GOVERNANCE IN NAMESPACES

Stefan Bechtold∗

The assignment of numbers is also handled by Jon. If you are developing a protocol or application that will require the use of a link, socket, port, protocol, or network number please contact Jon to receive a number assignment.[1]

Anyone can assign names. We each do that all the time.[2]

eBay reserves the right to modify, alter or suspend any User ID at any time (at our sole discretion and without notice) for any reason whatsoever.[3]

∗ Research Assistant, University of Tübingen Law School, Germany; Fellow, 2002–2003, Center for Internet & Society, Stanford Law School; J.S.M., 2002, Stanford Law School; Dr. Iur. (J.S.D.), 2001, University of Tübingen Law School, Germany; Referendar (J.D.), 1999, University of Tübingen Law School, Germany. I would like to thank Peter Bechtold, Jonathan Greenberg, Jeff Gould, Brian Hemphill, Kurt Jaeger, Lawrence Lessig, Nelson Minar, Wernhard Möschel, Milton Mueller, Markus Müller, Tomas Sander, and the participants who attended workshops and seminars at Stanford Law School and the University of Tübingen Law School, Germany, as well as the TPRC 2002 participants for their valuable comments and suggestions.

1. Jon Postel, *Assigned Numbers*, Request for Comments (RFC) 776, at 1 (Jan. 1981), *at* http://www.rfc-editor.org/rfc/rfc776.txt.

2. Carl Ellison & Bruce Schneier, *Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure*, 16 COMPUTER SECURITY J. 1, 2 (2000), *available at* http://www.counterpane.com/pki-risks.pdf (last visited Jan. 22, 2003).

3. eBay, Inc., Frequently Asked Questions About User IDs, *at* http://pages.ebay.com/help/basics/f-faq-UserId.html#9 (last visited Jan. 9, 2003).

ABSTRACT

Since the creation of the Internet Corporation for Assigned Names and Numbers (ICANN), the regulation of the Domain Name System (DNS) has become a central topic in Internet law and policy discussions. ICANN's critics argue that ICANN uses its technical control over the DNS as undue leverage for policy and legal control over the DNS itself and over activities that depend on the DNS. Such problems are not unique to the DNS. Rather, the DNS discussions are an example of the more abstract governance problems that occur in a set of technologies known as "namespaces."

A namespace is a collection of all names in a particular system. Namespaces are ubiquitous. They can be found both in real space and cyberspace. Namespaces analyzed in this Article include the DNS, IP addresses, ENUM, Microsoft Passport, peer-to-peer systems, TCP port numbers, public key infrastructures as well as digital rights management and instant messaging systems. This Article also shows that many of its findings can also be applied to namespaces outside of cyberspace—such as bibliographic classification schemes, P.O. boxes, Social Security numbers, as well as the names of DNA sequences, diseases, and chemical compounds.

Namespaces are an overlooked facet of governance both in real space and cyberspace. This Article develops a general theory of the governance of namespaces. Designing namespaces and exercising control over them is not a mere technical matter. Rather, the technical control over a namespace creates levers for the intrusion of politics, policy, and regulation. In particular, the technical control may lead to speech, access, privacy, copyright, trademark, liability, conflict resolution, competition, innovation, and market structure regulation. The Article provides several dimensions along which namespaces can be analyzed. From a legal and policy perspective, it matters, for example, whether a namespace is centralized or decentralized, whether the namespace is controlled by a public or private entity, and the degree to which the internal structure is adaptive. These and other dimensions influence how namespaces protect social values and how they allocate knowledge, control, and responsibility. This Article will also demonstrate that the "end-to-end argument" was implemented on the Internet by a particular design of a specific namespace.

The taxonomic structure developed in this Article can be useful to legal and policy debates about the implications of various namespaces. It may also be helpful to designers of namespaces who consider the legal and policy consequences of their actions.

I. INTRODUCTION

In the fall of 2000, a Web site offered a new service allowing politicians, individuals, and corporations to bid on and buy political votes from citizens. The first Internet auction site for real votes had opened. The election in question was the U.S. presidential election of 2000, a memorable event for many reasons. The Web site in question, which described itself as "satirical," was located in Austria. It bore the name "voteauction.com."

After the Chicago Board of Election Commissioners filed a lawsuit against voteauction.com on October 18, 2000, the Circuit Court of Cook County, Illinois, issued an injunction against the Web site.[4] The company that registered the domain name was named as a co-defendant in the lawsuit.[5] After the court issued the injunction, the registrar cancelled the domain name, effectively shutting down the Web site all over the world.[6]

About a week later, the Web site appeared again under the new domain name "vote-auction.com." This time, the domain name was registered with a Swiss registrar. A few days later, it was also cancelled. However, no court issued any injunction ordering the cancellation. No official authority addressed the question of whether a domain name registered in Switzerland and located in Austria is subject to U.S. jurisdiction. Rather, the domain name was cancelled after some telephone and e-mail discussions between the Chicago Board of Election Commissioners and the Swiss domain name registrar. The Swiss registrar, a private entity, exercised its power over an asset, the domain namespace, to exclude this domain name from the Internet.[7]

4. *See* Henry H. Perritt, Jr., *Towards a Hybrid Regulatory Scheme for the Internet*, 2001 U. CHI. LEGAL F. 215, 242.

5. *See id.*

6. *See id.*

7. For more information on this case, see *id.* at 241–44; RTMark, Inc., Voteauction.com, *at* http://www.rtmark.com/voteauction.html (last visited Jan. 23, 2003).

In September 1998, a freshman at Northeastern University in Boston began working on a software program that would revolutionize online music business.[8] Only two and a half years later, the Napster network had over seventy million users who downloaded up to 2.8 billion music files per month.[9] In July 2000, the District Court for the Northern District of California issued a preliminary injunction effectively ordering Napster to shut down its service. The Court of Appeals for the Ninth Circuit later affirmed the injunction with some modifications.[10]

Voteauction.com and Napster each raise different problems. Voteauction.com is a case about election fraud, freedom of speech, and personal jurisdiction. Napster is a case about copyright infringement and innovation policy. At the same time, both cases are very similar. They illustrate how technical control over a particular component of a network can be used as leverage for legal and policy control. Voteauction.com lost both of its domain names because private entities—the domain name registrars and, ultimately, the domain name registry—could exclude its domain names from an authoritative list recognized by all computers connected to the Internet. Music files could no longer be shared over the Napster network because Napster could exclude them from an authoritative list of files recognized by all computers connected to the Napster network. In both cases, the network component that enabled this control was a namespace.

While namespaces may seem like an obscure concept of computer science, we are in fact surrounded by them. In the world of computers, the DNS, public key infrastructures (PKIs), Yahoo! Categories, Usenet newsgroups, and computer file systems are all examples of namespaces. Yet, namespaces are not confined to computers. Telephone numbers, Social Security numbers, the International Standard Book Number (ISBN), zip codes, bar codes, and bibliographic classification schemes form namespaces too.

8. *See* Karl Toro Greenfeld, *Meet the Napster*, TIME, Oct. 2, 2000, at 60; Steven Levy, *The Noisy War Over Napster*, NEWSWEEK, June 5, 2000, at 46.

9. *See* Jefferson Graham, *A Slimmed-Down Napster Gets Back Online; Trial Run Heavy on Little-Known Artists*, USA TODAY, Jan. 10, 2002, at D1.

10. *See* A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002); A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1004 (9th Cir. 2001).

Both Voteauction.com and Napster illustrate that, in cyberspace, the ability for legal regulation often depends on the technical control over a namespace. Technical namespaces are not unalterable given facts. Rather, technology is a social construct.[11] The cultural and societal structure of those who produce technology shape the technology itself.[12] Conversely, technology enables, shapes, and limits social, legal, and political relationships among citizens, businesses, and the state. Technology and law are therefore inherently intertwined. As Lawrence Lessig has shown, this interrelation between technology, law, and society implies that technology is not a neutral artifact, but can be shaped according to conscious design decisions that originate from external value systems.[13] Many design choices implicitly entail legal and policy choices.[14] The particular design of a namespace determines its

11. *See* MANUEL CASTELLS, THE INTERNET GALAXY 36 (2001); Thomas P. Hughes, *The Evolution of Large Technological Systems*, *in* THE SOCIAL CONSTRUCTION OF TECHNOLOGICAL SYSTEMS 51 (Wiebe E. Bijker et al. eds., 1994).

12. For an analysis of how the different cultures of early Internet users shaped the Internet, see CASTELLS, *supra* note 11, at 36–63.

13. *See, e.g.*, LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 26 (1999) [hereinafter LESSIG, CODE] (explaining that access to the Internet at University of Chicago and Harvard Law School differs because of administrators' dissimilar beliefs about free speech); *see also* WILLIAM J. MITCHELL, CITY OF BITS 111–12 (1995) (discussing effects of emerging civic strictures and spatial arrangements of the digital era); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 554 (1998) (technological capabilities and system design choices impose rules on participants). For an application of this theory in real space, see Neal Kumar Katyal, *Architecture as Crime Control*, 111 YALE L.J. 1039, 1039 (2002).

14. For analytical purposes, this Article follows an approach that distinguishes between a technology layer and a policy layer. *See* LESSIG, CODE, *supra* note 13; Reidenberg, *supra* note 13. Conversely, in his analysis of the domain name system, Milton Mueller uses a three-layered model. On the technical layer, name allocation is coordinated to ensure uniqueness and exclusivity of names. On the economic layer, finite namespaces deal with the allocation of scarce names. On the policy layer, decisions about rights attached to names are made. *See* MILTON L. MUELLER, RULING THE ROOT: INTERNET GOVERNANCE AND THE TAMING OF CYBERSPACE 17–26 (2002). However, it is questionable whether a distinction between an economic and a policy layer should be made. Economic decisions about name allocation are a subgroup of the various policy decisions that have to be made in namespaces. In general, a layered approach proves to be very helpful in analyzing cyberlaw questions. For the analysis of communication systems, Yochai Benkler has

regulatory impact. Therefore, namespaces can be seen as a technological tool to implement certain policy goals and legal value systems into a network.

This Article analyzes the interrelation between technology and law for namespaces in general. It attempts to highlight a common feature of namespaces: designing namespaces and exercising control over them is not a mere technical matter. The technical control over a namespace creates levers for the intrusion of politics, policy, and regulation.[15] By designing namespaces in a particular way, the implementation of many regulatory goals can either be achieved or prevented. To facilitate analysis, this Article develops several dimensions of namespace governance that prove helpful in assessing the regulatory impact of design decisions made at the technical level of a namespace. A namespace can be structured, for instance, in a flat, hierarchical, or decentralized manner. Its internal architecture can be heavily controlled or loosely coordinated. A namespace can be designed to serve many different purposes or a single, narrowly defined purpose. It can be controlled by technical or by contractual means. It can be administered by a public or private entity. Although such decisions seem of technical nature, they are in fact closely intertwined with legal and policy decisions. The Article will show that the very technological architecture of a namespace may encompass a regulation of speech, access, privacy, content, copyright, trademark, liability, conflict resolution, competition, innovation, and market structures. Therefore, legal and policy

developed a layered analytical framework. In Benkler's model, communication systems can be divided into the physical layer (e.g., the wires, cables, fibers, radio frequency spectrum, printing presses), the logical layer (the software and standards that decide which expression is transmitted over the physical layer and that enable this transmission), and the content layer. *See* LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 23–25 (2001) [hereinafter LESSIG, FUTURE OF IDEAS]; François Bar & Christian Sandvig, *Rules From Truth: Post-Convergence Policy for Access* 21 (Sept. 2000), *available at* http://www.stanford.edu/~fbar/Publications/Rules_from_Truth.pdf; Yochai Benkler, *Property, Commons, and the First Amendment: Towards a Core Common Infrastructure* 3 (Mar. 2001), *available at* http://www.law.nyu.edu/benklery/WhitePaper.pdf; Kevin Werbach, *A Layered Model for Internet Policy* (Sept. 1, 2000), *at* http://www.edventure.com/conversation/article.cfm?Counter=2414930.

15. *See* MUELLER, *supra* note 14, at 10.

considerations should be taken into account even during the design stages of a namespace.

The analysis of such questions is not novel. The best-known namespace on the Internet is the DNS. Most computers connected to the Internet are equipped with a unique numerical IP address and a unique domain name.[16] The DNS maps each domain name to an IP address. It is a prime example of how namespace control transcends the borders of technology and reaches into policy and law. Since 1998, the DNS has been managed by ICANN,[17] a private non-profit corporation under California law.[18] The status of ICANN is highly disputed. While some proponents assert that ICANN is a mere technical standardization and coordination body, critics argue that it more resembles a world government.[19] Furthermore, critics of ICANN think that it unjustly uses its control over the technical DNS infrastructure as leverage to control policy aspects of Internet communications such as trademark and copyright issues, surveillance of Internet users, regulation of content, imposition of tax-like fees, and the regulation of the domain name supply industry.[20]

The DNS governance discussions are an example of the regulatory questions this Article addresses. However, this is not an article about the governance of the DNS. Although many issues addressed by this Article are discussed in the context of the DNS, the discussions about the DNS and ICANN often fail to recognize that these issues are not unique to the DNS. Rather, they are general governance problems of namespaces that can be found in other namespaces—from peer-to-peer (P2P) systems to instant messaging systems—as well. They are not even confined to the computer world. In real space, many namespaces—from bibliographic classification schemes to Social Security numbers—exhibit the same problems.

16. Some computers are only equipped with an IP address, but not a domain name.

17. ICANN, About ICANN, *at* http://www.icann.org (last modified Jan. 11, 2002).

18. *See* ICANN, Background, *at* http://www.icann.org/general/background.htm (last modified July 16, 1999).

19. Mueller has criticized the ICANN regime as "a conservative, corporatist regime founded on artificial scarcity and regulatory control." MUELLER, *supra* note 14, at 267.

20. *See id.*

No literature exists that identifies and discusses governance dimensions of namespaces on such an abstract, general level.[21] This Article not only attempts to fill that gap, but its findings can be applied to a wide range of namespaces both in cyberspace and real space. While the study of namespaces at an abstract level may be novel, it does not operate in an analytical vacuum. Many namespaces are scarce resources: the number of names that can be assigned in such namespaces falls short of the demand.[22] In bottleneck namespaces, the assignment of names has to be controlled in some way. Analyzing the legal implications of such bottleneck situations is not an unknown task. In antitrust law, the essential facilities doctrine deals with the control of a monopolist over scarce resources.[23] In communications law, common carrier regulations cope with adverse impacts of privately owned bottlenecks in the communication infrastructure.[24] The discussion whether broadband cable providers should be forced to open their networks to non-affiliated Internet service providers ("open access") is a discussion about the impact of a privately owned bottleneck: the cable network.[25] In First Amendment law, courts have regularly allocated access to different types of mass media that are allegedly

21. For an analysis of the related problems of classification, see GEOFFREY C. BOWKER & SUSAN LEIGH STAR, SORTING THINGS OUT: CLASSIFICATION AND ITS CONSEQUENCES (1999).

22. The telephone number space, the current IP address space, and the generic top level domain namespace are examples of scarce namespaces. *See infra* note 191.

23. *See* United States v. Terminal R.R. Ass'n of St. Louis, 224 U.S. 383, 404–09 (1912); *see also* Robert Pitofsky, *The Essential Facilities Doctrine Under United States Antitrust Law*, *available at* http://www.ftc.gov/os/comments/intelpropertycomments/pitofskyrobert.pdf (last modified Jan. 7, 2003) (discussing the development of the essential facilities doctrine beginning with *United States v. Terminal Railroad Association of St. Louis*).

24. *See, e.g.*, James H. Lister, *The Rights of Common Carriers and the Decision Whether to Be a Common Carrier or a Non-Regulated Communications Provider*, FED. COMM. L.J., Dec. 2000, at 91; Peter K. Pitsch & Arthur W. Bresnahan, *Common Carrier Regulation of Telecommunications Contracts and the Private Carrier Alternative*, FED. COMM. L.J., June 1996, at 447.

25. *See* Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. REV. 925 (2001).

bottlenecks.[26] Finally, an emerging scholarship addresses specific regulatory problems of information and technology platforms, which can represent bottlenecks as well.[27]

Therefore, while analyzing bottleneck situations is not uncommon, this Article chooses a slightly different analytical approach. Rather than focusing on one specific area of law, it analyzes the implications of a particular technology—for example, namespaces—on a wide variety of areas of law and legal policy. It assesses how different design choices at the technical level create, alter, or eliminate the regulatory problems with which law and legal policy have to grapple.

---

26. *See generally* Arkansas Educ. Television Comm'n v. Forbes, 523 U.S. 666 (1998) (holding that a broadcaster could exclude a candidate from debate); Turner Broad. Sys., Inc. v. FCC, 520 U.S. 180 (1997) (reaffirming the decision that cable providers devote some channels to local broadcasting); Denver Area Educ. Telecomm. Consortium, Inc. v. FCC, 518 U.S. 727 (1996) (prohibiting indecent programming on leased channels does not violate the First Amendment, but prohibiting such programming on public access channels does); Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 656 (1994) (upholding congressional act requiring cable providers to dedicate some channels to local broadcasting); Columbia Broad. Sys., Inc. v. FCC, 453 U.S. 367 (1981); Miami Herald Publ'g Co. v. Tornillo, 418 U.S. 241 (1974) (striking down a state "right to reply" law that compelled newspapers to grant political candidates equal space to reply to criticism); Columbia Broad. Sys., Inc. v. Democratic Nat'l Comm., 412 U.S. 94 (1973); Red Lion Broad. Co. v. FCC, 395 U.S. 367 (1969) (upholding FCC interpretation of the "fairness doctrine" that required broadcasters to present both sides of public issues).

27. *See, e.g.*, Douglas Lichtman, *Property Rights in Emerging Platform Technologies*, 29 J. LEGAL STUD. 615 (2000); Pamela Samuelson & Susanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L.J. 1575, 1611, 1615–26, 1643–44, 1662 (2002); Molly S. Van Houweling, *Cultivating Open Information Platforms: A Land Trust Model*, 1 J. TELECOMM. & HIGH TECH. L. 309 (2002); Philip J. Weiser, *Internet Governance, Standard Setting, and Self-Regulation*, 28 N. KY. L. REV. 822, 832–42 (2001) [hereinafter Weiser, *Internet Governance*]; Philip J. Weiser, *Law and Information Platforms*, 1 J. TELECOMM. & HIGH TECH. L. 1 (2002); Bar & Sandvig, *supra* note 14; Philip J. Weiser, *Networks Unplugged: Towards a Model of Compatibility Regulation Between Information Platforms* (Sept. 24, 2001), *at* http://www.arxiv.org/html/cs/0109070; *see also* ANNABELLE GAWER & MICHAEL A. CUSUMANO, PLATFORM LEADERSHIP: HOW INTEL, MICROSOFT, AND CISCO DRIVE INDUSTRY INNOVATION (2002); Arti K. Rai & Rebecca S. Eisenberg, *The Public and the Private in Biopharmaceutical Research*, *available at* http://www.law.duke.edu/pd/papers/raieisen.pdf (last visited Jan. 22, 2003) (addressing the erosion of free access to new knowledge in the public domain as patent claims have expanded).

The Article proceeds as follows: Part II provides a more precise definition of namespaces. Part III develops several dimensions of namespace governance that can be applied to namespaces in general. Further, it shows the legal and policy implications of design decisions made along these dimensions. In Part IV, a more abstract account of the relationship between namespace design and the law is provided. Part V addresses the extent to which these insights can be applied in the actual design of namespaces. Part VI concludes the Article.

II. WHAT'S IN A NAME?

Names are important tools for identification and communication both in real space and cyberspace. From a legal and social science perspective, personal names are a crucial aspect of personal identity and dignity.[28] A complex mix of social norms, memories, connotations, and shared experiences influences the esteem of personal names, in particular first names.[29] From an economic perspective, commercial names and trademarks facilitate identification and thereby reduce consumer search costs.[30] From a computer science perspective, the definition of "name" is even more sober—a name is a string of bits or characters that refers to a resource.[31] In communication networks, some method to identify and locate the networked resources must exist. Names provide a method to facilitate sharing and communication.[32] They can bring consistency to the network—names uniquely identify resources, and

28. *See* Douglas A. Galbi, *A New Account of Personalization and Effective Communication* 4 (Sept. 2001), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=286288.

29. *See id.* at 6.

30. *See* William M. Landes & Richard A. Posner, *Trademark Law: An Economic Perspective*, 30 J.L. & ECON. 265, 269 (1987).

31. *See* ANDREW S. TANENBAUM & MAARTEN VAN STEEN, DISTRIBUTED SYSTEMS: PRINCIPLES AND PARADIGMS 184 (2002); John F. Shoch, *Inter-Network Naming, Addressing, and Routing*, *in* PROCEEDINGS OF THE 17TH IEEE COMPUTER SOCIETY INTERNATIONAL CONFERENCE 72 (1978); David R. Cheriton & Timothy P. Mann, *Decentralizing a Global Naming Service for Improved Performance and Fault Tolerance*, 7 ACM TRANSACTIONS ON COMPUTER SYS. 147 (1989).

32. *See* ROSS J. ANDERSON, SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS 125 (2001).

thereby eliminate the risk of confusion between different, but similar, resources. In general, names both store and filter information.

Computer science, in particular the theory of distributed systems,[33] developed a rather rigorous theory of naming that proves helpful for the following analysis of namespaces. In general, different kinds of names exist. An "address" is a special type of name that "identifies the location of the object rather than the object itself."[34] The IP address of a computer and a telephone number are addresses in this sense. Addresses are not well-suited to persistently identify objects. Once an object is moved to another location, its address changes. If a computer connected to the Internet, for instance, is moved to another location, its IP address often has to be changed as well.[35] If a phone customer moves to a new city, he receives a new phone number, even if he uses the same telephone. Without call-forwarding features and number portability regulations,[36] a phone number does not identify a particular telephone, but its location, that is, the jack into which it is plugged.

In many communication networks, these shortcomings of addresses are resolved by adding a layer of location-independent names on top of the addressing scheme.[37] While addresses *locate*

33. In a distributed system, hardware or software components are located at different computers that are only connected by a communication network. Although the components are dispersed throughout the network, a distributed system appears to its users as one single coherent system. *See* GEORGE COULOURIS ET AL., DISTRIBUTED SYSTEMS: CONCEPTS AND DESIGN 2 (3d ed. 2001); TANENBAUM & VAN STEEN, *supra* note 31, at 2. While numerous distributed systems exist, the most important example is the Internet. For research on naming infrastructures in homogeneous computer systems, see Roger M. Needham, *Names*, *in* DISTRIBUTED SYSTEMS 315, 317 (Sape Mullender ed., 2d ed. 1994); Jerome H. Saltzer, *On the Naming and Binding of Objects*, *in* OPERATING SYSTEMS: AN ADVANCED COURSE 99–208 (Rudolf Bayer et al. eds., 1978).

