

# GOVERNANCE IN NAMESPACES<sup>†</sup>

*By Stefan Bechtold<sup>‡</sup>*

*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.<sup>1</sup>*

*Anyone can assign names.  
We each do that all the time.<sup>2</sup>*

*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.<sup>3</sup>*

## 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 an undue leverage for policy

---

<sup>†</sup> Version 3.0, September 2002.

<sup>‡</sup> Research Assistant, University of Tübingen Law School, Germany; J.S.M., 2002, Stanford Law School; Dr. iur. (J.S.D.), 2001, University of Tübingen Law School, Germany; Visiting Scholar, 1999 & 2000, University of California at Berkeley, School of Law (Boalt Hall); Referendar (J.D.), 1999, University of Tübingen Law School, Germany. The author thanks Peter Bechtold, Jonathan Greenberg, Jeff Gould, Kurt Jaeger, Lawrence Lessig, Nelson Minar, Wernhard Möschel, Milton Mueller, Markus Müller, Tomas Sander, and participants at workshops and seminars at Stanford Law School and the University of Tübingen Law School, Germany, for their valuable comments and suggestions. This research was made possible in part by a scholarship of the German Fulbright Commission. Comments to the author are most welcome and should be directed to stef@n-bechtold.com. His webpage is <http://www.jura.uni-tuebingen.de/~s-bes1>.  
<sup>1</sup> Jon Postel, *Assigned Numbers*, Request for Comments 776, at 1 (1981), at <http://www.rfc-editor.org/rfc/rfc776.txt>.

<sup>2</sup> Carl Ellison & Bruce Schneier, *Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure*, 16 (1) COMPUTER SECURITY JOURNAL 1, 2 (2000), <http://www.counterpane.com/pki-risks.pdf>.

<sup>3</sup> eBay, Inc., *Frequently Asked Questions About User IDs*, at <http://pages.ebay.com/help/basics/f-faq-UserId.html#9> (last visited Sept. 1, 2002).

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 the collection of all names in a particular system. Namespaces are ubiquitous. They can be found both in real and cyberspace. Namespaces analyzed in this paper 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. The paper also shows that many of its findings can be applied to namespaces outside of cyberspace – such as bibliographic classification schemes, P.O. boxes, Social Security numbers and the names of chemical compounds – as well.

Namespaces are an overlooked facet of governance both in real and cyberspace. This paper 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 paper 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 it is controlled by a public or a private entity, and how adaptive its internal structure is. These and other dimensions influence how namespaces protect social values, and how they allocate knowledge, control, and responsibility.

The taxonomic structure developed in the paper can be useful to legal and policy debates about the implications of various namespaces. It can also be helpful to designers of namespaces who think about the legal and policy consequences of what they are doing.

## TABLE OF CONTENTS

|  |           |
|--|-----------|
| <b>I. INTRODUCTION.....</b>                          | <b>3</b>  |
| <b>II. WHAT’S IN A NAME? .....</b>                   | <b>9</b>  |
| <b>III. DIMENSIONS OF NAMESPACE GOVERNANCE .....</b> | <b>13</b> |
| A. Mechanisms of Namespace Governance.....           | 13        |
| 1. Governance by Contract.....                       | 14        |
| 2. Governance by Technology .....                    | 17        |
| B. Governance by Whom? .....                         | 18        |

