stable infrastructure technology is developed, infrastructure standards become extremely costly to change.²¹⁴ Finally, the incentive of preserving a coordinated installed base, may be positively externalized to the backbone telecommunications *services* market, as it may both encourage and facilitate the ability and will of early dominant infrastructure standard setters to remain pre-committed to future infrastructure transit compatibility. An early example of this model can be seen in the decision taken by eight subsidized industrial regional networks—BARRNet, CICnet, MIDnet, NEARnet, NorthWestNet, NYSERNet, SURAnet, and WestNet—which

nology may not be adopted even if it is superior to existing technology); Joseph Farrell & Garth Solaner, *Standardization, Compatibility and Innovation*, 16 RAND J. ECON. 70, 70-83 (1985) [hereinafter Farrell & Solaner, *Standardization*]. Paul David offered the anecdotal illustration of the perseverance of the "QWERTY" keyboard as an inefficient standard that was locked-in. See Paul A. David, *Clio and the economics of QWERTY*, 75 AM. ECON. REV. 332-337.

211. Notably, this is also the risk facing ICANN's present International domain name ("IDN") policies, as will be explained in Part V.C.

212. Joseph Farrell & Garth Solaner, *Coordination Through Committees and Markets*, 19 RAND J. ECON. 235 (1988).

213. See *id.* (following the authors suggestion that when the value of coordination on a standard is large relative to the value a firm attaches to adopting its preferred standard, the standard-setting committees are very likely to reach ultimate agreement on a standard but also vice versa).

214. Reidenberg, *Lex Informatica*, *supra* note 1, at 583 (estimating that the cost of change at the local level will be imposed directly on individual users, while change at the network level will be borne by network operators).

announced, the formation of the Corporation for Regional and Enterprise Networking (“CoREN”) on May 27, 1993. This decision was eventually intended to advance interconnection and blur the distinction between regional and backbone providers, by choosing MCI (subsequently acquired by WorldCom) as their backbone provider.²¹⁵ As a practical matter, by handling large amounts of Internet traffic, the CoREN backbone achieved a wide installed base of infrastructure technology, and accordingly, was able to bill regional affiliates an efficient internal transfer prices for the transport service provided.²¹⁶

Accordingly, it is unlikely that potential price competition will efficiently motivate *de facto* standard setters to switch infrastructures. Furthermore, *de facto* standard setters will generally be unable to establish monopoly power on infrastructure technology. Thus, they should not be encouraged to compete directly on infrastructure production and coordination at large.²¹⁷ Unless a monitored switch in infrastructure is centrally coordinated, it is highly expensive and typically not in the best interest of *de facto* standard setters to switch to uncoordinated, platform-dependent standards.²¹⁸ In sum, self-interested standard setters should not be left in charge of coordinating a new superior infrastructure because of direct early coordination sunk costs, best absorbed by *de jure* standard setters, and lost values from derivative negative network externalities.²¹⁹ A moni-

215. Michael A. Einhorn, *Pricing and Competition Policies for the Internet*, in PUBLIC ACCESS TO THE INTERNET 344 (Brian Kahin & James Keller eds., 1995).

216. *Id.*

217. *See, e.g.*, NICHOLAS S. VONORTAS, COOPERATIVE RESEARCH IN R&D-INTENSIVE INDUSTRIES 244 (1991). Vonortas stated,

In contrast [to “maturing segments of R&D-intensive industries” and the case of “declining industries”], multi-firm joint ventures for research are likely to be harmful in new, fluid technology industries . . . [C]ustomers of such industries are likely to lose from broad research cooperation since it will limit healthy competition in downstream markets.

Id.

218. *See, e.g.*, Jane K. Winn, *Consumers and Standard Setting in Electronic Payments Regulation*, 5 ELEC. BANKING L. & COM. REP. 11, 15 (discussing this dilemma in electronic payment standards).

219. FARRELL & SOLANER, *supra* note 12, at 4 (emphasizing the positive correlation between the early coordination (sunk) costs hurdle and avoiding later motivation to overcome dependent switching costs). One important mean of pre-committing leading *de facto* and even gray interest group standard setters to a stable infrastructure would be to “capture” their competitive motivations by enrolling them into infrastructure R&D by funding and subsidizing their early participation as was done in practice, as explained earlier.

toring policy regarding infrastructure developers is therefore imperative to generating the indispensable infrastructure installed base.

3. *Indirect Costs*

As a general matter, network effects positively benefit marginal participants due to the addition of new systems and the growing number of users.²²⁰ Typically, these effects suggest that network goods, priced by standard producers, and thus also network access costs, valued by the network consumers, would be optimally fixed, thus facilitating the widespread adoption of a standard.

However, due to the existing differences between the two main types of standards in cyberspace, namely infrastructure and application standards, each type of standard is affected by the network externality differently. Infrastructure standards seem to carry a positive network effect because there is a strong need for stable, performance-based infrastructure. Positive network effects are not merely a reflection of infrastructure interoperability but the very reason for their central *ex ante* adoption. Moreover, due to the non-competitive environment in which they are adopted, the positive influence of infrastructure standards on the installed base is indirect rather than direct because those standards end up leading to a derivative type of standards and markets,²²¹ in the form of application standards during a later standardization phase.

Accordingly, a derivative advantage of central coordination of infrastructure standardization is the minimization of the negative costs created by multi-standardization. Traditionally, in non-technological markets, these costs are present when persons other than the purchaser consume or use the product and may result from poor quality.²²² Conversely, in the early development phase, these costs are efficiently minimized, based on the qualitative rationale discussed earlier. For these reasons, central gov-

220. For primary works on the theory of network effects, see Farrell & Solaner, *Standardization*, *supra* note 210; Farrell & Solaner, *Installed Base*, *supra* note 210; Michael L. Katz & Carl Shapiro, *Network Externalities, Competition and Compatibility*, 3 AM. ECON. REV. 73, 424-40 (1985). See also Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CALIF. L. REV. 479 (1998).

221. For literature on indirect network effects, see Chien-fu Chou & Oz Shy, *Network effects without network externalities*, 8 INTL. J. INDUS. ORG. 259-70 (1990); Chien-fu Chou & Oz Shy, *Partial compatibility and supporting*, 41 ECON. LETTERS 193-97 (1993); Jeffrey Church & Neil Gandal, *Complementary Network Externalities and Technological Adoption*, 11 INTL. J. INDUS. ORG. 239-60 (1993); Jeffrey Church & Neil Gandal, *Network Effects, Software Provision, and Standardization*, 40 INTL. J. INDUS. ORG. 85-103 (1992).

222. Hirshhorn, *supra* note 129, § 3.

ernments are arguably best at achieving an ex ante critical mass of infrastructure standards, while most efficiently internalizing the costs of diffusing network effects, through funding industry organizations in research and ultimately, in endorsing and formally adopting standards.²²³

In contrast to infrastructure standards, application standards are largely subject to positive ex ante network effects in their traditional competitive form. Accordingly, they only create the need for ex post intervention meant to minimize negative effects, largely through antitrust law.²²⁴ Here it is commonly agreed that in a competitive environment, new generations of standards will work at a significant disadvantage unless they are compatible with prior generations, so that the installed base of consumers could transfer data from one product to the next subject to productive competition between standards and their *de facto* developers.

IV. THE MODIFICATION PHASE: THE COMMERCIALIZATION OF CYBER STANDARDS

During the development phase, the U.S. government directly coordinated infrastructure design. In fact, the TCP/IP model was originally born out of the Department of Defense's ARPANET.²²⁵ Sponsored and coordinated by ARPANET, TCP/IP was meant not to be owned by any corporation or individual, and was thus created outside the dominion of commercial *de facto* standard setters. As an open standard, the TCP/IP protocols are also defined by RFCs ("Requests for Comments"), which are now part of the public domain. Infrastructure production was primarily technically, rather than commercially, motivated. That policy eventually changed, with both technological and economic development taking place. These central changes are what arguably led to the substantial commercialization of standard-setting activity in cyberspace, followed by a substantive growth in the number and influence of *de facto* and gray standard setters. Empirically, it has yet to be proven whether these changes should be regarded as an independent phase in the technological standardization process or merely an intermediate technological step between two substantive phases

223. See, e.g., SHAPIRO & VARIAN, *supra* note 8, at 313-15 (discussing governments as cost-efficient in achieving critical mass of networks).

224. *Id.* at 313.

225. Dr. Vinton G. Cerf led the design team at Stanford University that developed TCP/IP and managed the U.S. governmental DARPA Internet project from 1976-1982. Along with Robert Kahn, both men are generally accepted as the early inventors of the TCP/IP as early as 1974. See Vinton G. Cerf & Robert E. Kahn, *A Protocol for Packet Network Intercommunication*, 22 IEEE TRANSACTIONS ON COMM. 637 (1974).

of standardization. Even so, the central implications of the modification phase on the institutional identity criterion are worthy of discussion.

In 1995, soon after federal funding of the North American backbone ceased, private companies began operating their own backbone networks and selling telecommunications service access to their networks and the Internet. That privatization turned the Internet into a wide-ranging linkage of interconnected public and private computer networks joined by privately owned telecommunications facilities. This development paralleled the experience of traditional telecommunications standardization where a similar shift came in the mid-1980's, with the further growth of private-sector participation supported by arguments that manufacturers, carriers, and users should take part in formulating policies directly affecting them.²²⁶

One of the consequences of the rapid growth of the user community was a growing demand for additional facilitating standards.²²⁷ Based on a largely platform-dependent approach, the resulting software products facilitated the basic Internet data communication infrastructure.²²⁸ Soon after the uniform TCP/IP infrastructure was in place, new commercial network effects provided incentive for vendors to build TCP/IP compatible products. This technological change seems to have been the main constraint leading to the commercialization of the Internet's standards.²²⁹ Yochai Benkler recently noted that there were three major, chronologically close, technological developments that marked the shift to commercialization in cyberspace: the web server, the first graphical browser, and

226. LEE, *supra* note 101, at 121-22.

227. See WERBACH, *supra* note 4, at 17 ("Like a digital tornado, the vortex continues, as the new level of demand creates the need for additional capacity, and so forth.")