34. COULOURIS ET AL., *supra* note 33, at 354; *see also* Shoch, *supra* note 31, at 72; TANENBAUM & VAN STEEN, *supra* note 31, at 184.

35. This problem is most prevalent with mobile computers. *See* TANENBAUM & VAN STEEN, *supra* note 31, at 184–85. Uniform Resource Locators (URLs) are another example of the shortcomings of addresses as consistent identifiers. *See* COULOURIS ET AL., *supra* note 33, at 356; *see also infra* note 240 (defining and explaining URLs).

36. *See infra* note 172.

37. *See* TANENBAUM & VAN STEEN, *supra* note 31, at 185; *see also* Richard W. Watson, *Identifiers (Naming) in Distributed Systems*, *in* DISTRIBUTED

resources, location-independent names *identify* them.[38] The domain *name* of a computer, for example, identifies a computer, while its IP *address* reveals its logical location. Location-independent names and addresses do not exist separately. Rather, names are resolved to addresses by so-called "name services."[39] Name services allow users and software programs to look up, add, change, and remove names.[40] The layering of location-independent names on top of an addressing scheme makes the communication network more flexible—the address of a resource can be changed without having to change its name. Thereby, resources can be moved without any alteration of their name. The aforementioned DNS is a name service that resolves domain names to IP addresses. Although a computer's IP address may have to be changed when its location is moved, its domain name may remain the same.

The collection of all valid names in a particular system forms a "namespace."[41] Some namespaces are designed for human use, while other namespaces are accessed by computers only. Names used by human beings should usually be "mnemonically useful," while the critical feature of names used by computers is that they are

SYSTEMS: ARCHITECTURE AND IMPLEMENTATION 191, 196 (Butler W. Lampson et al. eds., 1981).

38. "The *name* of a resource indicates what we seek, and *address* indicates where it is, and a *route* tells us how to get there." Shoch, *supra* note 31, at 72.

39. COULOURIS ET AL., *supra* note 33, at 357; *see* TANENBAUM & VAN STEEN, *supra* note 31, at 183. While a name service resolves names to addresses, a "directory service" connects names to a wider collection of attributes. Conventional name services can be compared to the telephone white pages, while directory services resemble the yellow pages. *See* COULOURIS ET AL., *supra* note 33, at 371; TANENBAUM & VAN STEEN, *supra* note 31, at 2.

40. *See* TANENBAUM & VAN STEEN, *supra* note 31, at 194.

41. *See* COULOURIS ET AL., *supra* note 33, at 358; TANENBAUM & VAN STEEN, *supra* note 31, at 186; Ronald Bourret, XML Namespaces FAQ, § 2.1, *at* http://www.rpbourret.com/xml/NamespacesFAQ.htm#q2_1 (last updated Feb. 2003). For a helpful proposition of a unified terminology for directories and namespaces, see Harald Tveit Alvestrand, *Definitions for Talking About Directories*, Request for Comments (RFC) 3254 (Apr. 2002), *at* http://www.rfc-editor.org/rfc/rfc3254.txt.

"unambiguously resolvable."[42] In such a namespace, names must be unique.[43]

Namespaces are pervasive, both in cyberspace and in real space. In cyberspace, namespaces are mainly used to identify four different kinds of resources: computers (or more generally, devices), users, files, and applications (or more generally, services).[44] Device namespaces include the DNS, the telephone number system, ENUM,[45] as well as IP and Ethernet addresses.[46] User namespaces include Microsoft Passport,[47] the Liberty Alliance Project,[48] PKIs[49] as well as user identification systems on eBay, in the AOL network, and in instant messaging systems and networked computer games.[50] URLs, P2P systems,[51] Yahoo! Categories and the different computer file systems available[52] are examples of file namespaces. Service namespaces are created, for instance, by Transmission Control Protocol/User Datagram Protocol (TCP/UDP) port numbers[53] and the Universal Description, Discovery and Integration (UDDI) service in

42. Saltzer, *supra* note 33, at 121; *see also* MUELLER, *supra* note 14, at 39 (asserting that mnemonics and providing single, more stable identities are two reasons for naming computers).

43. To achieve uniqueness, names are either universally valid, or are equipped with a representation of the context in which they are unique. *See* Needham, *supra* note 33, at 90.

44. *See* ANDERSON, *supra* note 32, at 131–32; COULOURIS ET AL., *supra* note 33, at 356; TANENBAUM & VAN STEEN, *supra* note 31, at 184; Cheriton & Mann, *supra* note 31, at 147; Jerome H. Saltzer, *On the Naming and Binding of Network Destinations*, Request for Comments (RFC) 1498 (Aug. 1993), *at* http://www.rfc-editor.org/rfc/rfc1498.txt.

45. *See infra* text accompanying notes 92–95.

46. *See infra* text accompanying notes 193–201.

47. *See infra* text accompanying notes 76–77.

48. *See infra* text accompanying note 156.

49. *See infra* text accompanying notes 86–87.

50. For a study of a virtual world computer game, such as Everquest, see Edward Castronova, *Virtual Worlds: A First-Hand Account of Market and Society on the Cyberian Frontier*, THE GRUTER INST. WORKING PAPERS ON LAW, ECON., AND EVOLUTIONARY BIOLOGY (Oct. 2001), *available at* http://www.bepress.com/cgi/viewpdf.cgi?article=1008&context=giwp.

51. *See infra* text accompanying note 127.

52. For an overview, see Martin Hinner, *Filesystems HOWTO*, *at* http://www.linux.org/docs/ldp/howto/Filesystems-HOWTO.html (last modified Aug. 22, 2000). For an overview of distributed file systems, see TANENBAUM & VAN STEEN, *supra* note 31, at 575–646.

53. *See infra* notes 202–04.

the context of Web services.[54] Some technologies even use multiple namespaces. Digital rights management (DRM) systems, for example, employ device, user, and file namespaces at the same time.[55] The list of namespaces used by computers and computer networks is endless.[56]

In real space, telephone, credit card, bank account, passport, Social Security numbers, and tax identifiers are namespaces which identify devices, natural persons, or corporate entities. People, streets, cities, countries, and species are all identified by namespaces as well. Other examples include P.O. boxes, natural languages, and the system of longitude and latitude. The travel industry uses several namespaces to identify travel agencies, hotels, airlines, car rental companies, travel insurance companies, and consumers.[57] The Dun

54. *See* http://www.uddi.org (last visited Feb. 3, 2003). UDDI enables organizations that develop Web services to register these services in a public database so that client applications may locate and use them. For an overview of UDDI, see ETHAN CERAMI, WEB SERVICES ESSENTIALS 157–99 (Simon St. Laurent ed., 2002); DAVID CHAPPELL, UNDERSTANDING .NET: A TUTORIAL AND ANALYSIS 65–71 (2002); THUAN THAI & HOANG Q. LAM, .NET FRAMEWORK ESSENTIALS 155–57 (Nancy Kotary ed., 2d ed. 2002).

55. By a combination of various technical and legal means of protection, DRM attempts to create a framework for the secure distribution of digital content to authorized users. DRM systems usually employ a number of different namespaces, such as namespaces for identifying users (important for digital fingerprinting and thereby individualizing content), identifying content (important for managing the rights attached to the content), and identifying devices (important for distinguishing authorized from unauthorized devices and for revoking compromised device keys). For an overview, see Stefan Bechtold, *From Copyright to Information Law: Implications of Digital Rights Management*, *in* SECURITY AND PRIVACY IN DIGITAL RIGHTS MANAGEMENT 213, 214–16 (Tomas Sander ed., 2002), *available at* http://www.jura.uni-tuebingen.de/~s-bes1/pub/2002/DRM_Information_Law.pdf [hereinafter Bechtold, *From Copyright to Information Law*]. For a more detailed discussion, see STEFAN BECHTOLD, VOM URHEBER-ZUM INFORMATIONSRECHT: IMPLIKATIONEN DES DIGITAL RIGHTS MANAGEMENT 34–75 (2002) [hereinafter BECHTOLD, VOM URHEBER-ZUM INFORMATIONSRECHT].

56. Other computer namespaces include variable names in computer languages, character sets, the X.500 directory service, XML namespaces, colorspaces such as RGB or CMYK, databases, and Microsoft Smart Tags. For even more namespaces, see IANA, Protocol/Number Assignments Directory, *at* http://www.iana.org/numbers.html (last updated Apr. 18, 2002).

57. Air travel customer information is usually stored in a so-called "Passenger Name Record" (PNR) in one of the major proprietary Global Distribution Systems (GDS) such as Amadeus, Sabre, or Apollo. Other

& Bradstreet Data Universal Numbering System (D-U-N-S) is used to identify sixty-two million business entities around the world,[58] while the Thomas Register of American Manufacturers provides unique supplier IDs for over 173,000 U.S. and Canadian manufacturers.[59] The system of bar codes that is used for product identification is another example of how widely namespaces are used today.[60] For example, millions of DNA sequences from over 100,000 species are uniquely identified and named by an international namespace provided by several databases.[61] The International Statistical Classification of Diseases and Related Health Problems (ICD) is a namespace maintained by the World Health Organization that classifies all statistically significant diseases.[62] In addition, traditional media can be identified by different namespaces such as the ISBN, the International Standard Recording Code (ISRC), the International Standard Serial Number (ISSN), the Unique Material Identifier (UMID), and the International Standard Work Code (ISWC).[63] Finally, bibliographic classification schemes,[64] the frequency spectrum, the various international classification systems for classifying inventions, trademarks, and

namespaces in the travel industry are administered by the International Air Transport Association. *See, e.g.*, Travel Industry Designator Service, *at* http://www.iata.org/tids/index (2001); *see* Rohit Khare, *Anatomy of a URL (and Other Internet-Scale Namespaces, Part 1)*, IEEE INTERNET COMPUTING, Sept.–Oct. 1999, at 78, 80.

58. *See* D&B D-U-N-S® Number, *at* http://www.dnb.com/US/duns_update/duns_update_print.asp (last visited Feb. 16, 2003).

59. *See* Thomas Register, *at* http://www.thomasregister.com (last visited Jan. 14, 2003).

60. For information on the Universal Product Code (UPC) and the European Article Number (EAN), see Uniform Code Council, Inc.: ID Numbers and Bar Codes, *at* http://www.uccouncil.org/main/ID_Numbers_and_Bar_Codes.html (2002) and EAN International, *at* http://www.ean-ucc.org (2002). The Auto-ID project at MIT attempts to extend this model with "electronic Product Codes" (ePC) that can be embedded into smart tags and resolved by an "Object Naming Service." *See* Auto-ID Center, *at* http://www.autoidcenter.org/abouttthetech_indepthlook.asp (last visited Jan. 16, 2003).

61. *See infra* text accompanying notes 162–65.

62. *See* BOWKER & STAR, *supra* note 21, at 55–57, 68–90.

63. For an overview, see BECHTOLD, VOM URHEBER-ZUM INFORMATIONSRECHT, *supra* note 55, at 39–41.

64. *See infra* text accompanying note 252.

industrial designs,[65] the ISO 3166 list of country codes,[66] as well as the names of all celestial objects[67] and chemical compounds[68] may complete this listing of namespaces. In short, namespaces are important and ubiquitous.[69]

As the variety and sheer number of all existing namespaces are overwhelming, it is an impossible task to analyze all of them in this Article. Fortunately, in order to develop a general theory of namespace governance, this is also an unnecessary task. This Article uses several namespaces to illustrate the presented theoretical framework. Nevertheless, the framework should also be applicable to namespaces that are not explicitly studied in this Article.

III. DIMENSIONS OF NAMESPACE GOVERNANCE

By analyzing the means, intensity, and scope of namespace governance, as well as the possible namespace topologies, this Part identifies several dimensions of namespace governance that illustrate the close intertwining of technology, law, and policy.

A. Means of Namespace Governance

In general, namespace providers have varying interests in regulating the use of and access to their namespace. They may, for example, want to grant access to the namespace only under certain conditions, or to prevent certain end users from using the namespace altogether. They may also grant third-party service providers, who use the namespace in their own services, access to the namespace only after payment of a fee. Namespace providers therefore want to regulate the behavior of namespace users and service providers.

65. The World Intellectual Property Organization (WIPO) administers four international classification systems. *See* WIPO, International Classifications, *at* http://www.wipo.org/classifications/en/overview.html (last visited Feb. 16, 2003).

66. *See* Maintenance Agency for ISO 3166 Country Codes, *at* http://www.iso.org/iso/en/prods-services/iso3166ma/index.html (last visited Jan. 13, 2003).

67. Commission 5 of the International Astronomical Union is the commission that names stars and other celestial objects. *See* International Astronomical Union, Designations and Nomenclature of Celestial Objects, *at* http://www.iau.org/IAU/Activities/nomenclature (last modified Dec. 27, 2000).

68. *See infra* note 264.

69. *See* BOWKER & STAR, *supra* note 21, at 37–39.

Such regulation can be achieved by different means. While several namespaces employ a web of contracts, all namespaces use technological means to regulate behavior that depends on the namespace.

1. Governance by contract

Namespace providers can condition access to and use of their namespace upon the prior conclusion of a contract. Namespace contracts include more than agreements about technical issues. They may limit the ways in which users access a namespace. They may also restrict the purposes and conditions under which the namespace can be accessed. Furthermore, they may restrict environments in which the names may be used or processed.

In many namespaces, the namespace provider attempts to bind all end users and service providers by contract. A web of contracts laid over the namespace is intended to protect various non-technical interests of the namespace provider (see Figure 1).

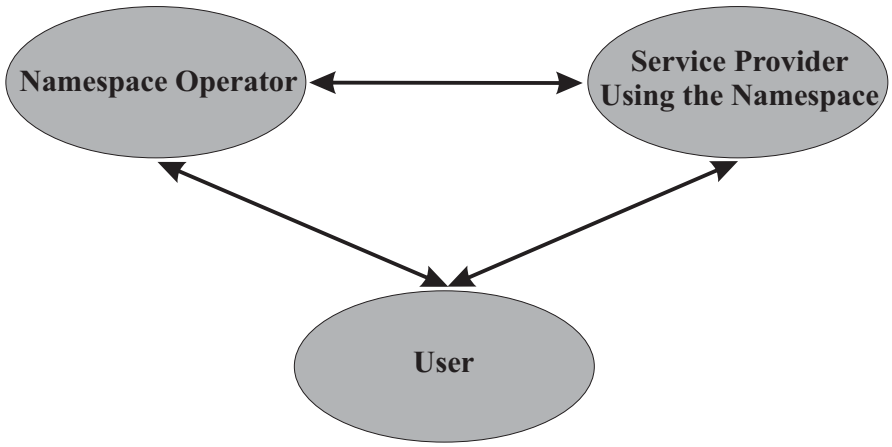

Figure 1: Namespace Governance by Contractual Webs

The DNS[70] uses such a web of contracts to govern the domain namespace. All registrants, registrars, and registries of domain

70. The DNS is a distributed name resolution service that resolves domain names to numerical IP addresses. For an overview of the architecture, history, and policy debate of the DNS, see MUELLER, *supra* note 14, at 47–48; A. Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution*, 50 DUKE L.J. 17 (2000); Jay P. Kesan &

names in generic top-level domains (gTLDs), such as .com, .biz, .net, and .org, are required to enter into contractual agreements that either directly or indirectly originate from ICANN, the entity that currently controls the DNS.[71] In order to resolve conflicts between domain name registrations and trademark law, ICANN, after considerable input from WIPO, created a dispute resolution mechanism. This Uniform Dispute Resolution Policy (UDRP)[72] enables a trademark holder to challenge the registration of a domain name and potentially gain control over it. As part of the contracts between ICANN and the gTLD registrars,[73] ICANN requires the registrars to impose the UDRP on everyone who wants to register a domain name.[74] As a result, on the one hand, ICANN binds all registrars to the UDRP as a condition of their accreditation. On the other hand, a consumer who wants to register a domain name under the .com gTLD, for example,

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 (2001) (detailing the privatization processes for the DNS and proposing measures for future privatization).

71. *See* A. Michael Froomkin & Mark A. Lemley, *ICANN and Antitrust*, U. ILL. L. REV.__, 13–16 (forthcoming 2003), *available at* http://papers.ssrn.com/sol3/delivery.cfm/SSRN_ID291221_code011128630.pdf?abstractid=291221#Paper%20Download. This contractual web does not exist for country code top-level domains (ccTLDs). The relationship between ICANN's overall governance of the domain namespace and the ccTLD registries is not entirely clear. ccTLD registries have at least some independence in determining policies for their ccTLD sub-namespaces. *See* MUELLER, *supra* note 14, at 205–08; Tamar Frankel, *The Managing Lawmaker in Cyberspace: A Power Model*, 27 BROOK. J. INT'L L. 859, 886–93 (2002). Although ICANN is known for managing the DNS, the U.S. government still retains residual authority over the DNS root and has not expressed its intent to give up this authority in the future. For the relationship between the U.S. Department of Commerce and ICANN, see MUELLER, *supra* note 14, at 197; Froomkin, *supra* note 70, at 91, 105–25; Froomkin & Lemley, *supra*, at 11–13.

72. *See* ICANN, Uniform Domain Name Dispute Resolution Policy, *at* http://www.icann.org/udrp/udrp-policy.htm (last modified May 17, 2002).

73. For many ccTLDs, no equivalent to the UDRP system exists. In such countries, domain name trademark conflicts are left to the traditional court system to resolve. This, for example, is the case in Germany. In other namespaces such as the telephone number space, no UDRP equivalent exists either. *See In re* Toll Free Service Access Codes, 13 F.C.C.R. 9058, 9067 (1998).

74. *See* ICANN, Registrar Accreditation Agreement § II.K, *at* http://www.icann.org/nsi/icann-raa-04nov99.htm (Nov. 4, 1999).

will only be able to register it if he agrees to the terms of the UDRP as well. Through a hierarchical web of contracts originating from ICANN, ICANN has ensured that every registrar and every registrant is bound to the UDRP.[75] ICANN effectively enveloped the domain namespace with a web of contracts that they use to protect, among other things, the trademark holder's interests.

Another example of contractual webs as a means of namespace governance is Microsoft Passport.[76] By mapping unique identifiers to individual users, this system allows users to establish lasting digital identities on the Internet. Once a user is registered in this user namespace, he can access all Web sites that use Microsoft Passport as their authentication service without having to authenticate himself at each individual Web site, as Microsoft Passport will provide the participating Web site with the necessary authentication information.[77]

In order to ensure that participating Web sites do not use this authentication information for data mining and user profiling purposes, Microsoft has entangled the technical namespace with a web of contracts. Before a Web site can use the Passport authentication service, it has to agree by contract with Microsoft to obtain the user's consent before it uses the profile information for marketing purposes. It is also contractually required to post privacy policies on its site, both in a human-readable and machine-readable, P3P-compliant[78] format.[79]

75. *See* MUELLER, *supra* note 14, at 192.

76. *See* Microsoft Corp., Microsoft .NET Passport, *at* http://www.passport.net/Consumer/default.asp?lc=1033 (last visited Dec. 16, 2002).

77. User namespaces such as Microsoft Passport therefore enable a so-called "single sign-in" (SSI). *See* Microsoft Corp., .NET Passport Review Guide, *at* http://microsoft.com/netservices/passport/passport.asp (Nov. 2002) [hereinafter Microsoft Corp., .NET Passport Review Guide]. With more than 200 million accounts performing more than 3.5 billion authentications each month, Passport is currently the prevailing general authentication system. *See* Microsoft Corp., .NET Passport Overview, *at* http://www.microsoft.com/netservices/passport/overview.asp (Mar. 20, 2002).

78. The Platform for Privacy Preferences Project (P3P) allows Web sites to express their privacy policies in a machine-readable format. It enables users to evaluate these policies and make informed decisions about the privacy implications of accessing a particular Web site. For more information on P3P, see Ruchika Agrawal, *P3P Viewpoints*, *at* http://www.stanford.edu/~ruchika/P3P/home.html (last modified Mar. 11, 2002); World Wide Web Consortium,

In addition to the contractual relationship between Microsoft and participating Web sites, Microsoft attempts to establish a contractual relationship with each Passport user as well. Before a user can register with Microsoft Passport, he must agree to the "Microsoft .NET Passport Terms of Use and Notices."[80] In this user contract,

Platform for Privacy Preferences, *at* http://www.w3.org/P3P/ (last modified Nov. 8, 2002).

79. *See* Microsoft Corp., .NET Passport Review Guide, *supra* note 77, at 22. Furthermore, if, in the process of delivering goods or services to the user, the participating site has to share personal information (e.g., the user's address) with a third party (e.g., a shipping service), the participating site is required by Microsoft to impose certain contractual obligations on the third party as well. *See id.* at 21. In effect, Microsoft's strategy resembles a "viral contract" attached to private data. A viral contract attempts "to make commitments run with a digital object. . .so that everyone who comes into possession of the [object]. . .also inherit[s] the obligations to the initiator [of the contract]." Margaret Jane Radin, *Humans, Computers, and Binding Commitment*, 75 IND. L.J. 1125, 1132 (2000).

80. Microsoft Corp., Microsoft .NET Passport Terms of Use and Notices*, at* http://www.passport.net/Consumer/TermsOfUse.asp (last revised Aug. 2002). It is contested whether such "click-wrap licenses" are enforceable contracts. The problems posed by click-wrap licenses are similar to the question whether computer software shrink-wrap licenses are valid contracts. Traditionally, U.S. courts have been reluctant to enforce shrink-wrap licenses. *See* Step-Saver Data Sys., Inc. v. Wyse Tech., 939 F.2d 91, 98–100 (3d Cir. 1991); Ariz. Retail Sys., Inc. v. Software Link, Inc., 831 F. Supp. 759, 764–66 (D. Ariz. 1993); *see also* Novell, Inc. v. Network Trade Ctr., Inc., 25 F. Supp. 2d 1218 (D. Utah 1997) (explaining that the shrinkwrap license is invalid against first purchaser pertaining to the title of the software in copyright owner), *vacated in part by* Novell, Inc. v. Network Trade Ctr., Inc., 187 F.R.D. 657 (D. Utah 1999); Morgan Lab., Inc. v. Micro Data Base Sys., Inc., 41 U.S.P.Q. 2d 1850 (N.D. Cal. 1997). However, in 1997, Judge Easterbrook of the Seventh Circuit Court of Appeals found a shrink-wrap a valid contract. *See* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1450–53 (7th Cir. 1996). Following this decision, other courts have enforced shrink-wrap licenses as well. *See* Hill v. Gateway 2000, Inc., 105 F.3d 1147 (7th Cir. 1997); M.A. Mortenson Co. v. Timberline Software Corp., 998 P.2d 305, 313 (Wash. 2000); Brower v. Gateway 2000, Inc., 676 N.Y.S.2d 569, 572 (N.Y. App. Div. 1998). Courts have also held click-wrap licenses as enforceable contracts. *See* I.Lan Sys., Inc. v. Netscout Serv. Level Corp., 183 F. Supp. 2d 328, 338–39 (D. Mass. 2002); Caspi v. The Microsoft Network, L.L.C., 732 A.2d 528 (N.J. Super. Ct. App. Div. 1999); *see also* Groff v. America Online, Inc., 1998 WL 307001 (R.I. Super. Ct. 1998) (discussing how the click-wrap contract binds a party to a forum selection clause); *but see* Specht v. Netscape Communications Corp., 306 F.3d 17 (2d Cir. 2002). For a general overview, see Robert A. Hillman & Jeffrey J. Rachlinski, *Standard-Form Contracting in the Electronic Age*, 77 N.Y.U. L. REV. 429 (2002).