|   |           |
|---|-----------|
| C. Namespace Topology .....   | 21        |
| 1. Vertical Distribution of Namespaces .....                        | 21        |
| 2. Horizontal Distribution of Namespaces .....                      | 24        |
| a) Centralized Namespaces .....                                     | 24        |
| aa) Regulability .....  | 25        |
| bb) Privacy .....   | 26        |
| cc) Liability .....   | 27        |
| dd) Competition.....  | 27        |
| b) Federated Namespaces.....  | 28        |
| aa) Competition.....  | 28        |
| bb) Regulability.....   | 32        |
| cc) Privacy.....  | 33        |
| c) Decentralized Namespaces.....                                    | 34        |
| aa) Regulability .....  | 34        |
| bb) Liability and Privacy.....                                      | 35        |
| D. Intensity of Namespace Governance.....                           | 35        |
| 1. Control versus Coordination .....                                | 36        |
| 2. Control versus Uncoordination and Decentralized Innovation ..... | 37        |
| E. Scope of Namespace Governance .....                              | 43        |
| 1. Information-rich versus Information-poor Namespaces .....        | 43        |
| 2. Single-purpose versus Multi-purpose Namespaces .....             | 44        |
| a) Regulability .....   | 44        |
| b) Innovation around Namespaces .....                               | 44        |
| aa) Horizontally Innovation-friendly Namespaces .....               | 45        |
| bb) Vertically Innovation-friendly Namespaces .....                 | 45        |
| 3. Fixed versus Adaptive Internal Structure.....                    | 48        |
| a) Changing Number of Names.....                                    | 48        |
| b) Changing Kinds of Names .....                                    | 49        |
| <b>IV. IMPLICATIONS OF GOVERNANCE DIMENSIONS .....</b>              | <b>52</b> |
| A. Namespace Architectures Protect and Express Values .....         | 52        |
| B. Allocation of Knowledge, Control, and Responsibility .....       | 55        |
| <b>V. DESIGNING NAMESPACE GOVERNANCE.....</b>                       | <b>56</b> |
| <b>VI. CONCLUSION .....</b>   | <b>61</b> |

## 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 took place in the United States. It 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 had filed a lawsuit against voteauction.com, on October 18, 2000, the Circuit Court of Cook County, Illinois, issued an injunction against the web site. The U.S. registrar, who had registered the domain name, had been named as a co-defendant in the lawsuit. After the injunction was issued, the registrar cancelled the domain name, effectively shutting down the web site all over the world.

About a week later, the web site appeared again under the new domain name “vote-auction.com”. This time, the domain name had been registered with a Swiss registrar. A few days later, it was cancelled as well. However, no court had issued any injunction demanding the cancellation. No official authority had addressed the question 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 name space, to exclude this domain name from the Internet.<sup>4</sup>

In September 1998, a freshman at Northeastern University in Boston began working on a software program that would revolutionize online music business. Only two and a half years later, the Napster network had over 70 millions users who downloaded up to 2.8 billion music songs per month. 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.<sup>5</sup>

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. 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

---

<sup>4</sup> For more information on this case, see Henry H. Perritt, *Towards a Hybrid Regulatory Scheme for the Internet*, 2001 U. CHI. LEGAL F. 215, 241-244; RTMark, Inc., *Voteauction.com*, at <http://www.rtmark.com/voteauction.html> (last modified 2000); Voteauction, at <http://www.voteauction.at> (last visited Sept. 1, 2002).

<sup>5</sup> See *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001), *remanded* 2001 WL 227083 (N.D. Cal. 2001), *aff'd*, 284 F.3d 1091 (9th Cir. 2002).

control. Voteauction.com lost 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 an arcane concept of computer science, we are in fact surrounded by them. In the world of computers, the domain name system, public key infrastructures, Yahoo! Categories, Usenet newsgroups, and computer file systems all are 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.

Both Voteauction.com and Napster show 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.<sup>6</sup> The cultural and societal structure of those producing technology shape the technology itself.<sup>7</sup> 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.<sup>8</sup> Many design choices implicitly entail legal and policy choices.<sup>9</sup>

---

<sup>6</sup> 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., 1987).

<sup>7</sup> For an analysis of how the different cultures of early Internet users shaped the Internet, see CASTELLS, *supra* note 6, at 36-63.

<sup>8</sup> LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* (1999); see also Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 *TEX. L. REV.* 553 (1998); WILLIAM J. MITCHELL, *CITY OF BITS* 111-112 (1995). For an application of this theory in real space, see Neal K. Katyal, *Architecture as Crime Control*, 111 *YALE L.J.* 1039 (2002).

<sup>9</sup> This paper follows an approach that, for analytical purposes, distinguishes between a technology layer and a policy layer; see LESSIG, *supra* note 8; Reidenberg, *supra* note 8. 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 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 developed a layered analytical framework. In Benkler’s model, communication systems can be divided into the physical layer (the wires,

The particular design of a namespace determines its regulatory impact. Therefore, namespaces can be seen as a technological tool to implement certain policy goals and legal value systems into a network.