228. The derivative dependence of application standards on infrastructure is of central technological importance, as it explains the shift between the first two phases, as part of the process argument, described earlier. For a discussion supporting this premise, see CARGILL, *supra* note 1, at 28-31, 119 (discussing "implementation standards," using the example of the IEEE 802.3 Ethernet infrastructure standard); WILDER, *supra* note 14, at 6, 357; Leiner, *Brief History*, *supra* note 118, at 12; Mähönen, *supra* note 102, at 42. Technically, the interchange between cyberspace's standardized infrastructure and applications is vertically coupled: network technology drives the applications, and applications drive the networks. This continuous feedback is also known as the "spiral design" process. See NEXT GENERATION INTERNET, *supra* note 173.

229. Kesan & Shah, *supra* note 115 (suggesting that the first use of the term "commercial use" was made by Stephen Wolff, Director of the NSF Division for Networking and Communications Research and Infrastructure, who had placed the term in the backdrop of his formal statement); see also COMMERCIALIZATION OF THE INTERNET SUMMARY REPORT n.93, RFC 1192 (Brian Kahin ed., IETF Network Working Group Nov. 1990), at <http://www.faqs.org/rfcs/rfc1192.html> (last visited Dec. 18, 2003).

the first proprietary service provider.²³⁰ Soon after these developments, the Internet became highly commercial in nature. According to the FCC, the Internet has grown from 10 million users in 1995 to over 40 million by 1999.²³¹ A similar pattern holds for the purchase of Internet services, which grew from \$6.2 billion in 1995 to over \$300 billion in 2002.²³²

The shift to platform-dependent compatibility was followed by consumer-oriented price competition.²³³ This shift ultimately led to the commercialization of application software.²³⁴ Eventually, cyber standardization became very closely related to the commercial decision-making done in industrial companies.²³⁵

Thus, a central change in the standardization process was a shift from centralized, government directed, standardization planning to short-term *de facto* standardization. Traditionally, industrial-age innovation followed the linear sequence from scientific discovery to applied research and development, followed by production and marketing. The standardization process is time consuming, particularly if the number of participants having divergent preferences is high. When a market exhibits rapid tech-

230. Yochai Benkler, *Net Regulation: Taking Stock and Looking Forward*, 71 U. COLO. L. REV. 1203, 1206 (2000) (“[Those three changes] changed it all. It turned out that the net was not in the future; it was here . . . in what suddenly became the new popular (not to say mass) medium.”); cf. Lemley, *Antitrust*, *supra* note 94, at 1052; Lawrence Lessig, *The Limits in Open Code: Regulatory Standards and the Future of the Net*, 14 BERKELEY TECH. L.J. 759, 760-61; Leiner, *Brief History*, *supra* note 118, at 13; Robert Cailliau, *A little History of World Wide Web: From 1945-1995* (1995), at <http://www.w3.org/history.html> (last visited Dec. 1, 2002).

231. See F.C.C., *CONNECTING THE GLOBE: A REGULAR S GUIDE TO BUILDING A GLOBAL INFORMATION COMMUNITY* (1999) (discussing the FCC’s policy record), at <http://www.fcc.gov/connectglobe/sec9.html> (last visited Dec. 1, 2002).

232. *Id.*

233. See FARRELL & SOLANER, *supra* note 12, at 5; Manfred M. Fisher & Börje Johanson, *Networks for Process Innovation by Firms: Conjectures from Observation in Three Countries*, in *PATTERNS OF A NETWORK ECONOMY: ADVANCES IN SPATIAL AND NETWORK ECONOMIES* 264 (Börje Johanson et al. eds., 1993) (arguing that “[i]n finished standardized product (or mature products) markets, which serve for mass production—price competition prevails, as a quantitative measurement, is the main criterion for the decision making of buyers”).

234. LESSIG, *supra* note 8, at 52.

235. See, e.g., Mark A. Lemley & David McGowan, *Could Java Change Everything? The Competitive Propriety of a Proprietary Standard?*, 520 PLI/PAT 453, 471; see also Ken Krechmer, *Cathedrals, Libraries and Bazaars*, Remarks at the Association of Computing Machinery (ACM) Symposium on Applied Computing Meeting (Mar. 10-13, 2002) [hereinafter Krechmer, *Cathedrals*] (suggesting that the production of standards and commercial software is becoming closely related, extracting ten lessons that may apply to standards development as well as software program development), at <http://www.csrstds.com/cathedrals.html> (last visited Dec. 2, 2003).

nological growth, as the cyber market has, the time required to develop an IT standard is typically longer than a single product or system's life cycle. To cope with this, standards bodies began, in the infrastructure development phase, to act in anticipation of the technology, developing standards before products were produced.²³⁶ In the infrastructure development phase these were known as anticipatory standards and included, for example, V.32 modem, X.25 packet interface, ISDN and ultimately TCP/IP.²³⁷

In practice, this standardization work, even at the technical committee level, was not related to R&D work or innovations. Innovations were submitted to the standards process, wherein state of the art technology froze to standards. Accordingly, in the development phase, standards were typically designed to include available high technology specifications, but did not drive towards new innovations within the standardization process itself. Yet with the growing shift to commercialization of application standards in the implementation phase, there has been an erosion in the effectiveness of the anticipatory standards process. This is evident in the rise of informal standardization. Thus, in practice, gray and *de facto* activity was initiated and driven by commercial implementers.²³⁸ Eventually, with less efficient incentives towards strategic social planning, and as a result of rapidly increasing consumer demand for application standards, the development and implementation of standards became decreasingly less anticipatory.²³⁹ Instead, anticipatory standards became responsive as they

236. CARGILL, *supra* note 1, at 45-46; Mähönen, *supra* note 102, at 38 (concluding that "the place for innovations is outside the formal standards meeting—standards just agree on the solution").

237. In fact, Bonino and Spring argue that anticipatory standards act as mechanisms for collective planning, i.e., they are an embodiment of a central industrial policy. Accordingly, their prevalence serves as an additional rationale favoring central standardization of the developmental phase. See Weiss & Spring, *Standards as Change Agents*, *supra* note 28, at 99.

238. See, e.g., Egyedi, *supra* note 3, at 55.

239. *Id.* at 54-55 (suggesting that, in fact, application standards development has began to occur in parallel). In a conversation with Carl Cargill, Egyedi further suggested that anticipatory standard-setting activity (as in the early phase of cyberspace standardization), is now practically "dead, followed by the shift to standardize 'existing practice.'" See Cargill Interview, *supra* note 158. For example, ECMAScript, which was standardized by ECMA—based on the Javascript programming language, established earlier by Netscape. *Id.*; see also Elaine Baskin et al., *The Six Dimensions of Standards: Contribution Towards a Theory of Standardization 2* (Nov. 17, 1999) (suggesting that due to high market demand followed by the decrease in anticipatory standardization, large users with specific needs may force standards creators to become standards seekers), at <http://www.standardsresearch.org/presentations/6Dimen.doc> (last visited Dec. 18, 2003).

adapted to preceding innovative activity that was only later standardized.²⁴⁰

The major risk of such rapid, market-oriented, standard-setting is the premature stifling of innovation.²⁴¹ It may produce design standardization too early in the technological life cycle. A technology may thus be forced into "early maturity" not because of technological limitations but rather by competitor collusion.²⁴² Consequently, with the growth of application standardization, a new institutional balance had to be struck. This balance was finally established in the implementation phase.

V. THE IMPLEMENTATION PHASE: THE RISE OF AUTONOMOUS INSTITUTIONS

Whenever technology matures, the explosion of new markets for both early core services and markets for peripheral technology, in the form of application-standardized products should promote the rise of autonomous standard-setting institutions. As cyberspace entered a substantive new phase of commercialization, network effects provided incentive to vendors to build TCP/IP-compatible products. Ultimately, commercial decision-making by application producers became a controlling factor in cyberspace's standardization reality. Thus, in the face of an increasing number of *de facto* and gray standard-setting institutions,²⁴³ government intervention would optimally take a secondary role. In practice, while the path has been neither clear nor straight, the trend of governmental interpretation of the public interest in the United States exhibits a definite pattern of decreasing intervention in standardizing cyberspace.

In the implementation phase, only self-restrained political institutions, typically governmental agencies and particularly the FCC, will come close to optimizing competition among autonomous standard setters for creating beneficial standards. However, a role for voluntary industry regulation to formalize *de facto* or gray standardization will become essential due to

240. See Krechmer, *Cathedrals*, *supra* note 235.

241. CARGILL, *supra* note 1, at 118 (concluding that "if standards, voluntary or otherwise, are introduced, they will fail, since standards act to stabilize a market"); Mähönen, *supra* note 102, at 38; Sloane, *supra* note 25, at 8 (exemplifying the HTML protocol); *cf.* LIBICKI, *supra* note 3, at 14-16 (suggesting that the optimal moment for standardizing should be "if the technology matures before the market takes off standardization can occur smoothly in between").

242. FREDERICK BETZ, *MANAGING TECHNOLOGY* 75 fig. 2 (1987); *see also*, Lemley & McGowan, *supra* note 220, at 471. In the following part the resulting institutional consequences of this change will be examined.

243. See CARGILL, *supra* note 1, at 102-03.

new risks of ex ante technological stagnation and/or ex post anticompetitive effects on the one hand, and the need to sustain private competition, on the other. By the same token, growing concerns about governmental technological bias toward standards that best serve its policies through “code control” lead to the conclusion that formal or *de jure* industry standardization may be the most efficient mechanism for chilling direct governmental incentives for mandated standardization, beforehand or ex post. In accordance, this part presents an updated cost-benefit analysis of the different standardization costs. This cost-benefit analysis supports the comparative institutional analysis.