Microsoft agrees to use personal information only in accordance with its Passport privacy policy. According to this policy, Microsoft discloses personal information only if the user has consented or if Microsoft is required to disclose information by law.[81]

As ICANN did in the DNS context, Microsoft has enveloped Passport in a web of contracts. This web is used by Microsoft to regulate non-technical, in particular privacy-related, aspects of its namespace. This is not to say that Microsoft Passport protects privacy perfectly or even adequately.[82] This example merely reinforces the claim that namespace providers use contractual webs as a tool to regulate non-technical behavior of namespace users and service providers.

The use of contractual webs for governing namespaces is not confined to the DNS and Microsoft Passport. DRM systems[83] use similar mechanisms. In general, the webs of contracts surrounding namespaces bind both service providers that depend on the namespace and individual namespace users. Namespace providers may use these contractual webs to regulate various legal and policy aspects of namespaces, ranging from intellectual property and privacy protection to competition issues.

2. Governance by technology

Contractual webs would not be a very promising means of namespace governance if the contracts were, as a practical matter, hard to enforce. In namespaces, however, it is the technology that enables the automatic enforcement of such contracts and policies. By threatening to exclude namespace users and service providers that do not adhere to namespace contracts or policies, namespace providers can enforce their interests in an over-efficient manner. The

81. For the specific terms of the privacy policy, see Microsoft Corp., *Microsoft .NET Passport Privacy Statement*, *at* http://www.passport.com/Consumer/PrivacyPolicy.asp?lc=1033 (last modified Aug. 2002).

82. *See infra* text accompanying notes 131–36.

83. In many DRM systems, technology license agreements are used to bind manufacturers of computer electronics and computers (i.e., namespace service providers). Usage contracts are employed to establish a contractual relationship between the DRM provider and individual consumers (i.e., namespace users). For an overview of this contractual protection in DRM systems, see Bechtold, *From Copyright to Information Law*, *supra* note 55, at 217–22, 227.

technical control over a namespace can be used by the namespace provider as leverage for policy and legal control.

This phenomenon occurs in most namespaces. As described above,[84] ICANN allows domain name registries, registrars, and registrants to enter the domain namespace only after they have agreed to certain contractual obligations. ICANN's web of contracts can be enforced by the technical control over the domain namespace, as the contractual quasi-trademark regulation of the UDRP demonstrates. By withdrawing or reassigning a domain name, any decision under the UDRP can be enforced in a very effective and inexpensive manner: through technology.[85]

PKIs are another namespace that uses technology as a governance tool. PKIs enable the secure, convenient, and efficient discovery of public keys in asymmetric encryption systems.[86] PKIs are a cornerstone of contemporary computer security architecture. By resolving public keys to individual persons or corporate entities and vice versa, PKIs create user namespaces. In PKI namespaces, various key revocation mechanisms exist by which compromised public keys can be excluded from further use of the namespace.[87] Technology enables PKIs to control which names exist in their user namespace. In a similar way, eBay reserves the right to suspend any user identifier in its user namespace.[88] DRM systems use various key revocation techniques to achieve the same goal.[89] In general, technology enables the namespace provider to control which names are assigned, modified, and revoked in a namespace. Technology is the most important governance tool in namespaces.

84. *See supra* text accompanying notes 71–75.

85. *See* MUELLER, *supra* note 14, at 191, 232–34. The combination of technological and contractual protection is a common feature in such diverse areas of Internet law as the DNS, DRM, privacy law, the cable open access debate, and hyperlinking. For an attempt to derive some unifying principles from these similarities, see BECHTOLD, VOM URHEBER- ZUM INFORMATIONSRECHT, *supra* note 55, at 439–48; Bechtold, *From Copyright to Information Law*, *supra* note 55, at 230.

86. *See* Radia Perlman, *An Overview of PKI Trust Models,* IEEE NETWORK, Nov.–Dec. 2000, at 38.

87. *See* RUSS HOUSLEY & TIM POLK, PLANNING FOR PKI 107–24 (2001).

88. *See supra* text accompanying note 3.

89. *See* BECHTOLD, VOM URHEBER-ZUM INFORMATIONSRECHT, *supra* note 55, at 26–31; Bechtold, *From Copyright to Information Law*, *supra* note 55, at 215.

B. Governance by Whom?

Namespaces can be created and governed by governments, private entities, or hybrid coalitions. Particularly in namespaces governed by private or hybrid entities, interests of third parties and the general public might become underrepresented. Private regulation of namespaces may clash with public values. Namespaces must be supported by sufficient accountability structures.

The ICANN debate is a prime example of this governance dimension. The extent to which ICANN should exercise control over the domain namespace and what accountability structures are appropriate is fiercely contested in Internet policy circles.[90] ICANN's UDRP has come under criticism for being biased towards the interests of trademark holders.[91] ICANN has been accused of

90. *See* MUELLER, *supra* note 14, at 192; Edward Brunet, *Defending Commerce's Contract Delegation of Power to ICANN*, 6 J. SMALL & EMERGING BUS. L. 1 (2002); Froomkin & Lemley, *supra* note 71, at 19–21; Froomkin, *supra* note 70; Gillian K. Hadfield, *Privatizing Commercial Law: Lessons from ICANN*, 6 J. SMALL & EMERGING BUS. L. 257 (2002); Kesan & Shah, *supra* note 70; Joe Sims & Cynthia L. Bauerly, *A Response to Professor Froomkin: Why ICANN Does Not Violate the APA or the Constitution*, 6 J. SMALL & EMERGING BUS. L. 65 (2002); Jonathan Weinberg, *ICANN and the Problem of Legitimacy*, 50 DUKE L.J. 187 (2000); Jonathan Zittrain, *ICANN: Between the Public and the Private, Comments Before Congress*, 14 BERKELEY TECH. L.J. 1071 (1999); Tamar Frankel, *Accountability and Oversight of the Internet Corporation for Assigned Names and Numbers (ICANN)* (2002), *at* http://www.markle.org/news/ICANN_fin1_9.pdf .

91. *See* Michael Geist, *Fair.com?*: *An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP*, 27 BROOK. J. INT'L L. 903, 936 (2002); Jeffrey P. Leonard, *Domain Name Disputes: An Analysis of the UDRP Resolution Process Thus Far*, 2001 WAKE FOREST INTELL. PROP. L.J. 4, *at* http://www.law.wfu.edu/students/IPLA/sp2001/art04.pdf; Milton Mueller, *Rough Justice: An Analysis of ICANN's Uniform Dispute Resolution Policy*, *at* http://dcc.syr.edu/roughjustice.pdf (2000). *But see* Annette Kur, *UDRP*, *available at* http://www.intellecprop.mpg.de/Online-Publikationen/2002/UDRP-study-final-02.pdf (2002). For general analyses of the UDRP, see A. Michael Froomkin, *ICANN's "Uniform Dispute Resolution Policy": Causes and (Partial) Cures*, 67 BROOKLYN L. REV. 605 (2002) [hereinafter Froomkin, ICANN's "Uniform Dispute Resolution Policy"]; Froomkin, *supra* note 70, at 96–101; Laurence R. Helfer & Graeme B. Dinwoodie, *Designing Non-National Systems: The Case of the Uniform Domain Name Dispute Resolution Policy*, 43 WM. & MARY L. REV. 141 (2001); Elizabeth G. Thornburg, *Fast, Cheap, and Out of Control: Lessons from the ICANN Dispute Resolution Process*, 6 J. SMALL & EMERGING BUS. L. 191 (2002); Luke A. Walker, *ICANN's Uniform Domain Name Dispute Resolution Policy*, 15 BERKELEY

creating a new body of international, but private trademark law that lacks any of the accountability structures under which traditional statutes operate.[92]

The ENUM namespace is another example of the tension between public and private namespace ordering. ENUM is a protocol that aims to create greater convergence of traditional fixed and mobile telecommunication networks with the infrastructure of the public Internet.[93] It basically translates telephone numbers into domain names. If a user types an ENUM number into his mobile device or his computer, it can be used to query the DNS.[94] The DNS

TECH. L.J. 289 (2000); Milton Mueller, *Success by Default: A New Profile of Domain Name Trademark Disputes Under ICANN's UDRP*, *at* http://dcc.syr.edu/markle/markle-report-final.pdf (2002); UDRPinfo.com, *at* http://www.udrpinfo.com (last visited Dec. 16, 2002); UDRPlaw.net, *at* http://www.udrplaw.net (last visited Dec. 16, 2002). For an analysis of the UDRP under antitrust aspects, see Froomkin & Lemley, *supra* note 71, at 50–52.

92. *See* Froomkin, ICANN's "Uniform Dispute Resolution Policy," *supra* note 91, at 612; Thornburg, *supra* note 91, at 208.

93. *See* Craig McTaggart, *E Pluribus ENUM: Unifying International Telecommunications Networks and Governance* 2 (2001), *at* http://www.arxiv.org/ftp/cs/papers/0109/0109091.pdf. It is clear that ENUM is an abbreviation, but it is unclear what this abbreviation stands for. The explanations range from "Electronic NUMbering," "tElephone NUmbering and Mapping," and "E-number" to "E.164 Number Mapping." For an overview of ENUM, see Patrick Faltstrom, *E.164 Number and DNS*, Request for Comments (RFC) 2916 (Sept. 2000), *at* http://www.rfc-editor.org/rfc/rfc2916.txt; Internet Engineering Task Force, Telephone Number Mapping (ENUM) Charter, *at* http://www.ietf.org/html.charters/enum-charter.html (last modified Sept. 9, 2002); Washington Internet Project, DNS: ENUM, *at* http://www.cybertelecom.org/dns/enum.htm (last modified Jan. 7, 2003); International Telecommunication Union, ENUM, *at* http://www.itu.int/osg/spu/infocom/enum (last visited Dec. 16, 2002).

94. ENUM assigns each telephone number a unique domain name. The phone number 1 (555) 497–2815, for example, is translated by ENUM into 5.1.8.2.7.9.4.5.5.5.1.e164.arpa. While no technical necessity exists why ENUM numbers have to be telephone numbers, the Internet Engineering Task Force (IETF) ENUM working group determined that ENUM numbers would equal telephone numbers. *See* Robert Cannon, *ENUM: The Collision of Telephony and DNS Policy* 5, 14–17 (2001), *at* http://papers.ssrn.com/abstract=287492; *see also* Faltstrom, *supra* note 93, § 2; Junseok Hwang et al., *Analyzing ENUM Service and Administration from the Bottom Up: The Addressing System for IP Telephony and Beyond* 3, *at* http://www.arxiv.org/ftp/cs/papers/0109/0109044.pdf (2001) (analyzing possible administrative models of ENUM service and discussing policy related issues stemming from ENUM).

then performs a name lookup and returns personal contact information such as telephone numbers, e-mail addresses, or fax numbers.[95] With ENUM, a user could be assigned one "universal number" under which he then could be reached by any imaginable means of communication—for example, telephone, cell phone, e-mail, fax, WWW pages, voicemail, and instant messaging.[96] With ENUM's interconnection of the domain namespace and the telephone number space, two different regulatory frameworks clash. Traditionally, the Internet has been dominated by light regulation that was often exercised by private entities. On the other hand, the national and international telephone system has always been heavily regulated by public actors, ranging from the U.S. Congress, the Federal Telecommunications Commission, and the North American Numbering Plan Administration[97] to the International Telecommunication Union (ITU). The discussion how the ENUM device namespace should be governed oscillates between these two extremes.[98]

95. *See* Cannon, *supra* note 94, at 4; McTaggart, *supra* note 93, at 5. Therefore, ENUM competes with other discovery services for personal information; one competitor might be Microsoft .NET My Services. *See id.* at 23.

96. *See* Autorité de Régulation des Télécommunications, Principles and Conditions for Implementation of an ENUM Protocol in France 7 (2001), *at* http://www.art-telecom.fr/publications/syntconsenum-ang.doc; Cannon, *supra* note 94, at 2.

97. *See* ELI M. NOAM, INTERCONNECTING THE NETWORK OF NETWORKS 204–05 (2001).

98. Currently, it is planned that the international ENUM database ("Tier 0") will be operated by traditional Internet governance bodies such as RIPE NCC (http://www.ripe.net) in the Netherlands, but administered under the regulatory auspices of the ITU. On the national level ("Tier 1"), ENUM service providers will be selected by national regulatory authorities. *See* Autorité de Régulation des Télécommunications, *supra* note 96, at 12–13; Roy Blane, *Liaison to IETF/ISOC on ENUM*, Request for Comments (RFC) 3026, at 2 (Jan. 2001), *at* http://www.rfc-editor.org/rfc/rfc3026.txt; Cannon, *supra* note 94, at 7–8, 24–26; *The History and Context of Telephone Number Mapping (ENUM) Operational Decisions*, Request for Comments (RFC) 3245, at 7–8 (John C. Klensin ed., Mar. 2002), *at* http://www.rfc-editor.org/rfc/rfc3245.txt [hereinafter RFC 3245]; Hwang et al., *supra* note 94, at 4–5. Due to the involvement of the ITU at Tier 0 and the national governments at Tier 1, ENUM has been criticized as a government-backed monopoly. *See* Cannon, *supra* note 94, at 22.

Whereas the DNS and ENUM device namespaces are governed by hybrid entities, the IP[99] and Ethernet address,[100] Microsoft Passport,[101] P2P,[102] and TCP/UDP port number[103] namespaces are all examples of namespaces that are subject to purely private governance. Bibliographic classification schemes, which are also types of namespaces,[104] are usually sponsored by governments or by private consortiums of interested parties and users.[105] PKI systems are another example of namespaces that cover the whole spectrum—from publicly governed to hybrid and purely privately governed

99. IP addresses are administered by the Internet Assigned Numbers Authority (IANA). Under the auspices of IANA, currently three regional IP registries exist in North America, Europe, and Asia. The regional IP registries coordinate and represent local IP registries that operate usually within particular countries. Internet Service Providers (ISPs) can request IP addresses for their customers from regional registries or from upstream ISPs. *See* Kim Hubbard et al., *Internet Registry IP Allocation Guidelines*, Request for Comments (RFC) 2050, at 4 (Nov. 1996), *at* http://www.rfc-editor.org/rfc/rfc2050.txt. For an explanation of IP addresses, see *infra* text accompanying notes 193–200.

100. The 802 Committee of the Institute of Electrical and Electronics Engineers (IEEE) standardized the Ethernet system. IEEE still controls the Ethernet address space. *See* IEEE Registration Authority, *at* http://standards.ieee.org/regauth (last modified Jan. 7, 2003). For an explanation of Ethernet addresses, see *infra* text accompanying note 201.

101. With Microsoft Passport, the tension between public and private ordering becomes particularly obvious. As Lawrence Lessig wrote on Slashdot: "When we needed a passport system, we didn't tell Chase Manhattan bank [sic] that they could develop the passport system in exchange for a piece of every transaction. . . . [t]here was a recognition of the importance of neutral, commons-like, infrastructures upon which others could build neutrally." Slashdot, Lawrence Lessig Answers Your Questions, at Q 14, *at* http://slashdot.org/article.pl?sid=01/12/21/155221 (posted Dec. 21, 2001).

102. *See infra* text accompanying note 166.

103. *See infra* text accompanying notes 202–04.

104. *See infra* text accompanying note 252.

105. The world's two largest classification schemes, the U.S. Library of Congress Classification (LCC) and the Russian Library-Bibliographical Classification (LBC/BBK), are sponsored by their respective governments. The most popular classification, the Dewey Decimal Classification (DDC) and its offspring, the Universal Decimal Classification (UDC), are sponsored by private entities. *See* Allan Wilson, *The Hierarchy of Belief: Ideological Tendentiousness in Universal Classification*, *in* CLASSIFICATION RESEARCH FOR KNOWLEDGE REPRESENTATION AND ORGANIZATION 389, 393 (Nancy J. Williamson & Michèle Hudon eds., 1992).

namespaces. Who governs a namespace determines, in part, what values and whose interests the namespace protects.

C. Namespace Topology

Topology may be the most important governance dimension in namespaces.[106] In a namespace, system functions can be positioned in a central location or distributed along a vertical or horizontal axis. Choosing a topology along these axes has numerous policy and legal implications, as this Section will illustrate.[107]

1. Vertical distribution of namespaces

Namespace functions can be distributed along a vertical axis in various ways. Whereas a namespace without any such distribution is a "flat" namespace, a namespace with full vertical distribution is a "hierarchical" one (see Figure 2).[108]

106. In general, the study of a network's topology is concerned with the manner in which the network nodes are interconnected. *See* ROSHAN L. SHARMA, NETWORK TOPOLOGY OPTIMIZATION: THE ART AND SCIENCE OF NETWORK DESIGN 8 (1990).

107. Parts of the following analysis build upon the overview of different distributed systems topologies by Nelson Minar, *Distributed Systems Topologies: Part 1* (Dec. 14, 2001), *at* http://www.openp2p.com/pub/a/p2p/2001/12/14/topologies_one.html [hereinafter Minar, *Part 1*]; Nelson Minar, *Distributed Systems Topologies: Part 2* (Jan. 8, 2002), *at* http://www.openp2p.com/pub/a/p2p/2002/01/08/p2p_topologies_pt2.html [hereinafter Minar, *Part 2*]. Minar distinguishes between centralized, ring, hierarchical, decentralized, and hybrid topologies. This categorization reminds one of the different network topologies used in Local Area Networks (LANs): mesh topology, multi-drop topology, directed link topology, star topology, ring topology, and bus topology. *See* DOUGLAS E. COMER, COMPUTER NETWORKS AND INTERNETS 103–05 (3d ed. 2001); SHARMA, *supra* note 106, at 8–13; *see also* PRISCILLA OPPENHEIMER, TOP-DOWN NETWORK DESIGN 121–55 (1999) (discussing techniques to develop a network topology).

108. *See* Shoch, *supra* note 31, at 75–76.

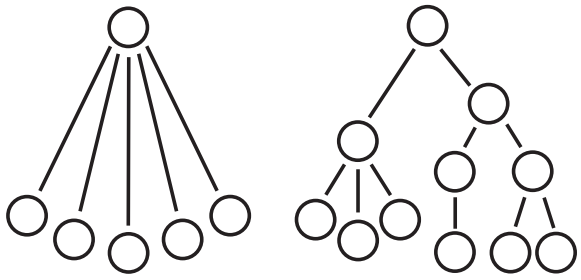

Figure 2: Flat Versus Hierarchical Namespaces[109]

In a flat namespace, a single entity provides the full name service and thereby operates the full namespace. Therefore, a single point of control exists. The namespace provider, the government, or hackers can easily regulate flat namespaces.[110] Flat namespaces also have a single point of knowledge:[111] one database stores the names of all objects as well as their locations and other attributes. If the database misuses this knowledge for data mining and marketing purposes, flat namespaces can pose a privacy risk.

Hierarchical namespaces have different characteristics. In a hierarchical namespace, the name service is distributed over a hierarchy of different entities. Each entity is responsible for a different subset of names. No single entity exercises direct and perfect control over the whole namespace.[112] Rather, different parts of the namespace can be managed by different entities[113] and,

109. This and the following figure were inspired by Nelson Minar. *See* Minar, *Part 1*, *supra* note 107.

110. This point is made in the PKI context by John Marchesini & Sean Smith, *Virtual Hierarchies: An Architecture for Building and Maintaining Efficient and Resilient Trust Chains* 3 (Draft of May 17, 2002), *available at* http://www.cs.dartmouth.edu/~pkilab/papers/vh.pdf.

111. *Cf.* Watson, *supra* note 37, at 207.

112. *See infra* Part IV.B. Nevertheless, even in a hierarchical namespace, the root node at the top of the hierarchy retains important regulatory power over the whole namespace. *See infra* text accompanying notes 295–96 (noting that ICANN's registry regulations and the UDRP can be understood as an attempt of the root node to retain control over the domain namespace).

113. Indeed, that was one of the reasons for introducing the concept of domains on the Internet in 1984. *See* Jon Postel & Joyce Reynolds, *Domain Requirements,* Request for Comments (RFC) 920 (Oct. 1984), *at* http://www.rfc-editor.org/rfc/rfc920.txt.

occasionally, governed by different policies.[114] Hierarchical namespaces therefore enable some competition to occur within the namespace.

The DNS may exemplify this governance dimension. The DNS is not a monolithic system. Rather, it consists of a hierarchically organized network of databases, operated by a network of so-called "registries." Therefore, domain names under the top-level domain (TLD) .de are assigned and administered by a different registry than domain names under the TLD .com. The registries have at least some discretion in the way they assign domain names. Many ccTLD registries, for example, do not impose ICANN's UDRP upon domain name registrars and registrants.[115] To some extent, responsibility for assigning domain names and for maintaining the name service is distributed throughout the hierarchical DNS network.[116] Thereby, the decision as to what policies are appropriate for governing the domain namespace is decentralized as well. This decentralization in deciding policy issues could only be achieved by making a technical decision at the design stage of the DNS—choosing a hierarchical structure as the DNS's topology.

ENUM,[117] IP addresses,[118] and the Library of Congress bibliographic classification are further examples of hierarchical

114. *See, e.g.*, COULOURIS ET AL., *supra* note 33, at 358; ICANN, ICP-3: A Unique, Authoritative Root for the DNS ¶ 1 (July 9, 2001), *at* http://www.icann.org/icp/icp-3.htm (discussing ICANN's commitment to a single public root for the Internet Domain System). For an example of different policies within a hierarchical PKI namespace, see CHARLIE KAUFMAN ET AL., NETWORK SECURITY: PRIVATE COMMUNICATION IN A PUBLIC WORLD 381 (2d ed. 2002); Perlman, *supra* note 86, at 41.

115. *See In re* Toll Free Service Access Codes, 13 F.C.C.R. 9058, 9067 (1998).

116. *See* MUELLER, *supra* note 14, at 6.