This paper analyzes the interrelation between technology and law for namespaces in general. It attempts to highlight a general 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.<sup>10</sup> By designing namespaces in a particular way, the implementation of many regulatory goals can be either achieved or prevented. As its analytical tools, the paper 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 or a single, narrowly defined purpose. It can be controlled by mere technical or, in addition, by contractual means. It can be administered by a public or a private entity. Although such decisions seem of technical nature, they are in fact closely intertwined with legal and policy decisions. The paper 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 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 in the Internet is the domain name system (DNS). Most computers connected to the Internet are equipped with a unique numerical IP address and a unique domain name.<sup>11</sup> 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 the

---

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 Yochai Benkler, *Property, Commons, and the First Amendment: Towards a Core Common Infrastructure* 3, at <http://www.law.nyu.edu/benklery/WhitePaper.pdf> (2001); see also Kevin Werbach, *A Layered Model for Internet Policy*, at <http://www.edventure.com/conversation/article.cfm?Counter=2414930> (2000); François Bar & Christian Sandvig, *Rules From Truth: Post-Convergence Policy for Access* 21, at [http://www.stanford.edu/~fbar/Publications/Rules\\_from\\_Truth.pdf](http://www.stanford.edu/~fbar/Publications/Rules_from_Truth.pdf) (2000); LAWRENCE LESSIG, *THE FUTURE OF IDEAS – THE FATE OF THE COMMONS IN A CONNECTED WORLD* 23-25 (2001).

<sup>10</sup> See MUELLER, *supra* note 9, at 10.

<sup>11</sup> Some computers are only equipped with an IP address, but not a domain name.

“Internet Corporation for Assigned Names and Numbers” (ICANN),<sup>12</sup> a private non-profit corporation under California law. The status of ICANN is highly disputed. While some proponents assert that ICANN is a mere technical standardization and coordination body, critics claim that it more resembles a world government.<sup>13</sup> Critics of ICANN argue 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.<sup>14</sup>

The DNS governance discussions are an example of the regulatory questions this paper addresses. However, this is not a paper about the governance of the domain name system. Although many issues addressed by this paper are known 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 which can be found in other namespaces – from peer-to-peer 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.

No literature exists that identifies and discusses governance dimensions of namespaces on such an abstract, general level. This article attempts to fill that gap. 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.<sup>15</sup> 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.<sup>16</sup> In communications law, common carrier regulations cope with adverse impacts of privately owned bottlenecks in the communication

---

<sup>12</sup> Internet Corporation for Assigned Names and Numbers, <http://www.icann.org> (Aug. 30, 2002).

<sup>13</sup> Milton Mueller has criticized the ICANN regime as “a conservative, corporatist regime founded on artificial scarcity and regulatory control”, MUELLER, *supra* note 9, at 267.

<sup>14</sup> *See id.*

<sup>15</sup> The telephone number space, the current IP address space, and the generic top level domain name space are examples of scarce namespaces. *See infra* note 168.

<sup>16</sup> *See* United States v. Terminal R.R. Ass’n, 224 U.S. 383 (1912).

infrastructure.<sup>17</sup> 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.<sup>18</sup> In First Amendment law, courts regularly have to allocate access to different types of mass media that are allegedly bottlenecks.<sup>19</sup> Finally, an emerging scholarship addresses specific regulatory problems of information and technology platforms, which can represent bottlenecks as well.<sup>20</sup>

While analyzing bottleneck situations is therefore nothing uncommon, this paper chooses a slightly different analytical approach. Rather than focusing on one specific area of law, it analyzes the implications of a particular technology – i.e. 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 law and legal policy have to grapple.

The purpose of this paper is twofold. First, the paper develops a uniform analytical framework under which a wide variety of namespaces can be assessed. Thereby, it highlights unifying features of technologies that are used in very different areas, yet lead to similar policy and legal implications. Secondly, the paper analyzes what the optimal design principles and architectures for namespaces may look like. Such findings may be important for legal, policy, and technical debates that deal with any of the existing namespaces.