A. Application Standardization: The Cost-Benefit Analysis

Application standards should primarily be the product of competition, subject to the widespread need to develop, approve, and compatibly adapt applications to infrastructures and other complementary applications. These production constraints suggest a delicate balance between two seemingly contradictory processes: the creation of innovative product variety,²⁴⁴ and the reduction of that variety through user-based qualitative selection. Effective technological acceptance requires that these two processes be kept in balance.²⁴⁵ In the highly competitive environment of cyberspace, this balance is not always maintained because of genuine risks of inefficient production. As far as development per se is concerned, this balance derives from the common threat that rapid commercial activity will curtail innovation prematurely. This may lead technology into early maturity at a point where standards are still inefficient. Thus, if a leading standard is set before a technology reaches maturity, more radical innovation may be economically inefficient. As anticipatory standardization has declined, the risk of early maturity seems only to have grown. Moreover, as far as standard adaptation and approval (or formalization) are concerned, formal industry standard setters should be in charge of optimizing compatibility, so as to generate and maintain new and competitive economies of scale in application standards. Thus, the need to diminish the basic cost of early maturity resulting from anticompetitive collusion and inefficient incompatibility may necessitate a role for formal industry policy planners in optimizing *de facto* and gray standardization. Projected costs of this sort of policy planning fall into three categories: administrative, compliance, and indirect.

244. When n actors bilaterally agree to a set of standards, then $n*(n-1)/2$ rules must be defined. See SHAPIRO & VARIAN, *supra* note 8; Shapiro & Varian, *Standards Wars*, *supra* note 182.

245. See SHAPIRO & VARIAN, *supra* note 8, at 233.

1. *Administrative Costs*

a) *Eliminating Duplicative Efforts*

Standardization authorities and formal standardization organizations should encourage cooperation and prevent R&D overlap.²⁴⁶ Proceeding on this assumption, Congress passed legislation, first in 1984 through the National Cooperative Research Act,²⁴⁷ and later, in 1993 through the National Cooperative Research and Production Act (“NCRPA”),²⁴⁸ indirectly aimed at facilitating autonomous commercial innovation initiatives. Designed to accelerate existing pro-competitive policy, the NCRPA clarified how U.S. antitrust laws substantively applied to joint R&D and joint production ventures. Drafted to promote R&D activity by providing a special antitrust regime for joint ventures, the NCRPA requires U.S. courts to judge the competitive effects of a challenged joint R&D, joint production venture, or a combination of the two, in appropriate relevant markets applying a “rule-of-reason” legal standard.²⁴⁹ This rule of reason takes into account “all relevant factors affecting competition.”²⁵⁰ The NCRPA also instituted a voluntary safe harbor procedure whereby the Attorney General and the FTC may be notified in advance of a joint R&D or production venture.²⁵¹ Accordingly, numerous U.S. consortia have already filed notices under section 4305(a) of the NCRPA²⁵² in order to limit their potential penalties and liabilities for anticompetitive standardization activities.²⁵³ Overall, however, the NCRPA has not been widely exploited by

246. See CARGILL, *supra* note 1, at 131-38; Chapin, *supra* note 207; Thomas M. Jorde & David J. Teece, *Acceptable Cooperation Among Competitors in the Face of Growing International Competition*, 58 ANTITRUST L.J. 529, 538 n.28 (1989).

247. National Cooperative Research Act of 1984, Pub. L. No. 98-462, 98 Stat. 1815 (codified as amended at 15 U.S.C. §§ 4301-4306 (1993)).

248. National Cooperative Research and Production Act, 15 U.S.C. §§ 4301-4306 (1993) [hereinafter NCRPA]. By enactment of the NCRPA Congress reinforced the existing tolerance expressed for joint ventures engaged in legitimate research and development and standard-setting projects, mandating application of the rule of reason in cases brought against registered ventures. See Jack E. Brown, *Technology Joint Ventures to Set Standards or Define Interfaces*, 61 ANTITRUST L. J. 921, 933 n.55 (1990) (adding that the congressional interest in furthering joint activities was also reflected in the repeated legislative attempts to extend the NCRPA’s protections to joint production and manufacturing, as well as research ventures).

249. 15 U.S.C. § 4302.

250. *Id.*

251. 15 U.S.C. § 4305(a).

252. See DENNIS W. CARLTON & JEFFREY M. PERLOFF, *MODERN INDUSTRIAL ORGANIZATION* 522 (3d ed. 2000).

253. See also LIPCZYNSKI & WILSON, *supra* note 157, at 229; W. Rupert Maclaurin, *The Process of Technological Innovation: The Launching of a New Scientific Industry*, 40

standard setters.²⁵⁴ This can likely be attributed to the difference between the protections present in the Act and the protections Congress apparently intended to grant.²⁵⁵ Designed primarily to enhance early innovative R&D activity, the amended 1993 Act arguably still suffers from certain limitations that result from the limited view of the technological standardization process.

First, subject to a few exceptions as set forth in 15 U.S.C. §§ 4301(b)(2)(A)-(C), NCRPA excludes joint marketing and sales ventures.²⁵⁶ The Act's distinction between "pure" research and its attendant business implementation such as marketing and selling, in both time and space is potentially artificial.²⁵⁷ In order to commercialize a product effectively, development engineers must receive feedback from the production and marketing stages.²⁵⁸ Moreover, especially in the implementation phase when standard-setting committees are no longer engaged in significant anticipatory standardization, the production of application standards gets a new commercialization and marketing emphasis instead of the R&D orientation seen in the early development phase. Indeed, innovation in manufacturing processes may be just as important for the success of a new product as the design innovations conceived in the early development phase.²⁵⁹

Second, the Act exhibits a xenophobic quality by disqualifying non-American joint ventures.²⁶⁰ Thus, the new law did not protect many production ventures, because the "principal facilities for such production"

AM. ECON. REV. 90 (1950). Another significant contribution to this policy came in 1987 with the agreement between the International Organization for Standardization ("ISO") and the International Electrotechnical Commission ("IEC") to cooperate in the Joint Technical Committee ("ISO/IEC JTC 1"). The purpose of this cooperation was to eliminate the serious overlap between ISO and IEC in their standardization activity. *See* LEE, *supra* note 101, at 44-45.

254. *See* Joseph Kattan, *Contemporary Antitrust Analysis of Joint Ventures: Why It Makes Sense to Stay the Course*, Remarks at the Federal Trade Commission's Hearings on Joint Venture Project (June 5, 1997), at <http://www.ftc.gov/opp/jointvent/kattan.htm> (last visited Dec. 3, 2003); Krechmer, *Cathedrals*, *supra* note 235 (suggesting that the production of standards and commercial software is becoming closely related, extracting ten lessons that may apply to standards development as well as software program development).

255. Kattan, *supra* note 254, Krechmer, *Cathedrals*, *supra* note 235.

256. 15 U.S.C. § 4301(b)(2) (2003).

257. *See* Anthony L. Clapes, *Blinded by the Light: Antitrust Analysis of Computer Industry Alliances*, 61 ANTITRUST L.J. 899, 916 (1993).

258. *See* Jorde & Teece, *supra* note 246, at 582, 589.

259. *Id.*

260. *Id.*

clause mandates that production ventures have their principal production facilities in the United States in order to qualify for coverage.²⁶¹ Furthermore, according to the Act “each person who controls any party to such venture” must be a United States company or must be incorporated in nations that treat United States companies fairly under their own antitrust laws governing production joint ventures.²⁶² Since both ad hoc and gray standard-setting is taking on greater international significance, the Act must be amended to reflect the international realities that change introduces.

In addition to coordinating R&D cooperation, another means of preventing overlap is achieved through the industry’s expanding voluntary promotion of electronic publishing of research materials. By increasing the efficiency of information flow to manufacturers trying to improve productivity it is possible to diminish the inefficiency associated with protracted trial and error in manufacturing processes.²⁶³ At the same time, it is important for manufacturers in this environment of increasing competition to protect their R&D investments against misuse in other markets.²⁶⁴ In practice, however, there is a notable growth in the standardization community in common R&D joint ventures, entered into to share high R&D costs and uncertainty about market developments. Accordingly, several industry standardization organizations, for example IETF, make their standards (or parts of them) called RFCs, available electronically and waive all publishing or use fees.

b) Reducing Search Costs

In markets of application standards, searching for information regarding the different value measurements of standards such as costs, quality,

261. 15 U.S.C. § 4306(1).

262. 15 U.S.C. § 4306(2). H.R. 1313 passed the House of Representatives on May 18, 1993. *See House Passes Bill Easing Antitrust Law for Parties Involved in Joint Ventures*, 64 ANTITRUST & TRADE REG. REP. (BNA) No. 1615, at 600 (May 20, 1993).

263. *See, e.g.*, Paul A. David & Shane M. Greenstein, *The Economics of Compatibility Standards: An Introduction to Recent Research*, 1 ECON. INNOVATION & NEW TECH. 1, 3-42 (1990).

264. Industry standard setters may try to use the information they control to influence market trends, against the public’s interest, while raising bargaining threat costs of standardization activities to a non-cooperative level beyond the NCRPA antitrust “rule of reason.” In “unreasonable” situations there will be a need for governmental intervention. Moreover, if certain de facto standard setters are excluded from such a joint venture, they may be competitively disadvantaged because they cannot conduct research on the same scale as the members of the venture. *See, e.g.*, LAWRENCE A. SULLIVAN, *HANDBOOK OF THE LAW OF ANTITRUST* 298-303, nn.167-70 (1977) (discussing the anticompetitive effects of membership restrictions).

and services should be communicated to consumers in a way that is easily comprehended and used as the basis for comparison. In such markets it is difficult to measure the quality or value of these products for consumers. This intrinsic difficulty is true for information markets at large.²⁶⁵ It is thus also true for consumer-oriented markets of application standards or software products.

As a result of this tension and because information about quality is more costly to supply and process than information as to price, public agents with sufficient information to make and certify quality judgments are needed to act as monitoring proxies for consumers approaching application standard markets.²⁶⁶ In cyberspace, such formal monitoring of standard-setting was largely achieved by creating a consensus around individual technologies. While the government is best suited to subsidize such activity,²⁶⁷ it was competitively neutral industry organizations that took charge of diminishing the search costs necessary to ensure the adoption of adequately efficient standards. In such a situation, industry standard setter's monitoring proxies should avoid the situation in which the market either does not pick up momentum because of too much variety, or malfunctions due to market failures.