117. IETF has proposed to structure the ENUM namespace according to a hierarchical model (so-called "golden tree" architecture). *See* Faltstrom, *supra* note 93, at 4; Anthony Rutkowski, *The ENUM Golden Tree: The Quest for a Universal Communications Identifier*, 3 INFO 97 (Apr. 2001), *available at* http://www.ngi.org/enum/pub/info_rutkowski.pdf. On top of this hierarchy lies the single international database tier 0 that points to the single national databases for each telephone country code, tier 1. For this single database in each country code, different service providers can offer registration services ("tier 2"). *See* Cannon, *supra* note 94, at 7; McTaggart, *supra* note 93, at 8–9; s*ee also supra* text accompanying note 98 (discussing whether ENUM should use a single, coordinated global DNS domain).

namespaces.[119] Conversely, Microoft Passport and TCP/UDP port numbers are flat namespaces. In PKI systems, both flat and hierarchical namespaces exist.[120]

Introducing hierarchical structures into a namespace can enable decentralization and thereby competition within the namespace. However, this is not a necessary consequence. Some hierarchical namespaces are controlled by a single entity at all levels of their hierarchy and therefore do not allow competition between different providers within the namespace.[121] In other namespaces, although different providers exist within the hierarchy, the provider at the top of the hierarchy—the "root"—exercises considerable control over the whole namespace by technological or contractual means. This feature can be found in the domain namespace[122] and in hierarchical PKI user namespaces.[123]

2. Horizontal distribution of namespaces

Besides different vertical distributions, namespace functions can be distributed along a horizontal axis in various ways. Whereas a namespace without any such distribution may be called a "centralized" namespace, a namespace with full horizontal distribution is a "decentralized" one. Between those two extremes

118. The IP address space is administered by a pyramid of authorities, consisting of IANA at the top and regional IP registries at the bottom. Namespace responsibility is distributed across this pyramid. *See* Hubbard et al., *supra* note 99, at 3–4.

119. For an argument against the popular belief that the telephone system is a strictly hierarchical namespace see Rutkowski, *supra* note 117.

120. *See* HOUSLEY & POLK, *supra* note 87, at 54–55; KAUFMAN ET AL., *supra* note 114, at 372; Perlman, *supra* note 86, at 38–42.

121. In the LCC, for example, it is the Library of Congress that exercises all the power in the hierarchical namespace. *See* RITA MARCELLA & ROBERT NEWTON, A NEW MANUAL OF CLASSIFICATION 87 (1994).

122. In the DNS namespace, the entity that controls the so-called "root zone file" could theoretically exclude lower-level registries from the DNS hierarchy. This technical regulatory power enables the entity to impose contractual obligations on lower-level registries. While the hierarchical structure of the domain namespace reduces the dependency of lower hierarchies on the root, its power is still considerably large. For a detailed discussion see MUELLER, *supra* note 14, at 47–56; *see also infra* text accompanying notes 295–96 (discussing how DNS structure leads to decentralization but regulations tend to reverse decentralization).

123. *See* Perlman, *supra* note 86, at 41.

lie various forms of "federated" or interconnected namespaces (see Figure 3).[124] Choosing a namespace topology along the horizontal axis determines its regulability as well as its privacy, liability, and competition implications.

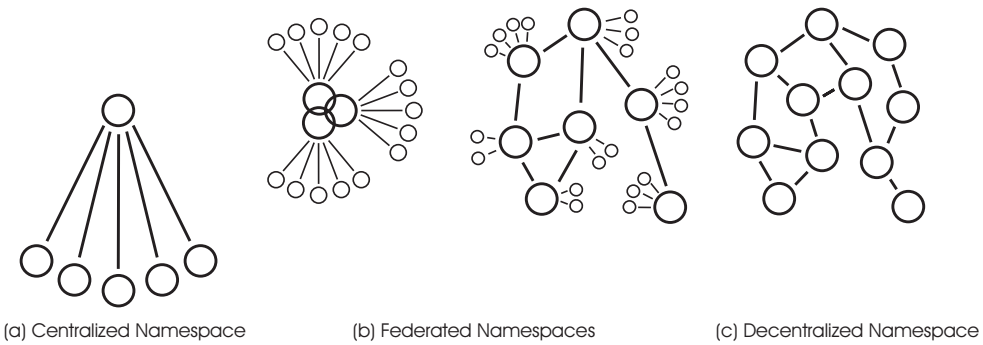

Figure 3: From Centralized to Decentralized Namespaces[125]

a. centralized namespaces

In a centralized namespace, a single entity provides the name service and thereby operates the full namespace.[126]

i. regulability

Centralized namespaces have a single point of control that can be regulated. This is most obvious in centralized P2P systems. P2P systems are networked computer systems in which the significant communication does not take place within a hierarchical system of servers and clients, but within a network of cooperating peers that have similar rights.[127] In a P2P network, files can be shared among

124. Minar, *Part 1*, *supra* note 107; Minar, *Part 2*, *supra* note 107.

125. *See* Minar, *Part 2*, *supra* note 107.

126. *See id.* Therefore, flat and centralized namespaces are essentially the same. While the dichotomy between flat and hierarchical namespaces deals with the vertical distribution of a namespace, the dichotomy between centralized and decentralized namespaces deals with its horizontal distribution. *See id.*

127. *See* Adam Langley, *Freenet*, *in* PEER-TO-PEER (Andy Oram ed., 2001); LESSIG, FUTURE OF IDEAS, *supra* note 14, at 134; *see also* Beverly Yang & Hector Garcia-Molina, *Designing a Super-Peer Network* 1 (2002), *at* http://www-db.stanford.edu/~byang/pubs/superpeer.pdf (discussing P2P

the participating peer computers without any intervention by a centralized server. However, in order to share files, the individual peer must know where files are located in the network. Therefore, P2P networks need a namespace in which each file available in the network is assigned to the address of the peer computer where the file is located.

Early P2P systems used a centralized namespace for locating files in the network. For example, until Napster was shut down by a court order in 2001, it used a centralized namespace located at a server operated by Napster.[128] P2P systems such as Napster have been criticized for facilitating mass-scale piracy. To suppress such piracy, record companies and other copyright holders demanded that Napster be shut down.

In a P2P network with a centralized namespace, shutting down the overall system is a relatively easy task: shutting down the central namespace destroys the whole P2P network because without the namespace a peer computer can no longer locate any file in the P2P network.[129] A centralized namespace opens the system to regulation of various sorts: the government or courts may order that the

networks as spreading costs of sharing data securely among peers in the network). For an overview of the innovation enabled by P2P systems, see LESSIG, FUTURE OF IDEAS, *supra* note 14, at 134–38.

128. *See, e.g.*, Sylvia Ratnasamy et al., *A Scalable Content-Addressable Network*, *available at* http://www.acm.org/sigcomm/sigcomm2001/p13-ratnasamy.pdf (last visited Jan. 17, 2003). In contrast to the original P2P idea, in this type of system some functionality—the name resolution—is centralized. Such systems are sometimes characterized as "hybrid" P2P systems. *See* Yang & Garcia-Molina, *supra* note 127, at 1; *see also* LESSIG, FUTURE OF IDEAS, *supra* note 14, at 135 (discussing Napster and the SETI project).

129. In the Napster case, record companies achieved this result by prompting a court to order Napster to shut down its central namespace. *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1027 (9th Cir. 2001), *aff'd*, 284 F.3d 1091 (9th Cir. 2002). The court required Napster to exclude files from its network that violated the plaintiff's copyrights. *See id.* By exercising control over its central namespace, Napster was able to exclude such files. *See id.* That Napster was in general able to exclude specific files from its P2P network was not a disputed issue during the Napster case. However, it was highly disputed who should bear the burden of identifying the files Napster should exclude, and what level of accuracy the employed filtering technologies needed to have. *See id.* at 1027.

namespace be shut down or the namespace may be shut down by the namespace provider or by hackers.[130]

ii. privacy

A centralized namespace is not only easy to regulate, it may also pose privacy risks. In a centralized namespace all information about the namespace is located within one entity. This entity assigns names so it knows who is accessing the namespace and which names are looked up. During Napster's operation, for example, Napster was in the unique position to know about every download occurring from every computer connected to the Napster network. Such information can be valuable data for surveillance, data mining, marketing, and personalization purposes.

However, centralized namespaces may have ambivalent implications for privacy protection, as the Microsoft Passport user namespace exemplifies. Microsoft Passport is a centralized namespace because Microsoft is currently[131] the only provider of the namespace. User namespaces can theoretically be used to collect large amounts of personal data. Microsoft Passport stores user account names and corresponding passwords in its namespace database. Also, if the user so chooses, it can also store the name of the user, the user's credit card information, address, and demographic or preference data such as gender, occupation, state, ZIP code, time zone, birthday, and language preference.[132] Passport does not transmit such data to participating Web sites without the user's consent.[133] Rather, as a default, Passport only transmits a sixty-four-bit-long unique user identifier.[134]

With this identifier, users can access third-party Web sites—such as eBay or McAfee—without having to provide the Web site with any personal information such as the user's name, e-mail address, or phone number. The only service that possesses such

130. If a hacker succeeds in attacking a central P2P file namespace, the whole P2P network is shut down. *See* Ian Clarke et al., *Protecting Free Expression Online with Freenet*, IEEE INTERNET COMPUTING, Jan.–Feb. 2002, at 40, 44.

131. For announcements of Microsoft to open Passport to competing authentication services, see *infra* note 155.

132. *See* Microsoft Corp., *supra* note 81.

133. *See id.*

134. *See id.*

information is Passport itself.[135] Through the design of Passport's namespace, the storage of private data is therefore centralized. Such namespace design can enhance the privacy of its users in light of the fact that the amount of information a user has to share with a particular Web site to gain access can be decreased.

This is not to say that the user's privacy is perfectly or even adequately protected in Microsoft Passport.[136] If user names, passwords, personal preferences, addresses, and credit card information are all stored at one central location on the Internet, securing this location against malicious attacks and accidental server failures becomes a primary issue. Furthermore, the centralization of information storage may lead to increased privacy risks if the central information storage provider is not trustworthy.

Yet, the Passport example illustrates how different namespace topologies lead to different allocations of privacy risks. Centralized namespaces may protect privacy interests because services that depend on the namespace do not have to store personal information by themselves. However, they may also threaten privacy interests as the central storage may be insecure or the namespace provider itself may misuse the stored information.

iii. liability

In a centralized namespace, knowledge about all issues relating to the namespace is centralized as well. This centralization of knowledge means that, under certain circumstances, the single namespace provider might be held responsible for the activities that

135. *See id.*

136. After a complaint by privacy advocacy groups led by the Electronic Privacy Information Center (EPIC), the Federal Trade Commission conducted an investigation of Microsoft Passport and, in August 2002, proposed a consent order that would prohibit Microsoft from misrepresenting information practices and force the company to implement a comprehensive information security program in Microsoft Passport. *See In re* Microsoft Corp., 2002 WL 1836831 (FTC 2002), *available at* http://www.ftc.gov/opa/2002/08/microsoft.htm. In Europe, after an investigation by the European Union's data protection authorities, Microsoft agreed in January 2003 to substantially modify the information flow in the Passport system. *See Microsoft to Alter Online System to Satisfy Europe*, N.Y. TIMES, Jan. 31, 2003, at W1; Article 29 Data Protection Working Party, Working Document on On-line Authentication Services, *at* http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp68_en.pdf (Jan. 31, 2003).

its users engage in with the names. Doctrines of contributory and vicarious infringement can be used against centralized namespaces. The courts, for example, held Napster responsible for alleged copyright violations of its users because, as a provider of a centralized namespace, Napster had knowledge about every event occurring within the namespace.[137]

iv. competition

Choosing a centralized topology for a namespace also influences the competitive framework in which the namespace operates. Namespaces are subject to network effects.[138] The more users and service providers use a particular namespace, the larger and therefore more valuable the namespace becomes to them.[139] As a result, in communication markets shaped by network effects, the optimal number of namespaces is often one. Network effects can lead to *de*

137. *See A&M Records*, 239 F.3d at 1011.

138. In a market shaped by positive network effects, a consumer's utility of a good "increases with the number of other agents consuming the good." Michael L. Katz & Carl Shapiro, *Network Externalities, Competition, and Compatibility*, 75 AM. ECON. REV. 424, 424 (1985). The existence, importance, and impact of network effects is controversial on a theoretical as well as an empirical level. *See* S. J. Liebowitz & Stephen E. Margolis, *Network Externality: An Uncommon Tragedy*, J. ECON. PERSP., Spring 1994, at 133, 149; *see also* BECHTOLD, VOM URHEBER-ZUM INFORMATIONSRECHT, *supra* note 55, at 351–64; Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CAL. L. REV. 479, 485, 591, 601, 610 (1998) (discussing that because theoretical implications have not been fully developed in economic literature and that the controversy makes it difficult to use network economic effects in legal argument). As Gerald Faulhaber correctly points out, in many communication networks it is the underlying namespace, rather than the network itself, that is subject to network effects. *See* Gerald Faulhaber, *Network Effects and Merger Analysis: Instant Messaging and the AOL-Time Warner Case*, 26 TELECOMM. POL'Y 311, 317 (2002).

139. This increasing utility prompts more and more users and service providers to use the namespace. After passing a certain "tipping" point, such a market shows so-called "positive feedback" effects. Positive feedback effects can lead to a vicious cycle in which a network good absorbs the market share of all competing goods. *See* CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 175–79 (1999); *see also* Lemley & McGowan, *supra* note 138, at 496–97 (noting that "tipping is neither inherently good nor bad.").

facto standards, or even monopolies in a market.[140] In such markets, switching from one namespace to another may involve such high costs for both consumers and producers ("switching costs") that the market is locked into a particular namespace.[141]

Many centralized namespaces are subject to these effects. Network effects are one of the main reasons why no competitor to the ICANN-administered DNS has succeeded in providing universally accessible alternate TLDs.[142] The refusal of AOL to interconnect its instant messaging systems[143] with competing systems can be explained by network effects as well.[144] If, in a market shaped by network effects, a centralized namespace is used, competing namespaces may effectively be driven out of the market.

140. *See* Michael L. Katz & Carl Shapiro, *Systems Competition and Network Effects*, J. ECON. PERSP. 93, 105 (1994).

141. *See* SHAPIRO & VARIAN, *supra* note 139, at 104; *see also* OZ SHY, THE ECONOMICS OF NETWORK INDUSTRIES 4–5 (2001) (outlining various types of switching costs that affect the amount of lock-in).

142. For an overview of the debate on alternate DNS roots, see *infra* note 170.

143. Instant messaging is a service that lets users communicate over the Internet with each other in real time. With its Instant Messaging and ICQ systems, AOL Time Warner is the largest provider of instant messaging systems. *See In re* Matter of Applications for Consent to the Transfer of Control of Licenses and Section 214 Authorizations by Time Warner, Inc. and America Online, Inc., Transferors, to AOL Time Warner, Inc., Transferee, 16 F.C.C.R. 6547, 6606 (2001) [hereinafter AOL/TW Merger Order]. Competitors in real-time communications include Yahoo and Microsoft. Instant messaging systems employ distinct user namespaces—so-called "names and presence databases" (NPDs)—that enable the system to know who is online. *See id.* If an instant messaging provider decides to share access to its NPD with other providers, it makes the instant messaging system interoperable or, in other words, federates the namespace. *See id.* For general information about instant messaging, see Faulhaber, *supra* note 138; *see also* James B. Speta, *A Common Carrier Approach to Internet Interconnection*, 54 FED. COMM. L.J. 225, 235–38 (2002) (discussing the effect of FCC's order in AOL/Time Warner on instant messaging); Weiser, *Internet Governance, supra* note 27, at 842–46 (describing the NPD as the core of instant messaging as well as interconnectability issues).

144. *See* Faulhaber, *supra* note 138, at 315–16, 324.

b. federated namespaces

i. competition

Although network effects can lead to a namespace monopoly, this is not inherently bad from an economic perspective. If, in a particular market, having a single namespace is more efficient than having several competing namespaces, then this is desirable.[145] Having a single namespace does not mean, however, that the namespace should be owned by a single company, or that only one company should provide the whole namespace.[146] Rather, such namespaces can be opened to competitors. Several competitors may offer competing namespace services that all adhere to one common standard. Open standards reduce the lock-in effects produced by network effects.[147] They shift the locus of competition from competing *for* the market to competing *within* the market, using common standards.[148] Such a market structure may combine the best of both worlds—the efficiency gains of one common namespace pushed by network effects, and the efficiency gains of competition between different providers in this namespace.[149]

Centralized namespaces can be opened to competition by introducing interoperability and interconnection between different namespace providers, for example, by "federating" the namespace (see Figure 3). Federating namespaces introduces competition into the namespace market.[150] It frees namespaces from proprietary

145. *See* Lemley & McGowan, *supra* note 138, at 497.
146. *See id.*
147. *See id.* at 516, 600; *see also* MUELLER, *supra* note 14, at 53.
148. *See* SHAPIRO & VARIAN, *supra* note 139, at 231.
149.

> Even if network effects force all consumers to migrate to a single product standard, they (and society) will benefit if numerous companies compete to provide products compatible with that standard. Not only will the price of the product standard fall, and the adoptions of the standard correspondingly rise toward the optimal level, but competition within a standard should spur technological innovation toward improved standard . . . .

Lemley & McGowan, *supra* note 138, at 599–600 (citations omitted).
150. *See* AOL/TW Merger Order, *supra* note 143, ¶ 131.

control. In a federated namespace, functions are horizontally distributed across several providers participating in the federation.[151]

Microsoft Passport may exemplify the difference between a centralized namespace and a federated one. Microsoft formerly structured its Passport namespace as a proprietary service.[152] Passport did not interoperate with other competing identification and authentication services. In such a centralized namespace, technical, economic, and policy control are exercised by a single entity. However, in September 2001, Microsoft announced that it would open Passport to other authentication systems.[153] By "federating" Passport, competing authentication systems could interoperate with Passport. A user with an account at a competing authentication system could still access Web sites that use Passport as their authentication service.[154] Passport would accept the authentication from the competing service and issue a Passport ticket for this user. In other words, Passport would translate the "foreign" identity into a Passport identity.[155] A different proposal for a federated user namespace was made in July 2002 by the Liberty Alliance Project.[156]

151. As a relatively small number of namespace providers exist, federated namespaces are hybrids between fully centralized and fully decentralized namespaces. Their regulatory implications lie between those two extremes as well.

152. *See* Microsoft Corp., .NET Passport Review Guide, *supra* note 77, at 22.

153. *See id.*

154. *See id.*

155. Underlying this new architecture of Passport will be the Kerberos 5.0 security architecture. This technology enables a distributed computer environment in which different users are registered with different authentication servers. In Kerberos 5.0, "cross-realm authentication" allows a user to prove his identity to any authentication server in the system since all authentication servers in the network mutually accept tickets issued by other authentication servers. Under this architecture, Passport would accept Kerberos tickets supplied by other federated authentication services to issue its own authentication ticket. To achieve this "federation of trust," in Kerberos 4.0, every authentication server had to register with every other authentication server. Due to scalability and performance problems, Kerberos 5.0 now supports multi-hop (or transitive) cross-realm authentication, allowing keys to be shared hierarchically. For a detailed overview, see B. Clifford Neuman & Theodore Ts'o, *Kerberos: An Authentication Service for Computer Networks*, IEEE COMM. MAG., Sept. 1994, at 33, 36; *see also* John T. Kohl et al., *The Evolution of the Kerberos Authentication Service*, *in* DISTRIBUTED OPEN SYSTEMS 78 (1994); Ken Hornstein, *Kerberos FAQ, v2.0*, *at*

Further examples for federated namespaces are various PKIs. If, in a PKI system, a single organization is granted a *de facto* monopoly on granting certificates, this organization might charge excessive fees for certificates.[157] Centralized namespaces may stifle competition. Such problems can be prevented by using architectural approaches that enable federated PKI user namespaces. Bridge certification authorities,[158] oligarchy models,[159] "mesh

http://www.cmf.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html (last modified Aug. 18, 2000) (answering frequently asked questions about administrating, using, troubleshooting, and programming Kerberos); Brian Tung, *The Moron's Guide to Kerberos, Version 1.2.2*, *at* http://www.isi.edu/gost/brian/security/kerberos.html (last modified Dec. 16, 1996). For some information on Microsoft's strategy regarding federated identity, see Microsoft Corp., Microsoft's Federated Security and Identity Roadmap, *at* http://msdn.microsoft.com/library/en-us/dnwebsrv/html/wsfederate.asp (June 2002).

156. The Liberty Alliance Project attempts to establish an open standard for federated network identity that could either compete or cooperate with Microsoft Passport. Liberty-enabled networks would enable single sign-on with a choice of identity providers. With the user's consent, his identity with a particular service provider (such as a car rental company) can be linked to (or federated with) his identity stored at an identity provider (such as his bank or an airline). Then, after the identity provider has authenticated the user, he can use Web sites of all federated service providers without having to log in again. *See* Liberty Alliance Project, Liberty Architecture Overview (Version 1.1-05), *at* http://www.projectliberty.org/specs/v1_1draft/draft-liberty-architecture-overview-v1.1-05.pdf (Nov. 25, 2002) [hereinafter Liberty Architecture Overview].

157. *See* Perlman, *supra* note 86, at 39.

158. *See* HOUSLEY & POLK, *supra* note 87, at 64–66; KAUFMAN ET AL., *supra* note 114, at 378; William T. Polk & Nelson E. Hastings, *Bridge Certification Authorities: Connecting B2B Public Key Infrastructures* 8–9 (Sept. 2000), *available at* http://csrc.nist.gov/pki/documents/B2B-article.pdf.

159. In an oligarchy model, it is the user who can select which certification authorities he wants to trust. Thereby, the user can decide which part of the certification namespace he wants to use. Theoretically, this could enable competition between different certification authorities. The oligarchy model is commonly used in WWW browsers in SSL-protected and other secure communication. *See* HOUSLEY & POLK, *supra* note 87, at 55–56; KAUFMAN ET AL., *supra* note 114, at 374; Perlman, *supra* note 86, at 39; Microsoft Corp., Using Digital Certificates, *at* http://www.microsoft.com/windows/ie/using/howto/digitalcert/using.asp (posted Sept. 7, 2001). Interestingly, this is exactly the scenario which the proponents of a single DNS root zone file want to prevent for security and reliability reasons: that the user can decide himself which DNS root servers he wants to use.

architectures,"[160] and various means of cross-certification[161] are different approaches to create one large federated PKI namespace.

The move from centralized to federated namespaces is further exemplified by DNA sequence namespaces.[162] In order to identify DNA sequences in a permanent manner, many biological journals require authors who describe newly discovered sequences to submit the DNA sequence data to a public database as a condition of publication.[163] Formerly, each of these databases used different systems-or namespaces—to address DNA sequences. DNA sequence identification numbers were not consistent across the databases. However, in early 1999, the three major databases in the United States, Europe, and Japan[164] implemented a system that ensures the unique assignment of names across the databases. In other words, the DNA sequence namespace became federated.[165]

160. In a mesh PKI architecture, a web of trust relationships between peer certification authorities is created by cross-certifications between these authorities. *See* HOUSLEY & POLK, *supra* note 87, at 58–60; Marchesini & Smith, *supra* note 110, at 3–4; Polk & Hastings, *supra* note 158, at 5–8.

161. In cross-certification, one certification authority certifies another certification authority. Thereby, both certification namespaces become interconnected. *See* HOUSLEY & POLK, *supra* note 87, at 62–64; KAUFMAN ET AL., *supra* note 114, at 377.

162. For information on DNA sequence databases, see Dennis A. Benson et al., *GenBank*, 30 NUCLEIC ACIDS RES. 17 (2002); Ewan Birney et al., *Databases and Tools for Browsing Genomes*, 3 ANN. REV. GENOMICS & HUM. GENETICS, 2002, at 293.

163. *See* Benson et al., *supra* note 162, at 19.

164. These are GenBank (operated by the U.S. National Center for Biotechnology Information), the EMBL Nucleotide Sequence Database (operated by the European Bioinformatics Institute), and DDBJ (operated by the Center for Information Biology and DNA Data Bank of Japan). *See* Benson et al., *supra* note 162, at 17.

165. For information on the introduction of the "accession.version" system of sequence identifiers that led to a fully federated namespace, see National Center for Biotechnology Information, Sequence Identifiers: A Historical Note, *at* http://www.ncbi.nlm.nih.gov/Sitemap/sequenceIDs.html (revised Jan. 13, 2000); *see also* Dennis A. Benson et al., *GenBank*, 27 NUCLEIC ACIDS RES. 38, 39 (1999) (discussing sequence identifiers and accession numbers); Benson, *supra* note 162, at 19 (discussing how GenBank can assign an accession number to a sequence submission). However, the main reason for introducing this system was not the need to introduce competition among the databases, but to guarantee data consistency among the scientific databases. *See* National Center for Biotechnology Information, *supra*, at 2.

Other examples of federated namespaces include interconnected telephone networks,[166] the Internet,[167] hybrid P2P systems,[168] as well as discussions about interoperable instant messaging systems[169] and root zone level competition in both the DNS[170] and ENUM.[171]

166. Interconnection arrangements and mandates are tools to federate telephone namespaces. *See* NOAM, *supra* note 97 at 204–05; Mark Armstrong, *Network Interconnection in Telecommunications*, 108 ECON. J. 545 (1998).

167. On the Internet, interconnection between different networks is achieved by peering arrangements between backbone providers. *See* Stanley Besen et al., *Advances in Routing Technologies and Internet Peering Agreements*, 91 AM. ECON. REV. PAPERS & PROC. 292 (2001); Jean-Jacques Laffont et al., *Interconnection and Access in Telecom and the Internet: Internet Peering*, 91 AM. ECON. REV. PAPERS & PROC. 287 (2001). For a general analysis of interconnection problems on the Internet, see Speta, *supra* note 143.

168. Hybrid P2P networks use a namespace architecture that lies between the two extremes of a centralized and decentralized namespace. The FastTrack technology on which Grokster and KaZaA as well as the P2P system eDonkey, are based uses such an approach. *See* Beverly Yang & Hector Garcia-Molina, *Comparing Hybrid Peer-to-Peer Systems* 1, *available at* http://www-db.stanford.edu/~byang/pubs/hybridp2p_long.pdf (Sept. 2001) (explaining how hybrid P2P systems lie between pure P2P and client/server architectures); *see also* Kelly Truelove & Andrew Chasin, *Morpheus Out of the Underworld*, *at* http://www.openp2p.com/pub/a/p2p/2001/07/02/morpheus.html (July 2, 2001) (reviewing the origins, architecture, and major features of Morpheus, a network based on Fast Track technology and similar to KaZaA); Complaint for Damages and Injunctive Relief for Copyright Infringement, MGM Studios v. Grokster, Ltd., 2003 WL 186657 at ¶ 45 (C.D. Cal. 2003), *available at* http://www.eff.org/IP/P2P/MGM_v_Grokster/20011002_mgm_v_grokster_complaint.pdf (suit to stop the massive infringement of plaintiffs' copyrighted works on the Internet).

169. As a condition of the merger approval between AOL and Time Warner, the FCC required AOL not to offer any video-based instant messaging systems that are not interoperable (unfederated) with unaffiliated systems. *See* AOL/TW Merger Order, *supra* note 143, ¶ 325; Faulhaber, *supra* note 138, at 325; Speta, *supra* note 143, at 235–38; Weiser, *Internet Governance, supra* note 27, at 842–46. In July 2002, AOL Time Warner announced a shift in its strategy to offer interoperable instant messaging systems. *See* AOL Time Warner, Third Progress Report on Instant Messaging Interoperability, *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-02-1772A2.pdf (July 16, 2002); AOL Time Warner Inc. Submits Third Progress Report on Instant Messaging Interoperability, 17 F.C.C.R. 14263 (2002); 'Technical Challenges' Spike AOL IM Interoperability, *at* http://www.theregister.co.uk/content/6/26347.html (July 24, 2002). Several IETF working groups pursue divergent approaches to set standards for server-to-server instant messaging interoperability. *See* Application Exchange (apex), *at* http://www.ietf.org/html.charters/apex-charter.html (last modified Oct. 12, 2001); Presence and Instant Messaging Protocol (prim), *at*

By creating interconnections between different namespaces, competition between the federated, interoperable namespaces becomes possible. A competing user authentication service, for example, could offer its service under a privacy policy different from Passport's privacy policy. If Microsoft chose to offer Passport only on a high-usage fee basis, or if it tied the Passport service to another product, a competitor could always offer his authentication service under very different terms, but still interoperate with Passport. By federating user namespaces, they are no longer a proprietary tool for data mining, but rather an open authentication platform on which other applications can build.

However, the mere interconnection of different namespaces does not necessarily lead to well-functioning competition between them. Such competition can be hindered by prohibitively high switching costs. If users or participating Web sites are locked into a particular namespace, the possibility to switch to another federated namespace that offers better service under better terms is only a theoretical one.[172] Furthermore, a federated namespace architecture only leads

http://www.ietf.org/html.charters/prim-charter.html (last modified July 31, 2001); SIP for Instant Messaging and Presence Leveraging Extensions (simple), *at* http://www.ietf.org/html.charters/simple-charter.html (last modified Jan. 14, 2003).

170. For an overview, see Kent Crispin, *Alt-Roots, Alt-TLDs*, *at* http://www.icann.org/stockholm/draft-crispin-alt-roots-tlds-00.txt (May 2001); Internet Architecture Board, *IAB Technical Comment on the Unique DNS Root*, Request for Comments (RFC) 2826 (May 2000), *at* http://www.rfc-editor.org/rfc/rfc2826.txt; ICANN, *supra* note 114; Milton Mueller, *Competing DNS Roots: Creative Destruction or Just Plain Destruction?*, *available at* http://www.arxiv.org/ftp/cs/papers/0109/0109021.pdf (Oct. 2001). For the history of this debate, see MUELLER, *supra* note 14, at 130–34, 148–49, 152–53.

171. *See* Cannon, *supra* note 94, at 17–19. *But see* RFC 3245, *supra* note 98, at 2–3; McTaggart, *supra* note 93, at 10–14 (discussing "unofficial" ENUM namespaces). For an overview of different architectural alternatives for ENUM's design, see Hwang et al., *supra* note 94, at 13–21.

172. A user of one federated namespace may have invested considerable time and effort in shaping his identity in this namespace (by supplying additional personal information such as his address, taste, preferences, etc.). If he would switch to a competing user namespace, he could lose all of this information attached to his old identity, even though both namespaces are federated. This may deter the user from switching authentication systems in the first place, thereby impeding competition among authentication systems in the federation.

to competition if the providers actually do open their namespaces to competitors.[173]

ii. regulability

Federating namespaces prevents any single company from controlling the whole user namespace. Federated namespaces are therefore harder to regulate as no single point of control exists. For example, in a P2P system with such a namespace architecture,[174] shutting down any single namespace will not shut down the whole P2P system. Therefore, such systems promise to combine the advantages of both centralized and decentralized namespace architecture, particularly the efficiency of centralized namespaces

It is interesting to note that in other networks, such problems have been solved at a technical level. Under the U.S. Telecommunications Act of 1996, the FCC requires local exchange carriers to provide "local number portability," thereby allowing consumers to retain their telephone number when switching local telephone providers. *See* 47 U.S.C. § 251(b)(2) (2001); *In re* Telephone Number Portability, 11 F.C.C.R. 8352 (1996). Local number portability reduces customer's switching costs and facilitates competition between local telephone providers. *See* Thomas H. Reinke, *Local Number Portability and Local Loop Competition*, 22 TELECOMM. POL'Y 73 (1998); Joshua S. Gans et al., *Numbers to the People: Regulation, Ownership and Local Number Portability*, *at* http://papers.ssrn.com/abstract=223189 (Apr. 13, 2000); Justus Haucap, *Telephone Number Allocation: A Property Rights Approach*, *available at* http://papers.ssrn.com/sol3/delivery.cfm/SSRN_ID308003_code020423670.pdf?abstractid=308003 (Mar. 2002). *But see* NOAM, *supra* note 97, at 206–09; Reiko Aoki & John Small, *The Economics of Number Portability: Switching Costs and Two-Part Tariffs*, *available at* http://www.crnec.auckland.ac.nz/research/papers/Aoki_Small.pdf (Nov. 1999).

173. Microsoft, for example, has announced that it will open Passport only to other authentication systems that "meet the same high bar on privacy that we've set for Microsoft's own Passport service." Q&A: Open Passport Enables a "Network of Trust," *at* http://www.microsoft.com/presspass/Features/2001/Sep01/09-20passport.asp (Sept. 20, 2001). If the authentication system does not adhere to or enforce a comparable privacy policy, Microsoft could cut the connection between both authentication systems. *See id.* While this may be a laudable procedure, it is important to note that, in a federated authentication architecture, no structural reason exists why authentication providers could not also cut off competing systems for less laudable, strategic reasons. A similar point is made in the PKI context by Polk & Hastings, *supra* note 158, at 5. For an analysis of the legal consequences in the PKI context, see Michael S. Baum & Warwick Ford, *Public Key Infrastructure Interoperation*, 38 JURIMETRICS J. 359 (1998).

174. *See supra* note 168 and accompanying text.

with the robustness and lack of a single point of failure of decentralized namespaces.[175]

iii. privacy

The partial decentralization in federated namespaces can enhance the protection of privacy interests. In a centralized user namespace, such as the Microsoft Passport architecture, each user is assigned a globally unique ID. Globally unique IDs always pose privacy risks as they can easily be used to connect personal information gathered from various sources.

In the federated user namespace of the Liberty Alliance Project,[176] globally unique IDs that are tied to a particular identity provider do not exist.[177] Rather, users have different accounts with one or more identity providers as well as with numerous service providers. With the consent of the user, all or some of the user's identities can be linked together.[178] However, even if two identities are linked together, no common identity exists. Both services remember the other's handle for the user and communicate with each other only with these handles.[179] This architecture enables the user to decide in a very fine-grained way which identities become linked together and which should stay separate. Therefore, the user can control which providers can exchange personal information.[180]

Federated user namespaces can be designed in different ways. One alternative approach would be to federate all namespaces in

175. *See* Yang & Garcia-Molina, *supra* note 127, at 1–3.

176. *See* Liberty Architecture Overview, *supra* note 156.

177. *See id.* at 24–25, 29.

178. Identities can also be linked together in a chain. In such a case, providers cannot skip over each other in the trust chain. *See id.* at 25.

179. *See* Liberty Alliance Project, Liberty Protocols and Schemas Specification (Draft Version 1.1-07) 23, *at* http://www.projectliberty.org/specs/v1_1draft/draft-liberty-architecture-protocols-and-schemas-v1.1-07.pdf (Nov. 15, 2002) [hereinafter Liberty Protocols].

180. If, for example, a user has federated each of his identities at two different service providers with his one identity at an identity provider, the service providers are still unable to exchange information about him because the user has not created a federation between the two service provider identities. *See* Liberty Architecture Overview, *supra* note 156, at 26–27, 29. For a general account of the importance of modularity in system design, see CARLISS Y. BALDWIN & KIM B. CLARK, DESIGN RULES (2000).

their entirety by default. Such architecture would in fact create an ID that is unique and recognized by all namespaces in the federation. This would facilitate the exchange of personal information that is tied to the globally unique ID across namespace borders. However, the Liberty Alliance Project chose a different approach. By empowering the user to determine to what extent his identity is federated in the user namespace, the Liberty Alliance Project allows the user to control the dissemination of personal information across the namespace in a fine-grained way.[181] Federating namespaces can enhance privacy protection as the overall namespace is effectively modularized.

c. decentralized namespaces

While in a federated namespace a small number of interconnected namespaces exist, in a fully decentralized namespace the namespace itself is fully scattered across the network. Decentralized P2P networks are prime examples of such namespaces. In a fully decentralized P2P system, no single namespace exists. Rather, each peer has a namespace in which all locally stored files are registered.[182] In such networks the namespace is dispersed across the network beyond recognition. Resolving a name means searching the whole network or at least significant parts of it.[183] The P2P system Gnutella[184] uses such architecture.[185] Other

181. *See supra* text accompanying note 178.

182. Arguably, the individual peers do not even need a distinct namespace as they can just search their hard drive.

183. In fact, it is one of the most important research areas in P2P computing to develop efficient search algorithms for large distributed, decentralized systems. It is interesting to note that people use strikingly similar strategies to locate other individuals in a society (or, more precisely, the namespace of personal names in a society). In an experiment conducted in the late 1960s, randomly selected individuals were asked to direct letters to a target person in another, distant city in the United States whom they did not know by forwarding the letter to a single friend. On average, the letters that arrived at the target person made only six hops. *See* Jeffrey Travers & Stanley Milgram, *An Experimental Study of the Small World Problem*, 32 SOCIOMETRY 425 (1969). The search strategy employed by individuals in the namespace of personal names can be used in other decentralized namespaces, such as P2P systems, as well. *See* Duncan J. Watts et al., *Identity and Search in Social Networks*, 296 SCIENCE 1302, 1305 (2002).

184. *See* Gene Kan, *Gnutella*, *in* PEER-TO-PEER 94 (Andy Oram ed., 2001); Matei Ripeanu et al., *Mapping the Gnutella Network,* IEEE INTERNET

decentralized namespaces include encryption systems—such as the original Pretty Good Privacy (PGP) system—that do not employ a structured PKI architecture, but rather a more anarchical model in which public keys are certified on a P2P basis.[186] Decentralized namespaces possess interesting features regarding their regulability, privacy protection, and the liability of the namespace "providers."

i. regulability

If copyright holders want to shut down a fully decentralized P2P network, they cannot simply shut down a central namespace because the namespace is scattered across the individual peers of the P2P network. Shutting down any one of the peers in the network would not impact the overall network. As no single entity assigns all names, no single point of control exists. Fully decentralized namespaces are much harder to regulate than centralized namespaces.

ii. liability and privacy

As no single entity exists that operates the namespace, liability for actions occurring within the namespace is scattered as well.[187] Only individual users can be held liable, since no central entities exist.

COMPUTING, Jan./Feb. 2002, at 50; Clip2, The Gnutella Protocol Specification v0.4: Document Revision 1.2, *at* http://rfc-gnutella.sourceforge.net/Development/GnutellaProtocol0_4-rev1_2.pdf (last visited Feb. 4, 2003); Gnutelliums, *at* http://www.gnutelliums.com (last visited Jan. 16, 2003).

185. For efficiency and scalability reasons, Gnutella limits the hops a query message may take across peer computers by a "time-to-live" (TTL) parameter. *See* Kan, *supra* note 184, at 105–06, 110; *see also* Fernando R.A. Bordignon & Gabriel H. Tolosa, *Gnutella: Distributed System for Information Storage and Searching Model Description* 5, *at* http://www.unlu.edu.ar/~tyr/TYR-publica/paper-final-gnutella-english-v2.pdf (2001) (explaining the process by which a query message is rejected).

186. In such a system, no trusted certification authority certifies the identity or integrity of any public key or individual person. Rather, the individuals themselves decide which keys to trust. Thereby, a "web of trust" is created without the need for a central infrastructure. In such a system, the authentication namespace is totally dispersed throughout the whole network. *See* KAUFMAN ET AL., *supra* note 114, at 569; Perlman, *supra* note 86, at 40.

187. *See* LESSIG, FUTURE OF IDEAS, *supra* note 14, at 137; Kan, *supra* note 184, at 99.

In a fully decentralized namespace, knowledge for actions occurring on top of the namespace is dispersed throughout the network. In a decentralized P2P network, for instance, no central entity exists that knows all the transactions occurring in the network.[188] Some of these networks, such as Freenet, are even designed with the explicit purpose of preserving privacy for information producers and consumers while resisting censorship.[189] Surveillance of fully decentralized namespaces is an intricate task.[190] Decentralized namespaces lead to decentralized knowledge which protects the privacy of namespace users better than centralized namespaces.

As this Section has shown, choosing a topology for namespaces has far-reaching implications from a policy and legal perspective. The more decentralized a namespace becomes, the harder it becomes to regulate. The more it protects privacy and anonymity of its users, the more difficult, more expensive and more inefficient it becomes to hold someone liable for the actions occurring on top of the namespace, and the more competition it enables within the namespace.

D. Intensity of Namespace Governance

Namespaces can be governed with various intensities. Whether a namespace is tightly controlled or merely left to its own impacts various policy aspects of namespace governance, ranging from regulability to innovation issues.

188. *See* Kan, *supra* note 184, at 119 ("With Gnutella, every router and cable on the Internet would need to be tapped to learn about transactions between Gnutella hosts or peers.").

189. *See* Ian Clarke et al., *Freenet: A Distributed Anonymous Information Storage and Retrieval System*, *in* DESIGNING PRIVACY ENHANCING TECHNOLOGIES 46, 47, 62–64 (Hannes Federrath ed., 2001); Adam Langley, *Freenet*, *in* PEER-TO-PEER 123 (Andy Oram ed., 2001); Clarke et al., *supra* note 130, at 41. For other P2P systems that attempt to preserve anonymity, see Qin Lv et al., *Can Heterogenity Make Gnutella Scalable?*, *at* http://www.cs.rice.edu/Conferences/IPTPS02/165.pdf (2002); Andrei Serjantov, *Anonymizing Censorship Resistant Systems*, *available at* http://www.cs.rice.edu/Conferences/IPTPS02/120.pdf (Mar. 1, 2002).

190. *See* Kan, *supra* note 184, at 118 ("[T]he only way to monitor what is happening on the Gnutella network is to monitor what is happening on the entire Internet.").

1. Control versus coordination

Some namespaces are tightly controlled and coordinated. Some namespaces are coordinated, but not controlled. Other namespaces are neither controlled nor coordinated. In various namespaces, some control or coordination is necessary due to technical reasons. If a namespace, for example, provides fewer names than needed—for example, if it is a scarce namespace[191]—coordination mechanisms must exist to assign names in an efficient and resource-saving manner.[192] Therefore, in a scarce namespace some coordination is necessary. Coordination, however, is not the same as tight control. Coordination in scarce namespaces is specifically focused on dealing with one *technical* feature of the namespace, namely scarcity. If namespaces are subject to greater control, this control is exercised for policy or legal reasons—not technical reasons.

A namespace that illustrates the difference in degree between control and coordination is the IP address space. As described above,[193] the DNS resolves domain names into IP addresses. IP addresses form a distinct namespace that is administered by IANA.[194] Traditionally, IP addresses have been assigned entirely on

191. The telephone number space is a scarce namespace. Although only five percent of the 6.4 billion telephone numbers supported by the U.S. numbering plan had been assigned in the mid-90s, the telephone number space was already in danger of becoming exhausted. *See* MUELLER, *supra* note 14, at 20. A similar problem occurs in the IP address space. To remove the artificial size limitation of the current IPv4 address space, IPv6, the next generation of a core protocol underlying Internet communications, will expand the size of the IP address space from thirty-two bits to 128 bits. *See id.* at 38–39. Scarcity also exists in the namespace of gTLDs. The current ICANN-administered DNS recognizes only a limited number of gTLDs (.com, .net, .org, .aero, .biz, .coop, .info, .museum, .name, and .pro). *See id.* at 201–05. For other scarce namespaces, see *infra* text accompanying notes 248–49.

192. Various ways exist to allocate scarce namespaces. Names can be assigned on a first-come, first-served basis (assignment based on priority), auctioned or traded as a regular good (assignment based on market forces), assigned based on administrative rules or "beauty contests" (assignment based on administrative decisions), or they can be randomly assigned (assignment based on chance). Legal constraints can influence the assignment process as well (e.g., trademark law or dispute resolution policies). Some of these assignment procedures work better in some namespaces than in others. *See* MUELLER, *supra* note 14, at 23–26.

193. *See supra* text accompanying notes 37–40.

194. Hubbard et al., *supra* note 99, at 2–3. IANA's Web site can be found at http://www.iana.org (last modified Dec. 30, 2002).

a first-come, first-served basis.[195] Although IANA coordinated the IP address space, it exercised almost no policy control over the address space. In the early 1990s, however, it became evident that the IP address space would be used up in a few years.[196] The IP address space turned out to be a scarce resource. To cope with this scarcity, IP address registries began to impose policies that assigned IP addresses based on demonstrated need and made them subject to annual fees.[197] Thereby, the registries attempted to prevent the stockpiling of IP addresses and to conserve the current address space as long as possible.[198] The registries increasingly used their technical control over the IP address space to facilitate rationing and policy enforcement.[199] However, apart from this scarcity problem, the IP address assignment process is still restricted to mere coordination tasks. The IP address registries do not exercise any control over any other policy issues that would be worth mentioning.[200] Developments with respect to Ethernet addresses are similar.[201]

195. *See* MUELLER, *supra* note 14, at 36.

196. The scarcity of the IPv4 address space is not a result of the actual size of the address space. The address space theoretically supports about 4.3 billion unique addresses. However, special addressing and routing schemes led to the scarcity of the address space even though only a small fraction of the address space was actually used. *See id.*

197. It was even discussed whether IP address blocks should be auctioned or traded in a market. *See id.* at 37.

198. *See* Hubbard et al., *supra* note 99, at 3–8. The more restrictive assignment of IP addresses is not the only way to cope with the scarce address space. *See* MUELLER, *supra* note 14, at 36–39. One relief was the introduction of more new routing algorithms (classless inter-domain routing) that used up fewer IP addresses. *See id.* at 37–38. Another solution is the expansion of the IP address space, a goal pursued by IPv6. *See id.* at 37–39; *see also supra* note 185 (describing the P2P system Gnutella).

199. *See id.* at 36–38. For an overview of the IPv6 address assignment policy, see ICANN, IPv6 Address Allocation and Assignment Policy, *at* http://www.icann.org/aso/ipv6-statement-11jul02.htm (posted June 26, 2002).

200. *See* MUELLER, *supra* note 14, at 32–39; Hubbard et al., *supra* note 99. Besides the scarcity constraint, the assignment of IP addresses also needs to take the Internet routing architecture into account. *See* MUELLER, *supra* note 14, at 33–35.