Standard development best contributes to the collective R&D learning process when inefficient sources of variety in design are avoided by minimizing information costs through formal industry intervention. At the same time, the choice made by the industry naturally adds to the costs of the system, since rulemaking power remains with the *de facto* standard setters. In order to preserve the competitive benefits, while maintaining the 1997 Report's self-regulatory paradigm for application standardization, formal or *de jure* industry standardization organizations should be limited only to a secondary role of monitoring and certifying *de facto* production in the implementation phase.²⁶⁸

2. Compliance Costs

To be effective, infrastructure must be hegemonic and thus require compliance with infrastructure standards. Applications standards require a different type of compliance. There is a smaller need for a unified vision of anticipatory standard-setting activity for both internalizing and uli-

265. ARROW, *supra* note 157, at 615.

266. See Akerlof, *supra* note 165; Trebilcock, *supra* note 162, at 92-95; Kip W. Viscusi, *A Note on "Lemons": Markets and Quality Certification*, 9 BELL J. ECON. 277 (1978).

267. See discussion *infra* Part V.B.2.a.

268. Cf. OGUS, *supra* note 1, at 110.

mately reducing existing costs through formal institutions. In application standard-setting, compliance with standard-setting became a regulatory *preference*, not a requirement.

However, even in this competitive environment, too great a departure from unvarying standards by *de facto* standard setters still generates significant compliance costs. Firms are presently incentivised to overstate the costs of complying with other developers in order to increase the pre-bargaining threat costs of a desired coordinated standard.²⁶⁹ Such strategic behavior on the part of self-interested standard setters takes place whenever firms make their standards proprietary, which typically translates to less compatibility. On the other hand, imposition of inflexible standards on newer firms may create barriers to market entry thereby protecting older firms from competition. Reducing such compliance costs must therefore be accomplished within a paradoxical regulatory framework: the more *de facto* activity is encouraged by formal agents, the more independent and potentially non-compliant *de facto* standards may become.

The idea that compliance costs diminish with application standards also complies with economizing transaction costs, generated in cooperative production of standards. In the world outside cyberspace, it is agreed that when transaction terms are standardized, bargaining conditions are lubricated, resulting in reduced transaction and other costs to producers and users.²⁷⁰ It is also part of the general characteristic of compliance costs, especially with respect to the implementation phase, where bargaining as a means of coordinating standards becomes feasible.²⁷¹ Indeed, one of the primary purposes of standardization is to eliminate bargaining over details of individual transactions when bargaining costs and unpredictable customized bargains would deter producers from making valuable products like application software available.

The surplus created by standardization exists for a number of reasons. First, application standards embed an *ex ante* constraint as automated, self-adapting, and self-executing regulative subject matters. Standards can therefore be encouraged to impose, prevent, or permit transactions from occurring. Because standards define the level of access to both a technol-

269. *Id.* at 155.

270. *Id.* at 122-24.

271. *See, e.g.*, Clayton P. Gillette, *Intervention and Standardization in Electronic Sales Contracts*, 53 SMU L. REV. 1431, 1435 (2000) (discussing the importance of promulgating common terms of trade in cyberspace, for example, for the XML standardized languages market); Edward L. Rubin, *Computer Languages as Networks and Power Structures: Governing the Development of XML*, 53 SMU L. REV. 1455, 1475 (2000) (same).

ogy's source code and interface, before, during, and after application standards are produced, such standards profoundly affect transactions.²⁷² Second, in cyberspace, direct product-signaling options to consumers increase in both quality and number.²⁷³ Thus, based on software design, application standards give greater regulative control to users, which allow them to more efficiently express their preferences.²⁷⁴ As signaling options increase, production based on future consumer preferences is also likely to simplify and potentially reduce the cost of transactions among producers and users alike. Third, based on consensual practices of fair competition, users of application standards may lower enforcement costs against non-compliant standard setters through monitoring and compliance technologies, for example, blocking and filtering technology or even censorship software against uncooperative behavior on the part of such non-complying standard setters. These technological constraints can be designed to increase users' ability to facilitate demand for application standards in the face of the growing need for advanced widespread application standards.²⁷⁵ The effect of the expansion in consumer diversity on demand remains, therefore, contradictory. On one hand, cyberspace increasingly allowed consumers to be involved in regulative activity, allowing users to designate preferences for standards. On the other, the need to coordinate both production efforts and compatibility intended to meet diverse prefer-

272. The IETF is a good example of this front. All standard proposals and main standards are available at their web site. See *Internet Engineering Task Force Website*, at <http://www.ietf.org>. As well, GII Virtual Roundtable is an organization-neutral online forum that includes a large set of standardization organizations such as IEC, IrDA, ISO, JTC1, POSI, VESA, ETSI, DAVIC, etc. See *GII Virtual Roundtable Website*, at <http://www.globalcollaboration.org>. Its goal is to provide a common forum for users and consumers alike for voicing their opinions on various active standardization processes. Moreover, the principle that ensures that implementers of a standard should have open access to intellectual property rights and would be required to meet the standard on a non-discriminatory, fair and reasonable basis was adopted by many standards developing organizations, for example, ANSI, ISO, IEC, ITU and the IETF. *Id.*; see also Mähönen, *supra* note 102, at 44; Rada, *supra* note 98, at 29-30, 32.

273. See Reidenberg, *Lex Informatica*, *supra* note 1, at 570 (suggesting that signaling options for completing transactions in technological products increase).

274. *Id.*

275. To date, filtering software for data and documents on the Internet is mostly related to two main standard applications, namely, e-mail and the World Wide Web. Filters can facilitate individual choice at the browser or even the server level. See generally Paul Resnick & James Miller, *PICS: Internet Access Controls Without Censorship*, 39 COMMUNICATIONS OF THE ACM 87 (1996), at <http://www.w3.org/PICS/iacwcv2.htm> (last visited Dec. 1, 2002); R. Polk Wagner, *Filters and the First Amendment*, 83 MINN. L. REV. 755, 759-69 (1999); Jonathan Weinberg, *Rating the Net*, 19 HASTINGS COMM. & ENT. L.J. 453 (1997).

ences has increased as application standards became more complex and expensive to coordinate. Thus, with such regulative costs at stake, a role for industry formalization of *de facto* and gray standards remains essential.²⁷⁶

There is an additional general justification for industry stepping up and formalizing *de facto* and gray standards. Procedurally, formal industry has an ability to maintain compliance through rules of membership and procedure. Formal industry standardization is arguably the most efficient mediator of hegemony within the overall institutional framework because the industry as a whole is more likely to remain more competitively neutral, in comparison, and thus able to serve universal interests in the face of growing self-interested competition.²⁷⁷

In summary, changes in application standards designed by *de facto* or gray standard setters can mostly be promulgated based on a formalizing role of industry standard setters that possess the authority to both articulate and implement standards of their own. More importantly, they can formalize *de facto* and gray application standards and create common terms of trade. In addition, as centralized adopters of standards, industry organizations should be relied upon to publicize content and procedures of cooperative standardization practices.

3. *Indirect Costs*

Coordinating technologies required by new standards and innovative products may be cheaper for larger, well-organized agents than for smaller firms. However, this also means that the real winners in a system are *de facto* standard setters that are both flexible enough to identify opportunities to capture an architecture and powerful enough to sustain control over it. Whenever such *de facto* control is present, economies of scale may also generate external costs of delay in production. Often, one or more such *de facto* agents might be pushed towards delaying a final innovative outcome, hoping that technological or commercial developments will overtake an undesirable result. Beyond an efficient result, there is a risk that this process will produce an answer that will end by isolating vendors and fracturing the market. That may result whenever duplicative production is made,

276. See Rada, *supra* note 98, at 33; Reidenberg, *Lex Informatica*, *supra* note 1, at 587.

277. See 47 U.S.C. § 160 (2000); *id.* § 230 (a)(4) & (b)(2). In essence, this premise is also what led to the deregulation movement in telecommunications services. See WERBACH, *supra* note 4, at 29.

rather than uniting vendors behind a standard that would be well accepted by users.²⁷⁸

Because such inefficient competition is a market failure best minimized through governmental intervention, industry standardization organizations are not a natural proxy for such regulative activity.²⁷⁹ Nonetheless, as a policy matter, they may still serve to minimize the potential need for ex ante governmental intervention.

Thus, such ex ante industry intervention could coordinate *de facto* standard setters' right to supply standards. In an attempt to avoid self-regulating firms having monopolistic control over the right to supply standards, industry may channel such activity to competition for that right. Each competing self-regulatory firm may thus be required, as part of its bid, to submit its proposed regulatory rules. A second-tier public agency, acting as proxy for consumers, might then be able to determine the right to supply implementation standards or distinct classes of such standards. In cyberspace, this theoretical approach has not yet reached its potential. At present, the industry has the more limited role of coordinating production ex ante instead of coordinating the right to supply itself.²⁸⁰

278. See Kathleen M.H. Wallman, *The Role of the Government in Telecommunications Standard-Setting*, 8 COMMLAW CONSPECTUS 235, 239-40 (suggesting that this was the case with the wireless network standards situation that has ended up producing one set of prevailing standards for the U.S. market (Time Division Multiple Access and Code Division Multiple Access) and another for most of the rest of the world (Global System for Mobile Communications)).

279. See LEE, *supra* note 101, at 128-29 (following the example of the wireless phone industry and suggesting that their joint interoperable failure has been neither on consensual nor on technical grounds, but because of ability, given CCI rules, of core groups to dominate the standard-setting process).

280. See OGUS, *supra* note 1, at 110 (acknowledging that, to date, such a system is already used for the allocation of public franchises, for example, in broadcasting services or airline routes). This environment in which industries might control the market for the right to supply will also be subjected to antitrust law limitations. See *Joint Ventures and Standard-Setting: Problems in the Current Framework* (paper by Ernest Gellhorn & W. Todd Miller presented to the Federal Trade Commission in the hearings on the Changing Nature of Competition in a Global and Innovation-Driven Age) (Oct. 26, 1995) (suggesting that cooperation among industry participants with a collective market share of less than merely 35 percent creates few risks, especially in dynamic high-technology markets, and thus should be immune from antitrust challenges); William F. Baxter, *The Definition and Measurement of Market Power in Industries Characterized by Rapidly Developing and Changing Technologies*, 53 ANTITRUST L.J. 717, 723 (1984) (proposing that R&D joint ventures possessing market shares of lower than 20 percent be considered benign); Robert F. Bork, *The Rule of Reason and the Per Se Concept: Price-Fixing and Market Division*, 75 YALE L.J. 373, 397 (1966) (suggesting a restriction of 25 percent); Joseph F.