201. Ethernet addresses—officially called Ethernet Unique Identifiers (EUI)—are administered by the IEEE Registration Authority. *See* IEEE Registration Authority Overview, *supra* note 100. Ethernet addresses used to be forty-eight bits long. *See* MUELLER, *supra* note 14, at 28. As with IP addresses, the Ethernet address space gradually became a scarce resource.

If one compares the regulatory philosophy governing the IP and Ethernet address spaces with the current regulatory philosophy governing the domain namespace, the difference in degree between control and coordination becomes obvious. Name scarcity may necessitate a coordination of the name assignment process. It does not, however, necessitate any tight control over other policy-related issues of the namespace.

2. Control versus uncoordination and decentralized innovation

A central authority would not have to assign names if the sheer size of the namespace can solve coordination problems. Therefore, in some infinite namespaces, even any coordination is unnecessary. Such namespaces are fully "democratized." No entity in the namespace has more knowledge, control, or responsibility over the namespace than any other entity in the namespace. Such namespaces create open platforms that enable decentralized, uncoordinated innovation.

This governance implication of creating infinite namespaces can be best observed in the TCP/UDP port number space. The Internet enables different applications—a Web browser and a Web server, for example—to communicate over the network. To facilitate the communication among a wide variety of applications, a standardized mechanism has to exist so that applications can contact and communicate with remote applications. The TCP and UDP port number space provides such a standardized mechanism.[202] They are namespaces for identifying "channels" over which programs can

Therefore, the IEEE Registration Authority responded by imposing address space conversation policies. *See id.* at 28. Apart from measures to preserve the address space, the IEEE Registration Authority exercises no considerable policy control over the Ethernet address space. *See id.* at 27–28. Furthermore, to alleviate the scarcity problem, the Ethernet address space was enlarged to support sixty-four-bit-long addresses. *See id.* at 28.

202. While the following description generally applies to both TCP and UDP port numbers, for purposes of clarity, only TCP port numbers will be mentioned. The UDP is a connectionless transport layer protocol which uses port numbers just as the TCP does. *See* ERIC A. HALL, INTERNET CORE PROTOCOLS: THE DEFINITIVE GUIDE 24–25 (2000). While there are important technical differences between UDP and TCP, they are of no importance for this Article and are therefore not addressed. *See id.* For a more detailed description, see PETE LOSHIN, TCP/IP CLEARLY EXPLAINED 181–210 (3d ed. 1999).

communicate on the Internet. In combination with the IP address of a computer, port numbers uniquely identify every program running on any computer connected to the Internet.[203] Therefore, port numbers provide a service to the namespace that identifies applications running on networked computers.[204]

In total, 65,535 distinct port numbers exist. It would be quite cumbersome if, each time a Web browser wanted to communicate with a Web server, both programs had to agree on which port to use. Therefore, the network provides an *ex ante*, standardized agreement about which programs can be contacted on which ports: IANA maintains a list of TCP ports that are pre-assigned to specific programs or processes.[205] According to this list, Web servers can be contacted on port eighty. This means that a Web browser can simply contact a remote computer on port eighty. If a Web server is running on the remote computer, it will most likely listen to and respond on port eighty.

Port eighty is not the only "standardized" port. In fact, the first 1024 of the 65,535 ports are all so-called "well-known ports" which are assigned to processes that are used widely across the Internet.[206] Port numbers in the range from 1024 to 49,151 are called "registered ports."[207] They are assigned to less common programs and are

203. In the TCP port number space, this combination with IP addresses is called a "socket." *See* CRAIG HUNT, TCP/IP NETWORK ADMINISTRATION 46 (2d ed. 1998); LOSHIN, *supra* note 202, at 184–85 (Loshin also provides an explanation of server daemons which complicates this description slightly).

204. *See* HALL, *supra* note 202, at 274–86.

205. The list is available at http://www.iana.org/assignments/port-numbers (last updated Jan. 17, 2003). This site lists ports for both the UDP and the TCP protocol. From 1977 until 1994, the list was contained in a series of RFCs, the most current being RFC 1700. In January 2002, however, it was officially acknowledged that RFC 1700 was outdated and that IANA's Web site should be consulted instead. *See Assigned Numbers: RFC 1700 is Replaced by an On-line Database*, Request for Comments (RFC) 3232 (Joyce K. Reynolds, ed., 2002), *at* http://www.rfc-editor.org/rfc/rfc3232.txt. A copy of the list, for example, is stored on most computers connected to the Internet (e.g., "/etc/services" on UNIX systems) in whole or in part. *See* HUNT, *supra* note 203, at 43–44.

206. FTP (port 21), SSH (22), Telnet (23), SMTP (25), Domain Name Service (53), Finger (79), Kerberos (88), NNTP (119), IRC (194), Z39.50 (210), LDAP (389), and HTTPS (443) all are examples of widely used processes that have been assigned a "well-known" port number. *See* IANA, Port Numbers, *at* http://www.iana.org/assignments/port-numbers.

207. *Id.*

included in IANA's list of port numbers "as a convenience to the community."[208] While IANA exercises some control over the assignment of ports zero through 49,151,[209] the ports 49,152 through 65,535 are totally unassigned ("private ports"). Everybody is free to use them. Every application that wants to communicate with another application running on a remote computer can do so by simply using one of the private ports.

Therefore, twenty-five percent of the TCP port number space is not only uncontrolled, but also uncoordinated. Such regulation of the number space has advantages and disadvantages. A disadvantage of an uncoordinated port number space is the potential for a chaotic communication bazaar. An uncoordinated port number space does not prevent different applications from using the same port number.[210] However, the advantages of such number space regulation far outweigh this potential disadvantage. Leaving the port number space open arguably played a major role in fostering innovation on the Internet. To realize how this value is embedded in the port number space, one needs to imagine a different design. First, imagine that IANA assigned every port number to specific programs so that no private ports existed. Second, imagine that IANA assigned port numbers only according to a set of predetermined rules. It could assign ports on the basis of the technical quality of the application. It could auction ports or charge an administrative fee for assignment. It could choose to assign no

208. *Id.*

209. IANA's assignment of these lower port numbers follows the traditional approach of the technical Internet community: it is a very open process. Anybody who wants to receive a well-known or a registered port is free to apply. While IANA controls this part of the port number space, it does not discriminate between different applications. For more information, see IANA, Application for System (Well-Known) Port Number (Nov. 21, 2000), *at* http://www.iana.org/cgi-bin/sys-port-number.pl; IANA, Application for User (Registered) Port Number, *at* http://www.iana.org/cgi-bin/usr-port-number.pl (last updated Nov. 21, 2000).

210. If, for example, an instant messaging application tries to communicate with a remote instant messaging application on a port that is used simultaneously by a P2P application, the communication is likely to fail. In practice, however, this is not too severe a problem if the uncoordinated part of the number space is sufficiently large (16,383 port numbers). The chance that an application will connect to a computer on a port number to which a totally different application is listening is therefore relatively slim. Even if this happens, the application can simply switch to another of the private channels.

ports to P2P applications due to piracy concerns. It could choose to assign no ports to video streaming software because it did not want the Internet to become a competitor of cable TV. It could choose to assign only ports to applications that run on the Windows operating system. Fortunately, it is unrealistic that IANA would ever assign port numbers based on such criteria. Third, however, the scenario becomes more plausible if one imagines that it was not IANA that assigned the port numbers, but a company such as AT&T or Microsoft. In such a scenario, the control over the port number space could be used to allow the operation of certain kinds of applications on the Internet while shutting down other applications.[211]

211. This scenario may seem far-fetched. However, in other communication networks, this application discrimination is already happening. Over the last few years, several broadband cable providers that offer Internet access over their cable networks have restricted the kind of applications that can be run on the network. Proponents of a cable "open access" regime argue that this regulation impedes innovation occurring on the network. For an overview of this discussion, see Lemley & Lessig, *supra* note 25.

Even in the TCP/UDP port number space, the emergence of control structures can be observed. For a variety of reasons, technologies have been developed that enable several computers to share a single IP address. This is achieved by network address translators (NATs) which pick up all traffic coming to the group of computers sharing one IP address and distribute it to the appropriate computer in the group. They perform an equivalent procedure for outgoing traffic.

Most NATs also alter port numbers. These Network Address Port Translators (NAPTs) can exercise control over the data flow. As Lawrence Lessig explains, "[i]f the [NAPT] is unaware of how to process the data from that particular application (either because the [NAPT] was unaware of that application or because it was coded to ignore data of that type), then that application won't function on that [NAPT]-empowered network." *See* LESSIG, FUTURE OF IDEAS, *supra* note 14, at 172; *see also* Hans Kruse et al., *The InterNAT: Policy Implications of the Internet Architecture Debate*, *in* COMMUNICATIONS POLICY IN TRANSITION: THE INTERNET AND BEYOND 141 (Benjamin M. Compaine & Shane Greenstein eds., 2001) (stating that NAPTs are unable to "forward a connection request from the Internet to a private network unless an administrative mapping has been provided for the port requested in the incoming packet.").

NAPTs introduce a control structure into the port number space. This point of control can be used as a leverage to impede innovation on the network. For an overview of NAT and NAPT technology, see Pyda Srisuresh & Matt Holdrege, *IP Network Address Translator (NAT) Terminology and Considerations*, Request for Comments (RFC) 2663 (Aug. 1999), *at* http://www.rfc-editor.org/rfc/rfc2663.txt; Pyda Srisuresh & Kjeld B. Egevang, *Traditional IP Network Address Translator (Traditional NAT)*, Request for

By keeping twenty-five percent of the port number space open and uncoordinated, IANA has chosen a different path. It coordinates parts of the number space without controlling the whole number space. It cannot prevent anyone from writing an application that operates over the Internet using a private port. This particular regulation of the port number space plays a large role in the phenomenal innovation occurring on the Internet. Since nobody exercises control over the port number space, everybody is free to invent new technologies running atop of the Internet without having to ask anyone for permission. When Tim Berners-Lee invented the Hypertext Transfer Protocol (HTTP), one of the technologies underlying the World Wide Web, he did not have to ask the AT&Ts or Microsofts of this world for permission to use a port number. The port number space was a free resource.

The observation that certain design choices in the Internet architecture foster innovation occurring on the Internet is not novel. Indeed, it lies at the heart of the so-called "end-to-end argument" (e2e). E2e is one of the prime architectural principles that have governed the Internet over the last decades.[212] First described by Saltzer, Reed, and Clark in a seminal paper dating from 1984,[213] the

Comments (RFC) 3022 (Jan. 2001), *at* http://www.rfc-editor.org/rfc/rfc3022.txt. For an overview of the architectural implications of NATs, see Tony Hain, *Architectural Implications of NAT*, Request for Comments (RFC) 2993 (Nov. 2000), *at* http://www.rfc-editor.org/rfc/rfc2993.txt. For an explanation of the related concept of "Realm Specific IP" (RSIP), particularly Realm Specific Address and Port IP (RSAP-IP), see Srisuresh & Holdrege, *supra*, at 15–20.

212. "[T]he [Internet] community believes that the goal [of the Internet architecture] is connectivity, the tool is the Internet Protocol, and the intelligence is end to end rather than hidden in the network." *Architectural Principles of the Internet*, Request for Comments (RFC) 1958 (Brian E. Carpenter ed., June 1996), *at* http://www.rfc-editor.org/rfc/rfc1958.txt [hereinafter RFC 1958]; *see also* Marjory S. Blumenthal & David D. Clark, *Rethinking the Design of the Internet: The End-to-End Arguments vs. the Brave New World*, 1 ACM TRANSACTIONS ON INTERNET TECHNOLOGY 70, 71–72 (2001) ("[T]he bias toward movement of function 'up' from the core and 'out' to the edge node has served very well as a central Internet design principle.").

213. *See* Jerome H. Saltzer et al., *End-to-End Arguments in System Design*, 2 ACM TRANSACTIONS ON COMPUTER SYSTEMS 277–88 (1984). For an overview of e2e, see RFC 1958, *supra* note 212, at 2. For an analysis of the challenges to the e2e design principle posed by new technologies and new demands, see Blumenthal & Clark, *supra* note 212, at 71–80; *see also* Brian E.

e2e argument claims that as much intelligence as possible should reside at the "edges" of the network, that is, at applications running on networked computers, not in the network itself.[214] It vests power in end users and disables control by a central actor within the network.[215] E2e thereby ensures that the network is a neutral platform that does not discriminate between different applications or services.[216]

Concerning innovation,[217] e2e implies that "innovators with new applications need only connect their computers to the network to let their applications run."[218] They do not have to ask anyone for permission, especially not anyone controlling a namespace upon which the Internet depends. By decentralizing control, e2e enables decentralized innovation.[219]

E2e does not only decentralize control. It is also an architectural principle of how to design a computer network system under uncertainty—uncertainty concerning how the network will be used in the future, and uncertainty as to what kind of applications will be run

Carpenter & Scott W. Brim, *Middleboxes: Taxonomy and Issues*, Request for Comments (RFC) 3234 (Feb. 2002), *at* http://www.rfc-editor.org/rfc/rfc3234.txt.

214. *See* LESSIG, FUTURE OF IDEAS, *supra* note 14, at 34–39; Blumenthal & Clark, *supra* note 212, at 71; Lemley & Lessig, *supra* note 25, at 930–31; Saltzer et. al., *supra* note 213, at 286. In its purest form, the e2e argument deals with the placement of functions within a layered system. It states that most system functions should be located at upper rather than lower levels of a layered system. Functions should be moved upward, "closer to the application that uses the function[s]." Saltzer et al., *supra* note 213, at 277; *see also* Blumenthal & Clark, *supra* note 212, at 71 ("specific application-level functions usually cannot, and preferably should not, be built into the lower levels of the system"); David P. Reed et al., *Commentaries on "Active Networking and End-to-End Arguments"*, IEEE NETWORK 69 (1998) (discussing programmability's effect on design time function placement).

215. *See* Kruse et al., *supra* note 211, at 150.

216. *See* LESSIG, FUTURE OF IDEAS, *supra* note 14, at 37; Lemley & Lessig, *supra* note 25, at 931.

217. The e2e argument also has many implications for the security, integrity, performance, and other aspects of communication. In fact, e2e should be regarded as an umbrella for different, but related system design principles. *See* Saltzer et al., *supra* note 213; Brian E. Carpenter, *Internet Transparency*, Request for Comments (RFC) 2775 (Feb. 2000), *at* http://www.rfc-editor.org/rfc/rfc2775.txt.

218. LESSIG, FUTURE OF IDEAS, *supra* note 14, at 36.

219. *See* Kruse et al., *supra* note 211, at 150.

over the network. It is one of the goals of e2e to "support the widest possible variety of services and functions, to permit applications that cannot be anticipated."[220] Network architectures that violate the e2e design principle tend to build "complex function into a network [which] implicitly optimizes the network for one set of uses while substantially increasing the cost of a set of potentially valuable uses that may be unknown or unpredictable at design time."[221]

Although no single entity may exist in a network that can anticipate all possible uses of the network, this knowledge may indeed exist, but may be distributed among a myriad of individual actors in the network. E2e provides a mechanism to cope with such extremely dispersed knowledge in a network.[222] If the kind of

220. Saltzer et al., *supra* note 213, at 70.

221. *Id.*

222. To some extent, this is reminiscent of Friedrich Hayek's conception of competition as a discovery procedure. This conception stresses the importance of spontaneously ordering forces in an environment of extremely decentralized and dispersed knowledge:

> The real issue [of an economic order] is how we can best assist the optimum utilization of the knowledge, skills and opportunities to acquire knowledge, that are dispersed among hundreds of thousands of people, but given to nobody in their entirety . . . to treat [competition] as if all this knowledge were available to any one person at the outset is to make nonsense of it.

FRIEDRICH A. HAYEK, THE POLITICAL ORDER OF A FREE PEOPLE 68 (1979).

> The peculiar character of the problem of a rational economic order is determined precisely by the fact that the knowledge of the circumstances of which we must make use never exists in concentrated or integrated form, but solely as the dispersed bits of incomplete and frequently contradictory knowledge which all the separate individuals possess.

Friedrich A. Hayek, *The Use of Knowledge in Society*, 35 AM. ECON. REV. 519 (1945)*; see also* FRIEDRICH A. HAYEK, THE MIRAGE OF SOCIAL JUSTICE 70–71, 114–15 (1976); FRIEDRICH A. HAYEK, THE POLITICAL ORDER OF A FREE PEOPLE 67–70 (1979); Friedrich A. Hayek, *Competition as a Discovery Procedure*, *in* NEW STUDIES IN PHILOSOPHY, POLITICS, ECONOMICS AND THE HISTORY OF IDEAS 179 (1978) (considering competition as a means of discovering facts that would remain unknown or unusable without competition); Manfred E. Streit, *Cognition, Competition, and Catallaxy*, 4 CONST. POL. ECON. 223, 234–38 (1993). More generally, the claimed importance of the e2e argument for innovation is part of the larger debate concerning what the optimal market structure for innovation is and what the implications of centralized control for innovation are. *See* Lemley & Lessig, *supra* note 25, at 957–62; John E. Lopatka & William H. Page, *Internet Regulation and Consumer Welfare: Innovation, Speculation, and Cable*

innovation that will occur on a network is not predictable, e2e argues the network should not be biased by its very architecture towards any specific kind of innovation.[223]

The connection between e2e design and innovation is not a novel observation.[224] However, previous analyses of this connection did not notice that, in this regard, e2e was implemented on the Internet by a particular design of a namespace: the TCP/UDP port number space. As was described above, the port number space leaves twenty-five percent of all port numbers uncoordinated, thereby enabling decentralized innovation.[225] This openness of the TCP/UDP port number space is the Internet's implementation of the e2e argument.[226]

Uncoordinated namespaces can enable decentralized innovation. If the port number space were under close control of a company, any innovator would have to ask this company for permission before he could run a new software application over the Internet. Given the possibility that the company may act strategically, the innovator may be deterred from developing his application in the first place. Had the Internet in general and the regulation of the port number space specifically not complied with the e2e design principle, the

Bundling, 52 HASTINGS L.J. 891, 914–17 (2001); *see also* LESSIG, FUTURE OF IDEAS, *supra* note 14, at 139–40 (arguing that a decentralized architecture encourages experimentation, and that "innovation controlled by the state—[i.e., centralized control] fails.").

223. *See* LESSIG, FUTURE OF IDEAS, *supra* note 14, at 39; Lemley & Lessig, *supra* note 25, at 938. The e2e argument thereby tries to prevent any discrimination against emerging technologies. However, a counter-argument against e2e may be that some emerging technologies will need particular support by the network architecture to reach their full potential.

224. It was clearly formulated by Saltzer et al., *supra* note 213, at 70. Lawrence Lessig builds much of his analysis in his book *The Future of Ideas* on the impact of e2e on innovation. *See* LESSIG, FUTURE OF IDEAS, *supra* note 14; *see also* Blumenthal & Clark, *supra* note 212, at 72, 74 (discussing the e2e argument and "emerging requirements for the Internet today"); Kruse et al., *supra* note 211, at 141.

225. *See supra* text accompanying notes 209–11.

226. This is not to say that the openness of the TCP/UDP port number space is the only instance where e2e is implemented on the Internet. This Article does not attempt to provide a full assessment of the relationship between e2e, innovation, and the governance over the Internet.

development of HTTP, HTML, and the Web revolution might never have taken place.[227]

E. Scope of Namespace Governance

The governance of namespaces may differ not only in intensity, but also in scope. Namespaces can be designed to store large or small amounts of information. They can be constructed to be accessible for a single purpose or for multiple purposes. They may also have a fixed or an adaptive internal structure. Such design decisions determine various policy aspects of namespace governance, ranging from privacy and regulability to innovation issues.

1. Information-rich versus information-poor namespaces

Namespaces can be designed to collect large amounts of personal information about the persons who are accessing and registering with the namespace. They can also be designed to store as little personal information as possible. Whereas information-rich namespaces may lead to privacy concerns, information-poor namespaces may become a tool for privacy protection.

As described above,[228] Microsoft Passport creates a user namespace in which a large amount of personal information is stored in one location.[229] An information-rich namespace centralizes knowledge. Such architecture may be privacy-protecting because services that depend on the namespace do not have to store such information themselves. However, it may also pose threats to privacy as the central storage may be insecure or the namespace provider himself may misuse this information.[230]

Another example of an information-rich namespace is the DNS. Personal information about the registrants of Internet domain names has traditionally been publicly available through the WHOIS

227. *See* Saltzer et al., *supra* note 213, at 70.

228. *See supra* text accompanying notes 131–34.

229. After all, that is one of the goals of any authentication system. Today, one's identity on the Internet is fragmented across various identity providers, including employers, Internet portals, various communities, and business services. Authentication systems attempt to reduce such fragmentation. *See* Liberty Architecture Overview, *supra* note 156, at 9–16.

230. For this argument in the Microsoft Passport context, see *supra* text accompanying note 136.

database.[231] In contrast, no global public databases exist that contain personal information about every telephone subscriber. Therefore, from an outside perspective, the telephone network is an information-poor namespace.[232]

Also, to what detail a namespace identifies objects determines whether the namespace is information-rich or information-poor. In DRM systems, "metadata" namespaces are used to identify digital objects—such as music, video, or text files—that are protected by and transmitted over the DRM system.[233] The optimal granularity with which digital objects should be identified by the metadata namespace is an open question. Should a text be only identifiable in its entirety or should each paragraph, sentence, word, or even character be identifiable by the namespace?[234] Answering this

231. *See* Network Solutions, *at* http://www.networksolutions.com/cgi-bin/whois/whois (last visited Jan. 21, 2003).

232. The different treatment of personal information in the DNS and the telephone system creates problems for ENUM which attempts to connect both namespaces. As ENUM stands between the Internet and the telephone system, it is unclear which privacy model it should adopt. *See* Cannon, *supra* note 94, at 2, 4. ENUM potentially stores a large amount of private contact information. *See id.* at 4. Since such information is stored in a DNS-like database, it is questionable whether the traditionally lax privacy approach of DNS should also apply to ENUM. *See id.* at 35; Hwang et al., *supra* note 94, at 22–23; *see also* Electronic Privacy Information Center: ENUM, *at* http://www.epic.org/privacy/enum (last updated Dec. 2, 2002) (explaining the issue of privacy and the protection of personal information stored in ENUM); ENUM Forum—Working Documents, *at* http://www.enum-forum.org/workingdocs.html (last visited Dec. 16, 2002) (discussing privacy issues in ENUM implementation).

233. *See generally* Normal Paskin & Godfrey Rust, *The Digital Object Identifier Initiative; Metadata Implications*, *available at* http://www.doi.org/P2VER3.pdf (Feb. 10, 1999) (providing background information on "metadata" namespaces).