B. Government Intervention

Apart from the indirect support for routine and limited *infrastructure* standard-setting activity during the implementation phase, governments should continue to play a restrained indirect role in vital application standard-setting activity due to institutional barriers on efficient participation.

This study generally holds that government's role should diminish during the implementation phase. Governmental institutions should not take corrective action to minimize market failures, when the same result can be achieved through private sector standard-setting activity. Specifically, the U.S. government followed this comparative institutional guideline when it noted that "even where collective agreements or standards are necessary, private entities should, where possible, take the lead in organizing them."²⁸¹ Furthermore, under section 401 of the Telecommunications Act, the Commission must refrain from regulating, so long as forbearance is consistent with the public interest.²⁸²

1. Direct Intervention: The Problem of Efficiency

There are four main reasons why governments tend to be inefficient in standard-setting during the implementation phase. First, and most importantly from the view of an overall standardization process, rapid technological developments generally outpace the slow, *ex post* bureaucratic decision-making characteristic of government institutions.²⁸³ Moreover, once production patterns are adopted, they acquire a taken-for-granted quality and are not easily dismissed or changed.²⁸⁴ As a general matter, when standards are developed or ordered by governments, they tend to be designed for particular needs (especially, DoD programs), which are largely less commercially-oriented or desirable to small commercial programs with fast response times.²⁸⁵ Eventually, while the market may replace an inefficient standard by competitive technological "leapfrogging," there are typically fewer guarantees that government will do the same. Furthermore, except for the competitive self-standardization practice (backed by a governmental monitoring role), there is no market for *control* of application standard setters. Thus, the principals (politicians and citizens) cannot eas-

Brodley, *Joint Ventures and Antitrust Policy*, 95 HARV. L. REV. 1523, 1541 (1982) (proposing a restriction of 40 percent).

281. See Clinton & Gore, *A Framework*, *supra* note 14, § 9.

282. See sources cited *supra* note 277; see also WERBACH, *supra* note 4, at 29.

283. BREYER, *supra* note 1, at 106; LIBICKI, *supra* note 3, at 354; Gillett & Kapor, *supra* note 135.

284. MARCH & OLSEN, *supra* note 13, at 52.

285. LIBICKI, *supra* note 3, at 354-55.

ily dismiss ineffectual officials.²⁸⁶ Government agencies are generally composed of career public servants, not market participants and, as a result, they often do not involve the most qualified and industrially impartial individuals in the industry for the standard-setting process. This is the inherent danger of bureaucracy, particularly when it attempts to standardize a fast-moving area like the Internet.

Second, today's technology may limit the ability of governments to understand the issues in direct and substantive standardization. Particularly, in a market economy, such as that of the implementation phase, it is not apparent that the government will understand what constitutes an inefficient standard. Ultimately, the need to write standards with an eye toward enforcement raises difficulties that may potentially compel the agency to write standards that do not meet the primary policy objective of efficiency.²⁸⁷

Third, government standard-setting agencies may be slow in gathering information and may not always have access to the best information since information flows may be invisible to them.²⁸⁸ This problem also exists in the infrastructure development phase. However, in that pre-commodified phase, competition was scarcer than it is in the implementation phase and the U.S. government successfully monitored such information flows. Thus, even with the best of intentions, a government standard-setting agency may simply pick a less efficient standard, leading to stagnation of robust standards, even when they may appear technologically ill conceived. Alternatively, government agents may not always have the ability

286. MARCH & OLSEN, *supra* note 13, at 52; OGUS, *supra* note 1, at 112.

287. BREYER, *supra* note 1, at 112; OGUS, *supra* note 1, at 170.

288. See, e.g., Anton & Yao, *supra* note 169, at 252 ("Technical judgments are also critical to assessing whether the benefits of the standard outweigh the costs, but most courts and agency officials lack a technical background."); David Bazelon, *Coping with Technology Through the Legal Process*, 62 CORNELL L. REV. 817 (1977); Richard A. Posner, *Antitrust in the New Economy*, 68 ANTITRUST L.J. 925, 925 (2001) (arguing that in the new innovative economy the real legal problem lies on the institutional side because the enforcement agencies and the courts do not have adequate technical resources, and do not move fast enough, to cope effectively with a rapidly changing business sector); Howard Shelanski, *Regulating at the Technological Edge: New Challenges for the F.C.C.*, 2000 L. REV. MICH. ST. U. DET. C. L. 3 (2000). See generally Harry S. Gerla, *Federal Antitrust Law and Trade and Professional Association Standards and Certification*, 19 DAYTON L. REV. 471, 503 (1994) (examining how eventually "antitrust courts generally have been favorably disposed toward trade and professional association standards"); Howard Shelanski, *Competition and Deployment of New Technology in U.S. Telecommunications*, 68 U. CHI. L. REV. 1 (2000) (supporting a repeated-play policy in establishing the right equilibrium to the telecommunications industry in the FCC, in the face of the present technological change).

or will to perform such evaluations. As has been noted in the literature on public choice theory, government agencies in a position to influence the outcomes of market competition are highly susceptible to “capture” by private entities with an interest in the outcome. Thus, there is much less of a guarantee that a governmental standard-setting body will act efficiently in the public interest through direct standardization activity, even when it is possible for a government agency to discern what in fact that interest is.²⁸⁹

Fourth, there is the increasing trend towards globalization reflected in IT regulation and cyberspace’s standardization today. As suggested, institutional analysis refers narrowly to “collective action” and “interest groups” at the national level. These paradigms were generalized before new global regulatory realms were understood as such. These institutional paradigms assume a homogeneous national institutional structure, based on the United States or some hypothetical Western democracy rather than the borderless global arena. Accordingly, there is no good understanding of the relationship between national and international standardization, or even if this is an important or useful distinction. Indeed, fundamental to the developments affecting the institutional standardization debate is the emergence of a global economy in which the United States, as one national government, may not play the dominant role.²⁹⁰ In the future, the rise of international standardization organizations might change the current institutional balance by dominating both application and infrastructure

289. See Lemley, *Antitrust*, *supra* note 94, at 1063 n.76 (“This almost happened in the case of the United States HDTV standard. Only by an accident of timing did the government adopt a digital HDTV standard, rather than an analog standard which would have been immediately obsolete.”); see also NICHOLAS NEGROPONTE, *BEING DIGITAL* 37-40 (1995); Joseph Farrell & Carl Shapiro, *Standard Setting in High Definition Television*, 8 BROOKINGS PAPERS ON ECON. ACTIVITY 1 (1992).

290. See OFF. TECH. ASSESSMENT, U.S. CONG., *GLOBAL STANDARDS: BUILDING BLOCKS FOR THE FUTURE 90-94* (1992) (discussing the growth of international standardization efforts and the effect of multinational organizations), available at http://www.www.princeton.edu/cgi-bin/byteserv.pr1/~ota/disk1/1992/9220_n.html (last visited Dec. 4, 2003); LIBICKI, *supra* note 3, at 19, 341-42 (discussing the weakening of governments role in the midst of globalization of IT standard-setting activities).

standard-setting.²⁹¹ This potential development serves as yet another justification to support a more indirect role for the government.²⁹²

2. *Indirect Intervention: Roles of Government Regulation*

Historically, the FCC has avoided direct standardization of both Internet telecommunications services and application standards. Accordingly, the Global E-Commerce Report (“E-Commerce Report”) contains strong language concerning the proper *de facto* production of technological standards for electronic commerce.²⁹³ Although overly broad, the E-Commerce Report takes a strong position against direct government standard-setting in its section on technical standards.²⁹⁴ The E-Commerce Report states that industry groups rather than individual companies should set standards.²⁹⁵ In practice, Internet telecommunications services and application standard-setting are largely constrained by market forces, backed by general intellectual property and antitrust law.²⁹⁶ This policy should leave the government with only indirect means of standardization. Broadly, there are two governmental roles in application standard-setting. First, to regulate supervisory rules, which facilitate production of standards by market agents. Second, to regulate processes of standardization aimed at further legitimizing both decision-making and its outcomes, as will be described below.

Conceptually, there is a broad range of governmental regulative approaches to promote the production of standards. The approaches differ in extent and directness vis-à-vis the type of each technological standard. As to extent, government intervention can be promoted narrowly, for example through specific preexisting regulations such as network non-bundling of the services and facilities involved in providing advanced capability. Alternatively, government intervention could be designed widely to promote completely new regulations intended to increase competition and invest-

291. See, e.g., Linda Garcia, *A New Role for Government in Standard Setting?*, 1 STANDARDVIEW 2, 5 (1993) (suggesting that the United States may also have considerably less influence than in the past in determining the character of international standards institutions).

292. See, e.g., David C. Wood, *European Standardization Policy*, 3 STANDARDVIEW 112, 114 (1995) (suggesting that “[c]oncerned economic players should participate directly in the standardization process, without national coordination or representation”).

293. *Id.*

294. *Id.* (“The United States considers it unwise and unnecessary for governments to mandate standards for electronic commerce.”).

295. *Id.* (“We urge industry driven multilateral fora to consider technical standards in this area.”).

296. See BENJAMIN ET AL., *supra* note 63, at 915.

ment in superior services. As to directness, government intervention can be indirect, thus letting markets operate without any new specific regulation, typically with the verification of a “reasonable” procedure made in deployment. Alternatively, a government can engage in deregulating services from broad regulation, thus improving investment incentives and technological development. Then, as mentioned earlier, there is the remaining alternative, namely direct technological standardization, which would be less efficient, and is generally limited due to the restrictions discussed above.