234. *See* BECHTOLD, VOM URHEBER-ZUM INFORMATIONSRECHT, *supra* note 55, at 39; Annemique M.E. de Kroon, *Protection of Copyright Management Information*, *in* COPYRIGHT AND ELECTRONIC COMMERCE: LEGAL ASPECTS OF ELECTRONIC COPYRIGHT MANAGEMENT 229, 231 (P. Bernt Hugenholtz ed. 2000); Norman Paskin, *Towards Unique Identifiers*, 87 PROC. OF THE IEEE 1208 (1999). Whether information about the names should be embedded in the names themselves or should be stored in a separate database is a related problem. In the area of metadata systems, this led to a long-lasting battle between "intelligent" and "dumb" identifiers. Choosing an appropriate architecture along these lines has efficiency and privacy implications. *See* BECHTOLD, VOM URHEBER- ZUM INFORMATIONSRECHT, *supra* note 55, at 38; Keith Hill, *A Perspective: The Role of Identifiers in Managing and Protecting*

question has efficiency and privacy implications. The more precisely an object can be identified, the better and more extensively usage data can be collected and processed. Determining a namespace's granularity determines its implications for privacy interests. This tension occurs in other namespaces as well.[235]

2. Single-purpose versus multi-purpose namespaces

While some namespaces serve specific narrow purposes, other namespaces can be used for many different purposes and accessed by different applications. This has implications for regulating such namespaces and for innovation occurring on top of them.

a. regulability

The P2P file namespace Napster, for example, served a narrowly confined purpose: to identify and locate music files in the network. Conversely, the DNS device namespace serves many different purposes. From the perspective of the DNS, it does not matter whether domain names are resolved in order to locate music, text documents, video, persons, or any other resources. The DNS is a multi-purpose namespace.

Single-purpose namespaces are more prone to regulation than multi-purpose namespaces. As soon as a court determined that the Napster namespace was used mainly for illegitimate purposes, the namespace could be regulated. A namespace such as the DNS, which is used for some illegitimate, but also for many legitimate purposes, would be much harder to shut down under this rationale. Multi-purpose namespaces therefore tend to be more stable.

Intellectual Property in the Digital Age, 87 PROC. OF THE IEEE 1228, 1232 (1999); Paskin, *supra*, at 1209, 1213–14.

235. In the disease namespace ICD, it is difficult to determine how precise the namespaces should be in order to identify causes of death and, in particular, different accidents. Doctors, epidemiologists, and statisticians each have different opinions regarding the optimal granularity of the disease namespaces. *See* BOWKER & STAR, *supra* note 21, at 101, 144–46, 270–75. For some general information about the ICD, see *supra* text accompanying note 62.

b. innovation around namespaces

Whether a namespace serves more than one purpose also determines to a large extent whether the namespace fosters or hinders innovation.

i. horizontally innovation-friendly namespaces

A multi-purpose namespace does not control the purposes for which it is accessed and used. Multi-purpose namespaces are "horizontally innovation-friendly," as they can be accessed and used by any application. A single-purpose namespace, on the other hand, exercises control over the use of the namespace. It can, for example, subject access to the namespace to some contractual agreement that imposes some restrictions on the user. It can also use technology, such as authentication techniques, to restrict the range of users that can access the namespace.

The IP address space is a multi-purpose, horizontally innovation-friendly namespace. If, for example, a P2P network wants to use IP addresses to identify and locate peers in its network, it is free to do so, as the IP address space does not control the purpose for which it is used. The IP address space therefore enables new applications to be created that use the IP address space for any purposes. The same is true for the Ethernet address space, the domain namespace, and the TCP/UDP port number space. Microsoft Passport and proprietary instant messaging systems, on the other hand, are single-purpose namespaces. Suppose, for example, that a company wants to develop an application that delivers streaming video, interactive gaming, and e-commerce applications between users connected to the Internet. Rather than creating a new user namespace for this purpose, the company plans to create a plug-in to AOL's instant messaging systems. The application would thereby use AOL's instant messaging user namespace for its own purposes. However, as long as AOL could control which application is accessing its instant messaging user namespace, the company would fail.[236] Single-purpose namespaces that are not horizontally innovation-friendly allow only certain authorized applications to

236. *See* Faulhaber, *supra* note 138, at 317–18. For information about the FCC's requirement to open AOL's instant messaging systems to competing systems, see discussion *supra* note 169 and accompanying text.

access their namespaces and control for what purposes the namespace is accessed. They can impede innovation by non-affiliated innovators.

ii. vertically innovation-friendly namespaces

Some multi-purpose namespaces are not only horizontally innovation-friendly in the sense that they can be accessed by and used in other applications for whatever purpose, they are also "vertically innovation-friendly" in the sense that they do not prevent the creation of other namespaces on top of them (see Figure 4).

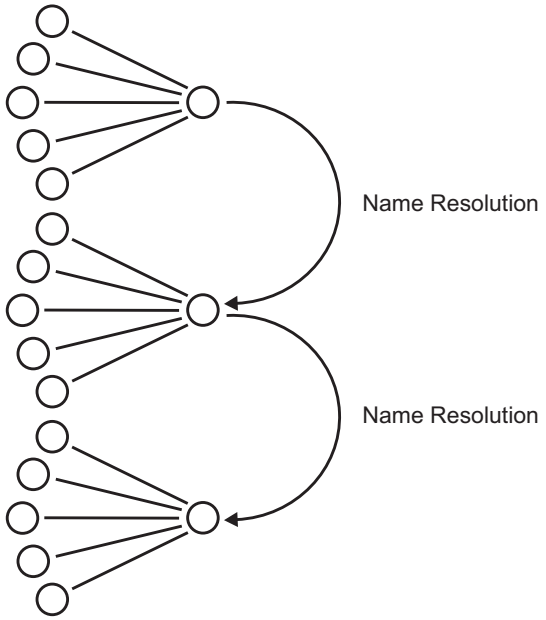

Figure 4: Vertically Innovation-Friendly Namespaces

Such multi-purpose namespaces facilitate innovation in software applications that need their own namespaces because such applications can use the existing namespace infrastructure and build their own namespaces on top of it. A single-purpose, non-vertically innovation-friendly namespace prevents such namespace creation by contractual or technological means.

A prime example of vertically innovation-friendly namespaces is the interrelation among the Ethernet address, IP address, and

domain namespaces. All three namespaces are vertically innovation-friendly as they are built on top of each other. While the DNS resolves domain names to IP addresses, an IP address is still not the address that is actually used when two computers communicate over the Internet on the level of the physical network. Rather, on this level, most computers are identified by Ethernet addresses.[237] The Address Resolution Protocol (ARP) enables the network to resolve IP addresses into Ethernet addresses. While the DNS connects the domain namespace with the IP address space, ARP in a similar way connects the IP address space with the Ethernet address space.[238]

Other examples include many P2P systems that create a proprietary namespace on top of the IP address space,[239] as well as Uniform Resource Names (URNs) (a location-independent namespace that is created on top of the namespace for identifying Web pages).[240] Biotechnological research crucially depends on vertically innovation-friendly namespaces.[241] Also, many instant messaging services build user namespaces on top of the IP address or

237. However, this is not the only addressing scheme. If a computer is connected to the Internet by a non-Ethernet network (e.g., ATM), the addressing scheme differs as well.

238. For an overview of ARP, see HALL, *supra* note 202, at 97–134. For a proposal to build even two more namespaces and search layers on top of the DNS, see John C. Klensin, *A Search-Based Access Model for the DNS*, *at* http://www.rfc-editor.org/internet-drafts/draft-klensin-dns-search-05.txt (Nov. 3, 2002).

239. This is done, for example, in the P2P system Overnet. *See* Overnet: How it Works, *at* http://www.overnet.com/documentation/how.html (last visited Jan. 15, 2003).

240. On the World Wide Web, Web pages are identified by URLs. As URLs include domain names, a document's URL has to be changed if it is moved to another computer with a different domain name. To solve this problem of ever changing URLs, URNs create a location-independent namespace on top of the URL namespace. For more information, see Leslie L. Daigle et al., *URN Namespace Definition Mechanisms*, Request for Comments (RFC) 2611 (June 1999), *at* http://www.rfc-editor.org/rfc/rfc2611.txt; Ryan Moats, *URN Syntax*, Request for Comments (RFC) 2141 (May 1997), *at* http://www.rfc-editor.org/rfc/rfc2141.txt; Karen Sollins & Larry Masinter, *Functional Requirements for Uniform Resource Names*, Request for Comments (RFC) 1737 (Dec. 1994), *at* http://www.rfc-editor.org/rfc/rfc1737.txt. For an overview of all registered URN namespaces, see IANA, URN Namespaces, *at* http://www.iana.org/assignments/urn-namespaces (last updated Aug. 16, 2002).

241. DNA sequence namespaces, for example, do not prevent higher-level namespaces from being built on top of them. *See* Birney et al., *supra* note 162.

the domain namespace.[242] On top of such instant messaging user namespaces, even other namespaces can be created. The Madster network,[243] for example, creates a "virtual private network" on top of the America Online Instant Messenger (AIM) user namespace. In essence, a distinct file namespace is created on top of the AIM user namespace. Madster enables users identified by the underlying AIM user namespace to share music and other files identified by the Madster file namespace.[244] This example shows that file namespaces can be built on top of user namespaces that, in turn, are built on top of several layers of device namespaces.

Vertically innovation-friendly namespaces facilitate the creation of new applications that need a new namespace which can be built on top of existing ones. The question of whether a namespace allows other namespaces to be built on top of it is an application of the e2e argument. As described above, the e2e argument states that system functions should be located at upper rather than lower levels of a layered system.[245] If a low-level namespace can control what happens on upper levels in a system of layered namespaces, this can thwart the openness and decentralized innovation the e2e argument attempts to achieve.

3. Fixed versus adaptive internal structure

Whether a namespace serves single or multiple purposes is a question that relates to how a namespace interacts with surrounding applications. Yet, the way in which namespaces are structured

242. *See* Michael Gowan, *How it Works: Instant Messaging*, *at* http://www.cnn.com/2000/TECH/computing/05/25/how.messaging.works.idg (May 25, 2000); Jeff Tyson, *How Instant Messaging Works*, *at* http://www.howstuffworks.com/instant-messaging.htm (last visited Jan. 21, 2003); Speta, *supra* note 143, at 236; *see also* Faulhaber, *supra* note 138, at 317 (concluding that the network effect of instant messaging is achieved via the service infrastructure rather than the instant messaging service itself).

243. *See* Madster, *at* http://www.madster.com (last visited Dec. 1, 2002). Madster was formerly known as Aimster. On October 30, 2002, a district court issued a preliminary injunction ordering Aimster to shut down its service. *See In re* Aimster Copyright Litig., 2002 WL 31443236 (N.D. Ill. 2002).

244. For an analysis of the copyright liability of Aimster, see Haydn J. Richards, Jr., *Is the Whole Greater Than the Sum of Its Parts? The Applicability of the Fair Use Doctrine to the New Breed of Instant Messaging Software*, 8 RICH. J.L. & TECH. 15 (Fall 2001), *at* http://www.law.richmond.edu/jolt/v8i2/article3.html.

245. *See* Reed et al., *supra* note 214.

internally also matters from a governance perspective. Designing the internal structure of namespaces is complicated by the fact that, to put it simply, history matters. Decisions made at the time of the initial technical design of the namespace may impede its use at a later time when the environment in which the namespace operates has changed. Designing namespaces has to take into account that the purposes for which the namespace may be used, the number of names that have to be addressable, and even the kind of names that can be addressed with the namespace may change over time. Building a comprehensive, rigid namespace structure at one time does not mean that this structure will be the best possible structure in the future.

a. changing number of names

The most widespread problem in this regard is that the size of a namespace may gradually prove too small. As was described above,[246] the size of the IP and the Ethernet address spaces was enlarged over time in order to accommodate more addresses.[247] Similar problems arose in the domain namespace,[248] the Social Security number space,[249] and the disease namespace ICD.[250]

246. *See supra* text accompanying notes 191–201.

247. Another namespace that is expanding due to scarcity concerns is the UPC bar code space. *See* Kate Murphy, *Bigger Bar Code Inches Up on Retailers*, N.Y. TIMES, Aug. 12, 2002, at C3.

248. Until the 1980s, each computer connected to the Internet stored a single list of all the names and IP addresses of all other connected computers. *See* MUELLER, *supra* note 14, at 40–41, 77–78. As the Internet increased in size, a more scalable namespace architecture was needed. The current DNS hierarchy is the result of this evolutionary process. *See id.* For a detailed history of the DNS, see *id.* at 73–208; Froomkin, *supra* note 70, at 50–92; Kesan & Shah, *supra* note 70, at 169–76.

249. Originally, Social Security numbers were used to administer potential retirement and survivor benefit payments under the Social Security Act of 1935. *See* SIMSON GARFINKEL, DATABASE NATION 18–20 (2000). Today, Social Security numbers are used by a wide variety of federal, state, and local authorities, as well as private companies for identification purposes. *See id.* at 21–25. Nevertheless, the small size of the number space, the lack of a check digit, and other disadvantages severely impede the utility of Social Security numbers for many purposes. *See id.* at 20.

250. Originally, the ICD featured a maximum of 200 disease categories. *See* BOWKER & STAR, *supra* note 21, at 64. This limitation was set not because only 200 diseases existed, but because Austrian census forms could not hold

Namespace architectures have to respond to changing demands. Making a namespace too small in the beginning may put a namespace at a disadvantage in the long run.[251]

b. changing kinds of names

A namespace can encode information about the kinds of names that are included in the namespace in its very structure. Because the kinds of names the namespace has to deal with change over time, its structure may become outdated. This is especially important in a particular class of namespaces, namely, bibliographic classifications schemes.

Libraries use bibliographic classification schemes to place books on bookshelves in a particular order and to create classified catalogues and bibliographies.[252] For a long time, classification schemes organized knowledge in a strictly hierarchical manner. For example, the LCC, one of the largest in the world, continues to do so up to the present day.[253] In such a classification scheme, each book or document is assigned one or several numerical classifiers which locate the contained knowledge in a hierarchical representation of all the existing knowledge.

However, all bibliographic classification schemes have to grapple with the problem that knowledge is constantly emerging and changing. As new subjects and areas of research emerge, classification schemes become outdated. They have a certain

more lines. *See id.* For some general information about the ICD, see *supra* text accompanying note 62.

251. This makes it particularly hard to estimate the appropriate size of a namespace when it is designed. It is estimated, for example, that a namespace for identifying scientific and technical literature should be able to identify at least 100 trillion articles. *See* Paskin, *supra* note 234, at 1212.

252. For a general overview of the theory, problems, history, and current examples of classification schemes, see MARCELLA & NEWTON, *supra* note 121, at 65–112 (giving an overview of the history and present examples of classification schemes). For a comprehensive account of the history of library classification systems, see EVGENIJ I. SAMURIN, GESCHICHTE DER BIBLIOTHEKARISCH-BIBLIOGRAPHISCHEN KLASSIFIKATION [The History of Librarian Bibliographic Classification] (1964).

253. "LCC is fundamentally and irrevocably an enumerative scheme, with perhaps the least synthesis of all the general schemes." MARCELLA & NEWTON, *supra* note 121, at 85. Over sixty-two percent of U.S. university libraries use the LCC. *See id.* at 80. It boasts over 60,000 distinct classification numbers. For an overview of the LCC, see *id.* at 79–89.

"built-in obsolescence."[254] Editors of the scheme (so-called "classificationists") then must add new classifiers to enumerate classification schemes. Although many classification schemes are updated on a regular basis, it can take years until new fields of science and knowledge are properly reflected in the schemes. Due to the sluggish internal structure of such namespaces, the integration of new kinds of names is a lengthy and tedious task. Sometimes, classification schemes are even incapable of integrating new subjects into their existing structure. Such classification difficulties impede the organization and processing of new knowledge, which can have a detrimental impact on scientific progress.[255] The problems of coding information into the structure of the namespace and the resulting path dependencies are not confined to bibliographic classification schemes, but can also be observed in other namespaces—such as the IP address space or disease namespaces.[256] Encoding information

254. *Id.* at 30.

255. Clause Poulsen gives a summary of the subject access problem as follows:

> A dynamic information society depends on subject access to pioneering literature from the dominant paradigms and literature from the marginal paradigms, as this literature is central for the innovation processes. Classification systems are made from yesterday's concepts of the dominant paradigms. Therefore classification systems are normally not suited to providing subject access to literature from marginal paradigms and pioneering literature in the dominant paradigms.

Claus Poulsen, *Subject Access to New Subjects, Specific Paradigms and Surveys: PARADOKS-registration*, 40 LIBRI 179, 183 (1990); *see also* S.R. Ranganathan, *Self-Perpetuating Scheme of Classification*, 4 J. DOCUMENTATION 223, 231 (1949) (stating that in the Library of Congress, Decimal Classifications and the Universal Decimal Classification, classifiers have little chance to anticipate class numbers for new formulations because they are virtually arbitrary); Gerhard J.A. Riesthuis, *Sociological Aspects of Classification*, 24 INT'L CATALOGUING AND BIBLIOGRAPHIC CONTROL 35, 36 (1995). A similar problem exists with disease namespaces, as Bowker and Star describe: "Even at ten-year intervals [of publishing a new edition of the disease namespace], a new disease entity may take more than twenty years to be included since the pace of medical discovery and the uncertain process of consensus can be very slow." BOWKER & STAR, *supra* note 21, at 122.

256. Initially, the IP address space was hierarchically structured in "classes" of different sizes ("classful IP addressing"). *See* COMER, *supra* note 107, at 283–85; *see also* MUELLER, *supra* note 14, at 33–35 (discussing routers and IP addresses). The information expressed by this hierarchy was used by the network routers to route traffic efficiently over the Internet. *See* MUELLER,

about the kinds of names into the internal structure of a namespace is not advisable in dynamically changing environments. Or, to paraphrase Geoffrey C. Bowker and Susan Leigh Star, the only good namespace is a living namespace.[257]

Regarding bibliographic classification systems, library and information science has invested large amounts of time and effort to get rid of these structural, innovation-hostile shortcomings. Over the last few decades, various "self-perpetuating" classification schemes have been proposed to solve these problems. The basic idea, developed by the Indian librarian Shiyali R. Ranganathan in the 1930s, is to fit "a [classification] scheme with [an] inner mechanism by which any classifier can arrive at the correct class number for a new formation in the field of knowledge without waiting for the classificationist to give the number."[258]

As it is beyond the scope of this Article to describe the so-called "faceted analytico-synthetic" approach in detail, suffice it to say that such classification schemes do not list all specific subjects of knowledge. Rather, they list "the fundamental constituent concepts [or "facets" of knowledge] by the combination of a few, from which the specific subjects are formed."[259] By using these facets and digits

supra note 14, at 33–35. As the Internet grew larger, this mechanism proved inefficient. *See id.* at 36. Therefore, new routing mechanisms (such as "subnet addressing" and "classless inter-domain routing") were developed. *See id.* at 37. However, for these mechanisms, the information expressed in the hierarchical structure of the IP address space was not unnecessary. *See id.* at 38. The fixed hierarchical structure itself was obstructive to the new routing mechanisms. *See id.* at 37–38. Therefore, the assignment procedure of IP addresses and the internal structure of the namespace had to be adapted. *See id.* at 36; *see also* COMER, *supra* note 107, at 289–92 (discussing the addressing scheme used by IP). Another example is the ICD, which constantly has to be adapted as new knowledge about existing diseases, new diseases, or other new causes of death emerge. *See* BOWKER & STAR, *supra* note 21, at 69–77, 80–85, 123.

257. *See* BOWKER & STAR, *supra* note 21, at 326 ("The only good classification is a living classification.").

258. Ranganathan, *supra* note 255, at 224; *see also* MARCELLA & NEWTON, *supra* note 121, at 30–31 (discussing the fully faceted approach).

259. Ranganathan, *supra* note 255, at 232. For an introduction to faceted classification schemes, see BRIAN C. VICKERY, FACETED CLASSIFICATION: A GUIDE TO THE CONSTRUCTION AND USE OF SPECIAL SCHEMES (1960) (providing a practical guide to classification techniques).

with mnemonic values,[260] librarians should be able to come up with a uniform classification number for newly emerging knowledge. Ideally, even different classifiers working in different libraries should be able to create new subjects without waiting for the next edition of the classification and still achieve identical results.[261] By providing librarians with modularized tools by which they can build classification numbers on their own in a decentralized, yet uniform way, faceted analytico-synthetic classification schemes attempt to enable a self-perpetuating classification.

That, at least, is the idea. The faceted analytico-synthetic classification approach faces numerous objections and has only partly been implemented in large contemporary classification schemes.[262] It is not the goal of this Article to analyze the details of

260. For an overview of the concept of seminal mnemonics as used in Colon Classification (CC), see RAGHUNATH S. PARKHI, DECIMAL CLASSIFICATION AND COLON CLASSIFICATION IN PERSPECTIVE 461–73 (1964); *see also* MARCELLA & NEWTON, *supra* note 121, at 58 (discussing seminal mnemonics aids within Ranganthan's CC scheme).

261. *See* Ranganathan, *supra* note 255, at 231. The approach is called "faceted analytico-synthetic" because subjects that have to be classified are first analyzed into their individual facets; then, these facets are synthesized or brought together to form a class number. *See* MARCELLA & NEWTON, *supra* note 121, at 25. An example for creating a new classification number with the faceted analytico-synthetic approach is given by PARKHI, *supra* note 260, at 469–70. For a comparison between enumerative and faceted classification schemes see MARCELLA & NEWTON, *supra* note 121, at 20–28. Marcella and Newton also provide a general description:

> The theory is based upon the argument that, instead of attempting to list all subjects, a classification should first identify main classes or distinct disciplines. Then, within each discipline, it need only enumerate basic concepts, or elements, arranging these within the appropriate category. Each category represents a *facet* of a subject. Most subjects are compounds made up of two or more elements from the various facets of a subject field or from facets common to all subjects, such as form of presentation, place and time. To classify an item, we analyse [sic] it into its facets and then focus on the appropriate element in each. We then employ what is called notational synthesis, by linking together in a specified order and manner the symbols representing these elements, or *foci*, thus building up an appropriate classmark.

Id. at 19–20.

262. Over the last half-century, the value of the facet approach for bibliographic classification schemes has been widely acknowledged. To various extents, it has been incorporated in the Dewey Decimal Classification, the Universal Decimal Classification, and the Bliss Bibliographic

classification schemes. Rather, faceted analytico-synthetic classification schemes are examples of namespaces that can be changed and adapted in a decentralized, yet uniform way because the *kinds* of names that must be identified change over time. By providing tools for modularized and decentralized name creation, such namespaces can be dynamically changed in substance and scope without changing their underlying basic modular components.[263]

These ideas can be applied and found in other namespaces as well. The chemical periodical system provides a limited number of elements by which all chemical compounds can be identified. If a new compound or mixture emerges, different chemists working in different laboratories will come up with a uniform name for it. As with the facets in analytico-synthetic classification schemes, the periodic system provides a modularized tool set by which the namespace of all chemical compounds can be dynamically changed in substance and scope without changing the underlying basic structure of the namespace (i.e., the periodic system).[264] Modularization and decentralization can enable innovation within the namespace itself.