An even more extreme scenario is the risk of a government—acting on its own or in concert with other national governments or industry members—taking over the standard-setting process by means of monopolization. It could then convene federal advisory committees for the purpose of obtaining organized industry and user input, as the U.S. government did in the sensitive case of security standards.²⁹⁷ Still, for the reasons mentioned government standard-setting intervention of this nature is routinely seen, by both the U.S. government and its critics, as the ultimate inefficient bottleneck.²⁹⁸ Thus far, the Clinton administration policy against such government intervention in application standard-setting is still valid and has not been replaced.²⁹⁹

a) Regulate Production Supervision Rules

To facilitate market production and its funding, a government should engage in three activities. First, encourage R&D activities by autonomous institutions, preferably through better-coordinated industries rather than *de facto* agents whenever such activity would not serve to duplicate *de facto* R&D initiatives. Against the backdrop of shortened technological lifecy-

297. See, e.g., LESSIG, *supra* note 8, at 35-36 (criticizing governmental code control of the use of encryption in cyberspace); A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 712, 718-35 (1995) (describing analogous government access and regulation possibilities); Lemley, *Standard-Setting*, *supra* note 94, at 478 (criticizing the U.S. government for dictating an encryption policy).

298. Referring generally to the Internet at large, the Telecommunications Act states that it is the policy of the United States “to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation,” and the FCC has a responsibility to implement that statute. See Telecommunications Act of 1996, 47 U.S.C. § 151 (2000); see also Clinton & Gore, *A Framework*, *supra* note 14, § 9, at 20; *The Emerging Digital Economy*, *supra* note 233; Rubin, *supra* note 271, at 1455 (concluding that, at present, the government does not want to undertake the task, private groups do not want government intrusion, and no one thinks government will develop the optimal standards).

299. Clinton & Gore, *A Framework*, *supra* note 14.

cles, autonomous self-interested standard setters, when left alone, are typically less willing to risk potential exposure to failure. This reality is what arguably makes governments most suitable for providing R&D funding, rather than forcing industry to internalize some of these development sunk costs.³⁰⁰ In addition, funds should be available to academic institutions and even small and medium sized enterprises (“SMEs”) to encourage these entities to participate in socially undervalued research activities.

A second production supervision rule is to encourage and maintain industrial competition by applying antitrust law against potential anticompetitive strategic behavior. Thus, the general antitrust rule should be applied for anticompetitive research or production co-ventures. Antitrust law should impose liability under section 1 of the Sherman Act and section 7 of the Clayton Act whenever collaborative standard-setting bodies erect barriers to entry to prevent new innovations from entering the market.³⁰¹

A third production supervision rule is indirect price regulation, whenever market competition curtails socially desirable variety in application standards.³⁰² Such price controls should be used to lower prices of otherwise undervalued social welfare benefits.³⁰³ In cyberspace, such initiatives included real-world analogous non-profit activities as research and education.³⁰⁴ In some cases such valuable benefits can be technologically inefficient. Similarly, for the purpose of preserving socially desired technologies, indirect government intervention would be essential so as to benefit low performance-sensitive applications such as remote retrieval software for text files, which benefit clients that otherwise might lose their incen-

300. See BREYER, *supra* note 1, at 10; NEXT GENERATION INTERNET, *supra* note 173, at 5.

301. See Sean P. Gates, *Standards, Innovation, and Antitrust: Integrating Innovation Concerns into the Analysis of Collaborative Standard-Setting*, 47 EMORY L.J. 583, 654-55 (1998).

302. For the U.S. government's declaration of support for this policy, see AGENDA FOR ACTION, *supra* note 114.

303. See OGUS, *supra* note 1, at 153.

304. Accordingly, during its first seven months, the Clinton-Gore Administration followed this policy. Initially, the President's FY 1994 budget included a \$100 million program to develop applications in areas such as education, manufacturing, health, and digital libraries. In addition, the U.S. government allocated \$50 million for National Telecommunications & Information Administration (“NTIA”) grants to demonstrate the applications of the NII for non-profit institutions such as schools, hospitals, and libraries. See *Administration NII Accomplishments* § 3, <http://www.ibiblio.org/nii/NII-Accomplishments.html> (last visited Dec. 3, 2003); see also H.R. 5983, 102d Cong. (1992); H.R. 5759, 102d Cong. (1992); S. 2937, 102d Cong. (1992) (seeking to develop high-speed technological infrastructure for schools, libraries, medicine etc.); S. 2813, 102d Cong. (1992) (seeking to facilitate public access to federal electronic information).

tive to reveal their preferences. Such inefficiency might result in the erosion of the qualitative rationale of standardization, over-emphasizing narrow performance-sensitive applications.³⁰⁵ This important supervisory rule should not be limited only to confronting strict economic productivity, but potentially technological efficiency as well. As explained, industry standard setters may not necessarily be *technologically* neutral—making government intervention in the latter not only important, but also ultimately irreplaceable.

b) Regulate the Process of Standardization

Inherent to commercial production of high technologies is the tension between efficient and fast evolving outcomes and slow and thus constraining procedures. With application standards, this difficulty is primarily the result of constant outside commercial pressure. As a result, even formal standard-setting bodies tend to focus on outcomes, as opposed to processes.³⁰⁶ Thus, as a comparative conclusion, March and Olson see the main role of fairly elected political institutions as formal standardization institutions, as best suited to confirm the legitimacy of these same undervalued procedural decisions.³⁰⁷ Translating this conclusion into practice, governments should emphasize regulating standardization processes next to technically standardizing products.³⁰⁸ As the ultimate guardians of the standards producing process, governments would thus promote the dynamics that are likely to satisfy the demand of fairness by the process used in their creation.³⁰⁹

305. Scott Shenker, *Service Models and Pricing Policies for an Integrated Services Internet*, in PUBLIC ACCESS TO THE INTERNET 326 (Brian Kahin & James Keller eds., 1995).

306. Egyedi, *supra* note 3, at 52 (“The formal standards bodies are, however, inclined to stress ‘outcome’ rather than ‘process’ results because of outside pressure.”); Joel West, *Institutional Constraints in the Initial Deployment of Cellular Telephone Service on Three Continents*, in INFORMATION TECHNOLOGY STANDARDS AND STANDARDIZATION: A GLOBAL PERSPECTIVE 198-221 (Kai Jakobs ed., 1999) (including a comparative empirical study on such external institutional pressures in the deployment of analog cellular telephone service standards, as experienced in the United States, Japan and Europe). Such outside pressure is already argued to stand in the way of ICANN, see, for example, Post, *Governing Cyberspace*, *supra* note 202 (“Any entity exercising control over the DNS will be subject to immense pressure to do more than mere ‘technical management.’”).

307. MARCH & OLSEN, *supra* note 13, at 50-52;

308. See Anton & Yao, *supra* note 169, at 248 (“[w]hile informed judgments about such procedures will still be necessary, technical judgments will be avoided”); Rubin, *supra* note 271, at 1473.

309. For a discussion on elements important in determining reasonableness of procedures in the face of potential anticompetitive effects of standard-setting, see Michael C. McCarey, Associate Director, FTC Bureau of Consumer Protection, *Industry Standards*

As indirect players, this role of governments may be achieved in different ways. First, by supervising formal industry initiatives. Beyond economic efficiency, governments would impose and encourage formal industries to maintain a democratic layer between the autonomous standardization institutions and their participants, and the standards that they design. In essence, as guardians of the process, standardization procedures would then serve, indirectly, to legitimize that same process. Second, by defining its own alternative procedures.³¹⁰ In either way, most participants in designing a standard should be made to benefit from the result.³¹¹ This role of government may then enhance the level of competitive participation in standardization itself,³¹² particularly participation of marginal participants.³¹³ The National Technology Transfer and Advancement Act of 1995³¹⁴ directed federal agencies to use standards developed by voluntary consensus bodies, except where doing so would be inconsistent with applicable law or when it would be otherwise impractical.³¹⁵ This legislation adds credence to the earlier U.S. government policy codified in the OMB Circular A-119 *Federal Participation in the Development and Use of Voluntary Standards* ("OMB Circular A-119").³¹⁶ Proposed revisions to OMB Circular A-119, characterize the nature of standards that government agencies are constrained to consider ahead of developing their own procurement or technological standards.³¹⁷ Accordingly, agencies will be submitted to an administrative burden of proof to justify why they did not

and Certification: Three Current Issues, Remarks Before the 26th Annual Symposium of the Trade Ass'n & Antitrust Law Comm. of the D.C. Bar (Feb. 1990).

310. *Id.*

311. Egyedi, *supra* note 3, at 52.

312. *Cf.* Balto, *supra* note 169, § 2 & nn.13-19 (adding that, in practice, "the antitrust jurisprudence on standard-setting focuses almost entirely on collective standard-setting and the process used to determine the standards").

313. CARGILL, *supra* note 1, at 233-34 (discussing the diversity of participants in autonomous standardization institutions both as an advantage and as a problem in reaching consensus).

314. National Technology Transfer and Advancement Act of 1995, Pub. L. No. 104-113, 110 Stat. 775 (1996)

315. *See* Rubin, *supra* note 271, at 1473 (suggesting that it would be possible for a federal statute to declare that the use of a computer language in interstate commerce that was not designed through a sufficiently cooperative process is an unfair trade practice under 15 U.S.C § 45(A)(1)). So far, however, this suggestion has not been adopted.

316. The OMB has been the guardian of the previous policy and is responsible for the more detailed regulations that all agencies will have to follow to meet the new law.

317. *See* OMB Circular No. A-119, *supra* note 30.

use a relevant “Voluntary Consensus Standard” prior to proceeding to design new government standards.³¹⁸

C. A Potential Deviation: The ICANN Case Study

One potential deviation from the supported general policy for infrastructure standard-setting may arise in the form of the federal government’s involvement with the ICANN domain name system. ICANN, a private non-profit corporation, was initially appointed to oversee the operation of the root server system. In this capacity, it was charged with supporting existing protocols and telecommunications services used to implement domain name facilities.³¹⁹ To that end, ICANN’s board of directors had two different functions. The first was to take steps towards introducing competition into the Domain Name registration system.³²⁰ The second was to uphold a policy against cybersquatting through what later became the Uniform Dispute Resolution Policy (“UDRP”) and arbitration panel.³²¹

ICANN’s establishment suggested two types of standardization concerns. The first concern regarded its potentially problematic institutional identity, the second was its wide technical mandate as a standardization organization. As a technical standardization institution, ICANN was initially constructed as a private interest group. As a private entity it exercised direct and central control with the U.S. government choosing to remain in the background.³²² As suggested earlier through public choice analysis, left alone such competitive interest groups might establish genuine public policy inefficiency. In addition, such groups might create a monopoly on the allocation of the DNS names and numbers.³²³ These latter

318. With a decrease in the governmental role in cyber standard-setting, there is some criticism of this policy as overly national in nature, in the midst of a global standardization trend. See Garcia, *supra* note 291 (for a critical analysis of OMB Circular A-119 policy, as insufficiently coordinating); Wood, *supra* note 292, at 114.

319. See RFC 882, *supra* note 77.

320. See White Paper, *supra* note 188, at 31, 749.

321. *Id.* at 31, 747. That policy was later adopted in the Uniform Domain Name Dispute Resolution Policy. See *Uniform Domain Name Dispute Resolution Policy* (Aug. 26, 1999), at <http://www.icann.org/dndr/udrp/policy.htm> (last visited Dec. 1, 2002).

322. See BENJAMIN ET AL., *supra* note 63, at 825.

323. See generally Froomkin, *supra* note 145, at 216 (suggesting that the analyses of the privatization of the DNS and TCP/IP highlights some of the reasons why the bottom-up process has failed); A. Michael Froomkin & Mark A. Lemley, *ICANN and Antitrust*, 2003 U. ILL. L. REV. 1 (discussing the various potentially anticompetitive effects of ICANN); Kesan & Shah, *supra* note 115, at 214 (suggesting that the Internet community was not able to resolve the uniformity problem through a bottom-up process, and, as a result, the U.S. government has begun to intervene).

challenges are not merely structural as they often interact with ICANN's unique technological mandate.

Thus, the second standardization concern is a function of ICANN's technical responsibilities. Arguably, ICANN was given too much technical discretion in a blurry mandate on code writing (i.e., technological standardization). ICANN controls issues such as the maintenance of the bit size of data packets, the architecture of the root services, and the preservation of unique protocol numbers for other various Internet functions.

Originally, the Department of Commerce ("DoC") initiated the *White Paper*, a non-binding statement of policy through which it informally declared that "the U.S. government should end its role in the Internet number and name address system."³²⁴ Like the *Green Paper* before it,³²⁵ the *White Paper* has conformed to the already existing vague and basic governmental "Principles for a New System"³²⁶ with no clear separation between a technical standardization policy and non-technical governance responsibilities.³²⁷ Accordingly, the DoC characterized ICANN's technical responsibility in vague terms. This new corporation was made responsible only for "technical management of the DNS," which was most likely defined as the "narrow management and administration of Internet names and numbers on an ongoing basis." Overall, most commentators still agree that the U.S. government holds *de facto* control of the root zone.³²⁸ However, it is also clear that the U.S. government has chosen not to have direct control over the root server.³²⁹ Consequently, the question of ICANN's technological standardization has still not been raised properly as a separate policy question, underscoring the need to decide on future technological risks.

324. See *White Paper*, *supra* note 188, at 31, 749.

325. NAT'L TELECOMM. & INFO. ADMIN., U.S. DEPT. COMMERCE A PROPOSAL TO IMPROVE TO TECHNICAL MANAGEMENT OF INTERNET AND ADDRESSES (1998) [hereinafter GREEN PAPER].

326. These are principles such as "stability, competition, private bottom-up coordination, and representation." *Id.*

327. See Froomkin, *supra* note 145, at 171 (suggesting that the DoC draw one henceforth).

328. See *id.* at 166 ("[T]here is no dispute that the U.S. government, through the Department of Commerce, currently enjoys *de facto* control of the DNS. Nor is there any dispute that DoC has at least temporarily ceded to ICANN, through a variety of contractual and quasi-contractual agreements, almost all the control the United States enjoys."); Steve Kettmann, *Will U.S. Release Grip on ICANN?* (Jan. 19, 2002) (emphasizing that post September 11 the gradual process by which ICANN will gain autonomy from the government has been slowed), <http://www.wired.com/news/infrastructure/0,1377,49836,00.html> (last visited Dec. 1, 2002).

329. *But see* Froomkin, *supra* note 145, at 169 (suggesting that for that reason the U.S. government had, in fact, only quasi-privatized the control on the root server).

To date, both ICANN and the DoC deny that ICANN is engaged in either regulation or governance. Instead, they suggest that ICANN is engaged in nothing more than routine standard-setting or presumably “technical coordination” or “maintenance.”³³⁰ Instead, the main controversy over ICANN’s governance mandate was limited to the question of its democratic decision-making accountability. Thus, although the DoC seems to be keeping only an indirect measure of control over the DNS and its root server, it is consistently doing so from a distance based on a rhetoric that pretends to support ICANN’s absolute self-regulation. However, with the mounting political pressures against the U.S. government’s intervention on the one hand, and commercial interests trying to “capture” ICANN’s wide technological discretion on the other, there are no guarantees that such a delicate, yet relatively successful balance can be maintained in the future. The need to balance these technological risks is not merely theoretical. Present infrastructure transparency concerns are already a good case in point for that.

In recent years, as part of ICANN’s concern with preserving end-to-end transparency, it has become involved with the various issues surrounding internationalized domain name (“IDN”) compulsory infrastructure standards. Thus, ICANN’s Board has begun to initiate inquiries about that role with regard to the various efforts to use non-ASCII characters to design international domain names supported by the domain name system at large.³³¹ On September 25, 2000, the ICANN Board approved a set of resolutions,³³² in which the Board recognized the importance of the Internet evolving to be more accessible to those who do not use the ASCII character set.³³³ Ultimately, ICANN recognized a need to specify an adequate standards track protocol based on supporting test bed findings and requirements. Upon final adoption in June 2003, IDNs became fully operational in a standards-based way.³³⁴ Consistent with ICANN’s policy,

330. See White Paper, *supra* note 188, at 31, 744.

331. The American Standard Code for Information Interchange (“ASCII”) is the most common standard for the code numbers used by computers to represent all the upper and lower-case Latin letters, numbers, punctuation, etc. There are 128 standard ASCII codes.

332. Formally relating to the 22 August Verisign Global Registry Services announcement about its introduction of the multilingual test bed.

333. See ICANN, *Minutes of Special Meeting of the Board* (Sept. 25, 2000) [hereinafter ICANN, *Minutes*], at <http://www.icann.org/minutes/minutes25sep00.htm#MultilingualDomainNames> (last visited Dec. 3, 2003).

334. See ICANN, *Guidelines for the Implementation of Internationalized Domain Names* (June 20, 2003) [hereinafter *Domain Name Guidelines*], at <http://www.icann.org/general/idn-guidelines-20jun03.htm> (last visited Dec. 3, 2003). With IDN, *de facto* designers of browsers or other Internet software would be able to program their software to convert any foreign-character domains typed in or linked to into the appropriately

the accepted standard would then have to be binding and fully compatible with the Internet's existing end-to-end model, and "preserve globally unique naming in a universally resolvable public name space."³³⁵

As the specially designed Internationalized Domain Names Committee has suggested, any Top Level Domain ("TLD") expansion should occur in a careful and controlled fashion, with regard for the overall stability of the DNS. On balance, as long as the DNS is subject to the present pre-designed scarcity policy that stability will be achieved within the limit of the total number of TLDs eligible for delegation to a given geographic unit.³³⁶ IDNs should, therefore be carefully and agreeably set at a number equal to the number of its official languages.

In part, this technological challenge was met successfully. However, it took more than a quasi-privatized ICANN to do so, as ICANN asked for the legitimacy and intervention of ISO. In fact, ICANN/IANA is still staying out of the business of determining what is and is not a country (or geographically distinct territory), and what name or abbreviation is semantically associated with any given geographic unit. Technically, the ISO-3166-1 IDS table developers at ISO, already solved the problem of what is and is not a recognized geographic unit (country or geographically distinct territory).³³⁷ However, it being a sensitive, politically oriented decision, the table only provides two- and three-letter ASCII codes for each such geographic unit. Thus, ISO's table does *not* solve the multi-faceted problem of what non-ASCII names (or abbreviations) should be assigned to each recognized geographic unit, and who should be in charge of assigning them.

In essence, the current ICANN/IANA policy permits the delegation of ASCII ccTLDs only when a given geographic unit and its associated specific 2-letter ASCII codes appear on the ISO 3166-1 list. Due to the significant political nature of this question, ICANN/IANA's policy has so far failed to authorize the use of non-ASCII characters, leaving ICANN without a given reference point for IDNs. On balance, those problems are properly excluded from the ICANN process, and resolved by a politically

convert any foreign-character domains typed in or linked to into the appropriately coded string, which could then be resolved using normal DNS queries.

335. See ICANN, *Minutes*, *supra* note 333.

336. See discussion *supra* Part III.B.2.a.

337. For most users of ISO 3166-1 the standard is the list of country names and codes. See Internet Standards Organization, *Background on ISO 3166*, <http://www.iso.org/iso/en/prods-services/iso3166ma/04background-on-iso-3166/index.html> (last visited Dec. 3, 2003).

expert, internationally recognized body, the ISO and its ISO 3166 Maintenance Agency.

ICANN's Board decided to further delegate to top-level domain registries the employment of an "inclusion-based" approach meaning that code points that are not explicitly permitted by the registry would be prohibited.³³⁸ However, in compliance with ICANN's IDN guidelines, registries are merely encouraged to work collaboratively with relevant and interested stakeholders to develop language-specific registration policies in a way that might then curtail ICANN's new main goal of privatizing today's DNS universal uniqueness in case such cooperation gets complicated.³³⁹ Left to the strategically dominant RIRs and nation-agents, in the "market of nations," ICANN/IANA's non-binding hegemony might be facing self-interested competing claims backed by different regional stakeholders, or worse, different national governments. As a one-shot game, achieving such consensus would be subject to a basic prisoner's dilemma flaw, where no efficient incentive to cooperate would prevail and parties would choose to act strategically: left alone, national registries still have the incentive to benefit their own customers at the expense of the DNS stability at large. Thus, maintaining such stability in case of lack of cooperation by RIRs, in the face of growing self-interested commercial intervention, would be a task poorly suited to a technical coordinating organization such as ICANN. Arguably, the non-binding quasi-privatized ICANN is now facing a set of political concerns for which it might not be well suited. Furthermore, ICANN might misuse its mandate of deciding when and to what neutral and authoritative arbiter such problems should be referred, thus risking potential DNS instability, politically, and ultimately, technologically.