Classification. *See* MARCELLA & NEWTON, *supra* note 121, at 28–30; Clare Beghtol, *'Facets' as Interdisciplinary Undiscovered Public Knowledge: S.R. Ranganathan in India and L. Guttman in Israel*, 51 J. DOCUMENTATION 194, 201 (1995). However, the best-known self-perpetuating classification scheme is the CC developed by Shiyali R. Ranganathan in the 1930s. *See id.* at 58, 71. In CC, the faceted analytico-synthetic approach is realized to the largest extent. For an assessment of the self-perpetuating feature of CC, see ABDUL MAJID BABA, DEWEY DECIMAL CLASSIFICATION, UNIVERSAL DECIMAL CLASSIFICATION AND COLON CLASSIFICATION 336–37, 449 (1988); ARTHUR MALTBY, SAYERS' MANUAL OF CLASSIFICATION FOR LIBRARIANS 199–201 (5th ed. 1975); *see also* SHIYALI R. RANGANATHAN, PROLEGOMENA TO LIBRARY CLASSIFICATION (3d ed. 1967) (discussing basic concepts and principals of classification); M.A. Gopinath, *Colon Classifiation*, *in* CLASSIFICATION IN THE 1970S 51, 75 (Arthur Maltby ed., 1972) ("CC is approximating towards a freely-faceted classification."). For a general overview of the CC, see ELAINE SVENONIUS, THE INTELLECTUAL FOUNDATION OF INFORMATION ORGANIZATION 174–76 (2000). CC is not used by many libraries worldwide and is fading away slowly for various reasons. *See* MARCELLA & NEWTON, *supra* note 121, at 103–04.

263. For a general analysis of the importance of modularity, see BALDWIN & CLARK, *supra* note 180.

264. *See* Ranganathan, *supra* note 255, at 232. For attempts to build a facet-oriented search layer on top of the DNS, see Klensin, *supra* note 238.

IV. IMPLICATIONS OF GOVERNANCE DIMENSIONS

Hitherto, this Article has identified several dimensions along which namespace governance can be studied (means, intensity and scope of governance, namespace topology, and who should govern). Choosing a particular design for a namespace has numerous legal and policy consequences. Although these dimensions differ in many respects, they are concerned with two basic aspects. First, choosing a particular design for a namespace along the governance dimensions described above has implications for the values protected and expressed by the namespace. Second, it also influences the allocation of knowledge, control, and responsibility within the namespace.

A. Namespace Architectures Protect and Express Values

As this Article illustrates, technical control over a namespace can be used as leverage for policy and legal control. Such control may encompass speech, access, privacy, content, copyright, trademark, liability, conflict resolution, competition, innovation, and market structure regulation.

Choosing particular namespace architectures can influence the way in which such values are protected. In the domain namespace, for instance, the namespace provider does not merely control trademark-related aspects of the namespace through the UDRP. It can also decide whether to charge a fee for domain name registrations,[265] what personal information a domain name registrant must provide, and who can access such information afterwards.[266] The namespace provider can regulate the domain name registration industry by imposing price controls and enforcing market structures.[267] It can decide what TLDs should exist.[268] For instance, whether to introduce a .biz TLD for businesses, a .ps TLD for

265. ICANN discussed introducing such a fee in 1999. *See* MUELLER, *supra* note 14, at 7, 188–90; *see also* Froomkin, *supra* note 70, at 87–89 (discussing ICANN's search for revenue).

266. *See* MUELLER, *supra* note 14, at 8. The current design of the domain namespace allows everyone to identify the name as well as the physical and e-mail address of every domain name registrant. *See id.* at 219, 235–38.

267. *See id.* at 219.

268. *See* Name.Space, Inc. v. Network Solutions, Inc., 202 F.3d 573 (2d Cir. 2000).

Palestine,[269] a .eu TLD for the European Union,[270] a .xxx TLD for Web sites with sexually explicit material, or a .kids TLD for Web sites which are suitable for children are all policy decisions a namespace provider makes.[271] Many such decisions are policy choices that involve issues of international politics, freedom of speech, and content regulation.[272]

Other examples of how the namespace architecture determines the values protected by the namespace include federated namespaces that enable competition between different namespace providers;[273] centralized P2P user namespaces that protect the interests of copyright owners;[274] decentralized P2P user namespaces that are specifically designed to preserve the privacy of information producers and consumers and resist censorship;[275] and uncoordinated namespaces such as the TCP/UDP port number spaces that create an open platform for decentralized, uncoordinated innovation.[276]

At the same time, by protecting certain values, many namespaces communicate a particular *Weltanschauung*.[277] This is particularly noticeable in bibliographic classification schemes.[278] In library and information sciences, it is a well-known fact that classification schemes often demonstrate structural biases on the basis of gender, sexuality, race, age, ability, ethnicity, language,

269. This TLD was created in 2000. *See* IANA, *Root*-Zone Whois Information, .ps-Palestinian Territories, *at* http://www.iana.org/root-whois/ps.htm (last updated Jan. 6, 2003); *see also* Froomkin, *supra* note 70, at 47–48 (discussing the .ps as the code for Palestine).

270. *See* Council Regulation 733/2002 of 26 April 2002 On the Implementation of the .eu Top Level Domain, 2002 O.J. (L 113) 1.

271. *See* MUELLER, *supra* note 14, at 9; Froomkin & Lemley, *supra* note 71, at 19–21.

272. *See* MUELLER, *supra* note 14, at 9.

273. *See supra* text accompanying notes 145–73.

274. *See supra* text accompanying notes 128–30.

275. *See supra* text accompanying note 189.

276. *See supra* text accompanying notes 202–27.

277. Defined as a "particular philosophy or view of life; a concept of the world held by an individual or a group." 20 THE OXFORD ENGLISH DICTIONARY 149 (2d ed. 1989).

278. *See* Wilson, *supra* note 105, at 392. Wilson writes: "In all these classifications, the dominant ideology is assumed to represent the society in which it was born. That is, in DCC and [LCC] the principal Weltanschauung is white, Protestant, English, capitalist male . . . . In the BBK, the equivalent is assumed to be white, atheist, Russian (i.e., European), Party member." *Id.* at 395 (citation omitted).

culture, or religion.[279] The DDC class for religion is biased towards—or, more gently spoken, heavily focused on—Christianity.[280] LCC exhibits distinct biases "towards the social structure, history, law and cultural concerns of the United States."[281] The major Russian classification system has been criticized for reflecting Socialist ideology.[282] Biases in bibliographic classification schemes do not only occur in publicly governed schemes. While government-sponsored classification schemes exhibit the greatest degree of ideological deformation, privately sponsored classification schemes tend to show various degrees of ethnocentricity.[283] The

279. For an overview of relevant empirical research literature, see Hope A. Olson & Rose Schlegl, *Standardization, Objectivity, and User Focus: A Meta-Analysis of Subject Access Critiques*, 32 CATALOGING & CLASSIFICATION Q. 61 (2001). A database surveying this literature is located at http://www.ualberta.ca/~holson/marginal/database.htm (last visited Jan. 13, 2003); *see also* Hope A. Olson, *Mapping Beyond Dewey's Boundaries: Constructing Classificatory Space for Marginalized Knowledge Domains*, 47 LIBR. TRENDS 233 (1998) (identifying classifications as bounded systems that marginalize certain groups and topics); Wilson, *supra* note 105, at 394 (describing how DDC "demonstrates national, linguistic, religious, and ethnic biases.").

280. In the twenty-first edition of DDC, the class on religion (200) is divided into the following divisions: "Philosophy & Theory of Religion" (210), "The Bible" (220), "Christianity & Christian Theology" (230), "Christian Practice & Observance" (240), "Christian Pastoral Practice & Religious Orders" (250), "Church Organization, Social Work & Worship" (260), "History of Christianity" (270), "Christian Denominations" (280), and finally, "Other Religions" (290). DDC, *at* http://www.oclc.org/dewey/about/hundreds.htm (last visited Feb. 4, 2003). For other biases in the DDC, see Olson, *supra* note 279, at 253 n.1; Wilson, *supra* note 105, at 394–95. Over the last few years, DDC has undertaken great efforts to reduce systematic biases in its classification scheme.

281. MARCELLA & NEWTON, *supra* note 121, at 88.

282. *See* Tamara S. Goltvinskaya & Eduard S. Sukiasyan, *Library-Bibliographical Classification: On the Path of Renovation*, 20 KNOWLEDGE ORG. 77, 78–79 (1993) (referring to the LBC/BBK, the most widely used classification system in Russia and some neighboring countries). Whereas the DDC starts with the division "generalities," the LBC/BBK starts with "Marxism-Leninism" as its first division. For a comparison of the major divisions in the DDC, LBC/BBK, and LCC, see Wilson, *supra* note 105, at 394–95. Other classification and subject heading schemes suffer from similar shortcomings. Classic biases in schemes used in the United States include the treatment of Native Americans as well as of African cultures and religions. *See* Olson & Schlegl, *supra* note 279, at 67–68.

283. *See* Wilson, *supra* note 105, at 393, 395.

plasticity of bibliographic classification schemes can also be used strategically: Chinese classification systems have been deliberately shaped to reflect particular political and ideological beliefs.[284]

This is not the place to criticize particular classification schemes. Indeed, some biases in classification schemes may be unavoidable.[285] Biased bibliographic classification schemes merely illustrate that namespaces are "social construct[s] . . . [which] reflect the same biases as the culture that creates [them]."[286] Such problems do not only occur in bibliographic classification schemes. The ICD is heavily focused on—or biased towards—accidents and diseases that occur in the western industrialized world and can be treated by western medicine.[287] Furthermore, it reflects ethical controversies, such as abortion, and stillbirth. Finally, the Apartheid regime in South Africa used namespaces to classify human beings according to a predefined set of races, with all the consequences to South Africa's

284. *See* William E. Studwell et al., *Ideological Influences on Book Classification Schemes in the People's Republic of China*, 19 CATALOGING & CLASSIFICATION Q. 61–64 (1994) (tracing back such influences to an early Chinese classification scheme in 26 B.C.). For a similar statement regarding the Russian LBC/BBK, see N. P. Zhurzhalina, *The Soviet Bibliothecal-Bibliographical Classification (BBK)*, INT'L CATALOGUING, Apr.–June 1980, at 21.

285. Unavoidable biases may result from the fact that their users are not free from biases themselves. As Holley and Killheffer point out, "biased terms may have to remain as cross-references unless we are prepared to sacrifice access for patrons who are accustomed to using the biased alternative." Robert P. Holley & Robert E. Killheffer, *Is There an Answer to the Subject Access Crisis?*, 1 CATALOGING & CLASSIFICATION Q. 125, 126 (1982). Furthermore, many scholars argue that it is simply impossible to design a totally objective, unbiased classification scheme. *See* Olson, *supra* note 279, at 252. However, other scholars propose that, due to their ability to construct themselves, faceted and analytico-synthetic classification schemes such as CC exhibit less inherent biases than other schemes. *See* Wilson, *supra* note 105, at 393.

286. Olson, *supra* note 279, at 233–34; Riesthuis, *supra* note 255; *see also* Eric de Grolier, *Classifications as Cultural Artefacts*, *in* 1 UNIVERSAL CLASSIFICATION I: SUBJECT ANALYSIS AND ORDERING SYSTEMS 19–34 (Ingetraut Dahlberg ed., 1982).

287. *See* BOWKER & STAR, *supra* note 21, at 66–67, 86, 120–21. "The ICD is richest in its description of ways of dying in developed countries at this moment in history; it is not that other accidents and diseases cannot be described, but they cannot be described in as much detail." *Id.* at 76. "A simple agonistic reading of the ICD is that the system was set up in an age of imperialism and helped impose an imperialist reading of disease from the West onto the rest of the world. There is truth in this . . . ." *Id.* at 115.

society, economy, and politics.[288] The structure of other namespaces, such as Web directories, can express values in similar ways.

B. Allocation of Knowledge, Control, and Responsibility

While this Article identifies several distinct governance dimensions, most of them can be reduced to a single, abstract dimension. Most governance dimensions described thus far differ in the allocation of knowledge, control, and responsibility within a namespace.

A flat namespace, for example, has a single point of *knowledge*.[289] One database knows all names and their related attributes. Such centralized knowledge can pose a privacy risk. At the same time, centralized knowledge can lead to centralized *control*. If one single entity in a namespace knows about all actions occurring within the namespace, it is an optimal starting point for namespace control. The existence of centralized control can lead to an environment in which the flat namespace is held centrally *responsible* for all actions occurring within the namespace. The Napster case is a prime example of such a centralization of knowledge, control, and responsibility.

On the other hand, in vertically distributed—or, hierarchical—namespaces, different parts of the namespace can be managed by different entities and, occasionally, different policies.[290] Hierarchical namespaces distribute knowledge, control, and responsibility over different hierarchies of the namespace.[291]

A similar dichotomy can be observed in horizontally distributed namespaces. Centralized namespaces concentrate *knowledge* in one location. They are therefore prone to surveillance and can be used for data mining purposes. Centralized namespaces have a single point of *control* that can be regulated. This may also lead to centralized *responsibility* within the namespace. In a decentralized

288. *See id.* at 195–225.

289. *See* Watson, *supra* note 37, at 207 (discussing two forms of addresses in common use, single level or flat, and hierarchical).

290. *See* COULOURIS ET AL., *supra* note 33, at 358.

291. Minar therefore writes that hierarchical systems are more "fault-tolerant and lawsuit-proof than centralized systems." Minar, *Part 2*, *supra* note 107, at 4.

namespace, however, knowledge, control, and responsibility can be dispersed throughout the network to such a degree that they essentially fizzle out of the network. In a decentralized namespace, such as Gnutella, no entity exists that has central knowledge, control, and responsibility for the actions occurring in the namespace.

Other dimensions of namespace regulation have similar features. As described above,[292] an uncoordinated namespace is fully "democratized" in the sense that no entity in the namespace has more knowledge, control, or responsibility over the namespace than any other entity. Figure 5 gives an overview of the allocation of knowledge, control, and responsibility in most of the dimensions of namespace governance identified in this Article.

292. *See supra* text accompanying note 202.

Namespace Architecture		Allocation of		
		Knowledge	Control	Responsibility
Vertical Distribution	Flat	c[293]	c	c
	Hierarchical	d	m	m
Horizontal Distribution	Centralized	c	c	c
	Federated	m	m	m
	Decentralized	d	d	d
Intensity	Controlled	c	c	c
	Coordinated	m	d	m
	Uncoordinated	d	d	d
Scope	Information-rich	c	c	c
	Information-poor	d	d	d
	Single-purpose	c	c	c
	Multi-purpose	d	d	d
	Rigid Internal Structure	c	c	c
	Adaptive Internal Structure	d	d	d

Figure 5: Allocation of Knowledge, Control, and Responsibility

V. DESIGNING NAMESPACE GOVERNANCE

Designing the architecture of namespaces is not merely a technical matter. It entails decisions about legal and policy

293. Key: c = fully centralized; m = intermediate between centralized and decentralized; d = fully decentralized.

questions. Structure has consequences. Legal and policy values can be frozen into the very structure of a namespace. While this Article provides a descriptive analysis of the close intertwining between technology, law, and policy in regards to namespaces, it has not addressed the normative consequences of this analysis. Should namespaces be designed according to certain principles? What are those principles?

Although answering these questions seems necessary to develop a full-fledged normative theory of namespace governance, this Article does not attempt to provide such answers. It is beyond the scope of the Article, and may even be impossible for several reasons:

1. Namespaces are used in many different areas, ranging from network authentication and communication to bibliographic classification issues. While this Article has stressed common features of namespaces, there are also large differences. Therefore, it is hard to draw any general conclusions that are applicable to namespaces. What may represent a wise regulatory decision for one particular namespace may be totally erroneous for another one. After all, authenticating users in a PKI is not the same as developing a method to place books in library shelves in some reasonable order.
2. Developing a theory of namespace regulation is complicated by the fact that it should be based on a sound general theory of regulation. Technology is plastic and, therefore, values such as freedom, competition, copyright, and privacy can be "engineered" into technology.[294] However, solving social problems by technological design usually is an *ex ante* regulation—the regulation takes place before the problem that is addressed can emerge. Regulation by technological design regulates the problem away. While such regulation may be the most efficient, it may not be the most desirable in an environment lacking predictability. If it is unclear what kind of problems will emerge in the future, how could an *ex ante* regulation—by

294. *Cf.* LESSIG, CODE, *supra* note 13 (discussing values and policies inherently infused in the laws regulating technology and the Internet).

technological design—ever deal with them? On the other hand, any *ex post* regulation has to grapple with the problem that certain regulatory options may be foreclosed due to path dependency. The regulation is restricted by the already-existing technology and earlier regulatory decisions. Ultimately, the tension between lack of predictability and path dependency could lead to an answer as to what kinds of values should be implemented by an *ex ante* regulation (i.e., by engineering them into technology), and what kinds of values should be left to *ex post* regulation (by the legislature, the courts, and other regulators). Such a normative theory of namespace governance could provide guidelines in which legal and policy considerations are taken into account during the technical design of a namespace. It could also prompt lawyers to become more involved in the design of namespace architectures. However, developing the underlying general normative theory of regulation is an endeavor that has far larger applications and implications than the mere governance of namespaces.

3. A complete theory of how namespaces should be governed is complicated by the fact that it is not enough to look solely at individual namespace governance dimensions. Rather, the interaction between different governance dimensions should be taken into account as well. Consider, for example, the DNS. As described above, the hierarchical structure of the DNS leads to a certain decentralization—different parts of the namespace can be governed by different entities.[295] Yet, ICANN's registry regulations and the UDRP can be understood as attempts to reverse some of the decentralization that is embedded in the namespace structure.[296] Different dimensions of namespace governance (here, contractual webs and topology) are not always used to achieve the same goal.

295. *See supra* text accompanying notes 115–16.

296. The author is indebted to Milton Mueller for this remark.

4. Finally, designing a namespace architecture must not only take into account the interactions between different governance dimensions in a namespace, but also those between different namespaces. If, for example, a namespace is specifically designed to protect certain values (such as privacy or freedom of expression), it is important to note that the mere protection of such values in the namespace is often not sufficient to protect them in reality. Often, namespaces depend on other namespaces. If one namespace is designed to be open and innovation-friendly, but depends on another namespace that is closed and innovation-hostile, openness and innovation are not preserved in the overall system. An example of this problem is the potential tension between the TCP port number space and centralized P2P file namespaces. When the recording industry wanted to shut down Napster, it could have done so by shutting down the "channel" over which Napster communicated. In other words, it could have tried to shut down the TCP port 6699. However, the e2e-compliant TCP port number space made such regulation impossible. No central entity exists that administers TCP port 6699. Furthermore, Napster could have easily switched to another TCP port. To achieve its goal, the recording industry turned to another namespace that is more controllable—Napster's own file namespace. While the regulation of TCP port 6699 would have only shut down one object in the TCP port number space, the recording industry succeeded in shutting down the whole file number space of Napster. As long as an open and decentralized namespace depends on another namespace with a different architecture and, therefore, value system, keeping the namespaces open and decentralized does not necessarily mean that openness and decentralization will ultimately reign (see Figure 6).[297]

297. Another example where the interaction between different namespaces becomes important is DRM. DRM systems often employ several device, file, and user namespaces at the same time. As many DRM systems try to serve the interests of content owners, a proprietary, centralized, intense namespace

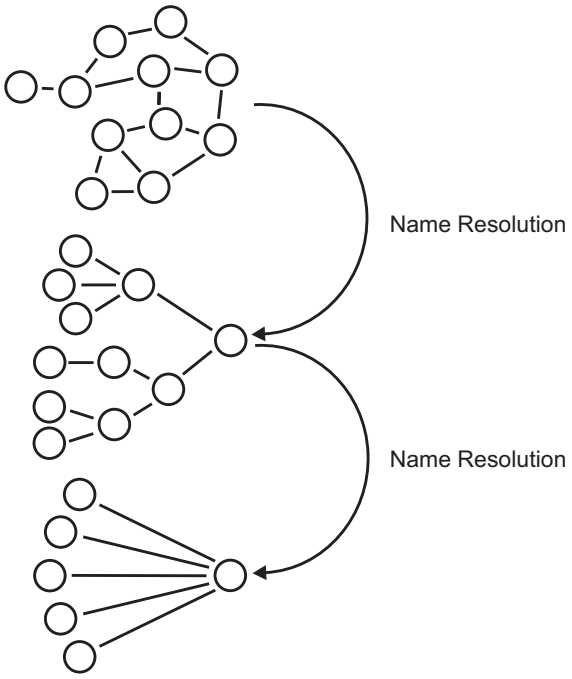

Figure 6: Interaction Between Namespaces

For all these reasons, this Article is confined to presenting a taxonomic structure under which the governance of various namespaces can be analyzed. This taxonomy proves helpful for discussing the legal and policy implications of a namespace during its technical design. If one determines, for example, that a namespace should be open, enable competition, protect privacy, and foster innovation, the taxonomy presented provides answers as to how these legal and policy goals may be implemented in a namespace. It provides a tool for analyzing and answering normative questions.

VI. CONCLUSION

Namespaces are an overlooked facet of governance both in real space and cyberspace. Although we are surrounded by namespaces,

governance structure is often appropriate. In order to achieve the utmost security and robustness, however, DRM systems have to design each of their namespaces according to these principles and must ensure proper and secure interaction and communication among them.

discussions have not regularly paid any attention to general policy problems of namespaces. This Article demonstrates that the technical design of namespaces in general has numerous legal and policy implications. As analytical tools, this Article has developed several dimensions—in fact, a namespace of the dimensions of namespace governance—that prove useful in analyzing governance questions in regards to namespaces. Many of these dimensions differ in the way knowledge, control, and responsibility are allocated within the namespace. They also differ in the values they protect. The taxonomic structure developed in this Article might be useful to legal scholars who think about the implications of various namespaces. It may also be useful to designers of namespaces who ponder the legal and policy implications of their actions. Finally, it may assist lawyers and policymakers in becoming involved in governance discussions at the time of the technological design of namespaces. While this Article has focused mainly on namespaces in cyberspace, many of its findings can be applied to namespaces in real space as well.[298] As we are literally surrounded by namespaces in cyberspace and real space, governance in namespaces is an ubiquitous theme.

298. The P.O. box system, for example, can be thought of as a namespace identifying personal or corporate names. In a given geographical region, the P.O. box number space is flat and centralized (i.e., controlled by one entity—the local Post Office). It is also proprietary; United Parcel Service (UPS), for example, does not offer P.O. box numbers compatible with the P.O. box numbers provided by the U.S. Postal Service. Furthermore, the P.O. box number space is a scarce, information-poor, publicly regulated, multi-purpose namespace that uses a contractual protection.