In such critical situations, as the broadly agreed lowest common denominator rule, ICANN should attempt to enforce binding standardization policies only when there is a clear need for uniformity based on a substantive consensus among those who must implement such policies and are impacted by them.³⁴⁰ But should ICANN be faced with full responsibility

338. See *Internet Domain Name Guidelines*, *supra* note 334, at 2.

339. *Id.* at 4. Few recent examples of such complications evolved when lucrative domain-name businesses, such as VeriSign, pushed forward with their own IDN initiatives. Complicating matters even more, the Chinese government has laid claim to control over Chinese-language domain names, etc. See Greg Goth, *Engineering Complexities*, 5 IEEE INTERNET COMPUTING 8 (May 2001), <http://www.acm.org/technews/articles/2001-3/0601f.html> (last visited Oct. 23, 2003).

340. See David R. Johnson & Susan P. Crawford, *The Idea of ICANN*, at http://www.icannwatch.org/archive/the_idea_of_icann.htm (last visited Dec. 3, 2003).

for the challenge in the first place? With potentially suboptimal level of agreement on the need for DNS uniformity, as in the emerging case of IDNs, ICANN might be arguably approaching its institutional limit. Even assuming that in the long run, both economically and technically, multiple language domain names are feasible in the short run, ICANN may still have to coordinate ad hoc undesired fragmentation that might weaken the stability of the DNS, and encourage destructive collusion between name owners. Inevitably, as a policy rule, ICANN's Board may have to be more steadily backed by more authoritative agents, namely formal industry standardization organizations as with the case of ISO's 3166 Maintenance Agency and in extreme scenarios of loss of DNS hegemony, even more notably by the DoC, and the U.S. government at large; thus, overriding the US government's rhetorical policy against intervention in coordinating infrastructure standardization and its risky policy (or otherwise pretended) to support ICANN's final privatization.

Here, as potentially elsewhere, seen narrowly as mere technological standard-setting activity, no governmental guidelines were adequately established for ICANN thereby undermining the necessity for a visible and continuous technological standardization policy with respect to infrastructure standardization. Left as a technologically independent, non-binding, quasi-privatized standard-setting organization that is charged with public responsibility, an unmonitored ICANN may design or adapt standards unproductively.

VI. CONCLUSIONS

In the future, changes in cyberspace will bring about new innovative developments as part of new technological generations.³⁴¹ Both the TCP/IP suite and the Internet as a whole will continue to be standardized,

341. See NEXT GENERATION INTERNET, *supra* note 173. The Next Generation Internet was a U.S. federal initiative including experts from business, government and academia, trying to anticipate the next generation of Internet standardized applications. *Id.* It was a three-year program, which started in 1996 with a \$300M budget divided among several government agencies (with the lead role going to DARPA). *Id.* The program involved a test network with 100 sites that were linked at a speed 1,000 times greater than today for the design of revolutionary applications. *Id.* Another program, the Internet2 K20 Initiative, led by over 200 universities working in partnership with industry and government, is focused on developing an advanced network and applications. See *Internet2 K20 Initiative Website*, at <http://k20.internet2.edu/index.php> (last visited Dec. 3, 2003). Together with the NGI initiative, these two private networks may be integrated into the present Internet or remain separate. *Id.*

and that standard-setting will continue to shape new and existing cyber markets. New protocols will be designed and old ones will be revised.³⁴²

With the growth in both the community of users and the demand for sophisticated applications, a more advanced standardized architecture is already needed. New standardization challenges are already here—such as IPv6, designed and coordinated by the IETF formal standardization organization to expand address space.³⁴³ Similarly, several external trends and influences such as the deployment of wireless network technologies, mobile-networked devices and special purpose IP devices will have a large impact on the status of the infrastructure network layer.³⁴⁴ Leaving aside the question of whether these specific developments will lead to a generation leap, any adoption of such central technologies should follow the by and large positive experience of cyber standardization exemplified by the last two decades.

As for infrastructure standards, and notwithstanding strong governmental rhetoric concerning the need for regulative restraint and ICANN's potential inconsistency, this study generally supports the rationalization of the early central institutional adoption of a unified infrastructure set of standards for inter-connective transmission, as in the case of TCP/IP. Justifiably, this early endeavor was not followed by private initiatives of creating a market for infrastructure standards for inter-connectivity. Instead, only a market of basic telecommunications services evolved with the involvement of diverse infrastructure equipment providers including data networking equipment, Internet connections, telecommunications equipment providers, and cable operators. As described, a market for application standards also subsequently developed. In essence, even with the later creation of the market for backbone telecommunications services, a common stable denominator was preserved in the face of a governmental inter-connective TCP/IP naturally monopolized standard. In addition, in this

342. See Hanseth & Monterio, *supra* note 3, at 174 (explaining that new generations of infrastructure evolve by combining, extending and aligning existing infrastructure).

343. For a relevant early warning about such a possibility, see Bayh-Dole University and Small Business Patent Act of 1980 § 63, 15 U.S.C. § 3701(8) (2000).

344. See Peter Brockmann, *User Demand for Internet Services: Is the Infrastructure Ready?*, 20 COMPUTER STANDARDS AND INTERFACES 117-21 (1998) (for a broader perspective on potential infrastructure trends); Kaat, *supra* note 188, § 1; see also Lucent Technologies, *Seamless Roaming between WiFi and 3G Networks* (Mar. 2003) (describing the integration of WiFi and Third-Generation (“3G”) mobile networks to create comprehensive solutions with seamless roaming), <http://itpapers.com/abstract.aspx?kw=3g+&docid=47696> (last visited Dec. 3, 2003); Syntel, *Wireless Applications: A Natural Evolution* (Oct. 2001), <http://itpapers.com/abstract.aspx?kw=wireless&docid=16150> (last visited Dec. 3, 2003).

phase a consensual architecture was formally mandated, efficiently overshadowing the potential inter-institutional infrastructure standardization arms race.

In retrospect, only an *ex ante* governmental standard-setting initiative delegated through its early federal agencies and followed by monitored activity through research institutions was inherently efficient in the early infrastructure development phase. In this development phase of poor price-competition, the only exception was gradually giving away much of the government's power over the early market for carrying and access services, as was mostly done in the early 1990's. In essence, these infrastructure standard-setting activities were primarily technically, rather than commercially, motivated. That policy eventually changed with its move towards commercialization of application and complementary standardized products. These central changes led to substantial competition in standard-setting activity in cyberspace. In the future, such changes will continue to occur whenever such technological and economic developments take place, as part of future intermediate modification phases of different standardized technologies.

Later, the optimal institutional choice changes in the implementation phase. In this phase of application and complementary standardization, political institutions like the U.S. government through its delegated agencies, particularly the FCC, should stick to a restrained indirect role in standardization activity due to its institutional barriers to efficient participation. The government and its agencies may continue to have a role in the form of limited indirect support for infrastructure routine standard-setting activity, for example promoting increase in bandwidth on the backbone transmissions links and better physical access from homes and businesses. As a general matter, such a policy should also facilitate essential competition among autonomous standard-setting institutions. In practice, while the conduit has not always been lucid, nor followed a single fixed route, the governmental understanding of the public interest in the United States reveals a positive and definite prototype of declining centralized interference, notwithstanding an increasing number of such institutional sources.

Of special importance in this commercial environment is the role of autonomous industry institutions. New risks of *ex ante* technological stagnation and/or *ex post* anticompetitive effects mean that a role for a voluntary industry regulative approach in formalizing *gray* and *de facto* standardization will become essential. In later technological implementation phases, industry efficiently chills direct governmental incentives for intervention beforehand or *ex post*. This is subject only to indirect governmental supervision rules, which facilitate market production of standards and

procedural regulative intervention. Although many of these policies are upheld in practice, so far neither the U.S. government nor the FCC have articulated sufficiently clear or comprehensive policy on the matter. Thus far, this has left institutional choice in the Internet's standardization subject to overly general principles of marketplace competition, made to assure "reliability, interoperability, ease of use and scalability."³⁴⁵

For specific infrastructure standardization, potential risks of deviation from the government's justified proactive practices, already suggests policy conformity. One important case study for such potential digression came in the form of federal governmental involvement with ICANN. Although the DoC seems to maintain an oblique measure of control over the DNS and its root server, it is consistently doing so from a distance, almost in denial, based on a rhetoric that seems to pretend support for ICANN's final privatization. However, with the mounting political pressures against the U.S. government's intervention on the one hand, its attempt to "capture" ICANN's wide technological discretion on the other, there are no guarantees that such delicate, and relatively successful balance would be maintained in the future. The ICANN case study demonstrates that the question of technological infrastructure standardization was not raised properly *ex ante* as a policy question. This undermined the ability to confront real technological threats, such as the fragmentation of the network layer and root splitting. Such policy made no adequate division between infrastructure standards and application standards for matters of regulative intervention, hence providing ICANN, as a potentially self-interested interest group, overly broad control over both, but especially over the former.

Indeed, ICANN's technical mandate reaches potentially much further than is literally understood from existing formal documentation. Seen narrowly as mere technological routine standard-setting through technological "maintenance," no adequate governmental guidelines were put in place, thus undermining the necessity for a stable and preferably open standardization policy.

As with analogous standardization regimes, there is the risk that unless the distinctive standardization policies set forth in this study are viewed *en bloc*, and thus sequentially and contextually, cyberspace's largely successful institutional practice might not be preserved already for the present ICANN case study and to provide future benefit.

345. For the specific context of standard-setting, see Clinton & Gore, *A Framework*, *supra* note 14, § 9.