---

<sup>17</sup> 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*, 53 FED. COMM. L.J. 91 (2000); Peter K. Pitsch & Arthur W. Bresnahan, *Common Carrier Regulation of Telecommunications Contracts and the Private Carrier Alternative*, 48 FED. COMM. L.J. 447 (1996).

<sup>18</sup> 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).

<sup>19</sup> See *Red Lion Broadcasting Co. v. FCC*, 395 U.S. 367 (1969); *Columbia Broadcasting, Inc. v. Democratic Nat’l Comm’n*, 412 U.S. 94 (1973); *CBS, Inc. v. FCC*, 453 U.S. 367 (1981); *Arkansas Educ. Television Comm’n (AETC) v. Forbes*, 523 U.S. 666 (1998); *Miami Herald Publ’g Co. v. Tornillo*, 418 U.S. 241 (1974); *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 656 (1994); *Turner Broad. Sys., Inc. v. FCC*, 520 U.S. 180 (1997); *Denver Area Educ. Telecommun. Consortium v. FCC*, 518 U.S. 727 (1996).

<sup>20</sup> See, e.g., Douglas Lichtman, *Property Rights in Emerging Platform Technologies*, 29 J. LEGAL STUD. 615 (2000); Philip J. Weiser, *Law and Information Platforms* (2002) (unpublished manuscript, on file with the author); Philip J. Weiser, *Networks Unplugged: Towards a Model of Compatibility Regulation Between Information Platforms* (2001), at <http://www.arxiv.org/html/cs/0109070>; Philip J. Weiser, *Internet Governance, Standard Setting, and Self-Regulation*, 28 N. KY. L. REV. 822, 832-842 (2001) (hereinafter Weiser, *Internet Governance*); Molly S. van Houweling, *Cultivating Open Information Platforms: A Land Trust Model* (2002) (unpublished manuscript, on file with the author); Bar & Sandvig, *supra* note 9; Pamela Samuelson & Susanne Scotchmer, *The Law & Economics of Reverse Engineering*, 111 YALE L.J. 1575, 1611, 1615-1626, 1643-1644, 1662 (2002). 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*, at <http://www.law.duke.edu/pd/papers/raieisen.pdf> (2001).

The paper proceeds as follows. In section 2, a more precise definition of namespaces is provided. Section 3 develops several dimensions of namespace governance that can be applied to namespaces in general. It shows the legal and policy implications of design decisions made along these dimensions. In section 4, a more abstract account of the relationship between namespace design and the law is provided. Section 5 demonstrates how these insights can be used in the actual design of namespaces. Section 6 concludes the paper.

## II. WHAT'S IN A NAME?

Names are important tools for identification and communication both in real and cyberspace. While it is clear that names play an important role in every society, this begs the question what a name actually is. From a legal and social science perspective, personal names are a crucial aspect of personal identity and dignity.<sup>21</sup> A complex mix of social norms, memories, connotations, and shared experiences influences the esteem of personal names, in particular first names.<sup>22</sup> From an economic perspective, commercial names and trademarks facilitate identification and thereby reduce consumer search costs.<sup>23</sup> 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.<sup>24</sup> In communication networks, some method to identify and locate the networked resources has to exist. Names provide such a method to facilitate sharing and communication.<sup>25</sup> They can bring consistency to the network: names uniquely identify resources, thereby eliminating the risk of confusion between different, but similar resources.

In fact, computer science has developed a rather rigorous theory of naming that proves helpful for the following analysis of namespaces.<sup>26</sup> In general, different kinds of names exist. An

---

<sup>21</sup> See Douglas A. Galbi, *A New Account of Personalization and Effective Communication* 4, at <http://papers.ssrn.com/abstract=286288> (2001).

<sup>22</sup> *Id.* 6.

<sup>23</sup> See William M. Landes & Richard A. Posner, *Trademark Law: An Economic Perspective*, 30 J.L. & ECON. 265, 269 (1987).

<sup>24</sup> *Id.* 184; David R. Cheriton & Timothy P. Mann, *Decentralizing a Global Naming Service for Improved Performance and Fault Tolerance*, 7 ACM TRANSACTIONS ON COMPUTER SYSTEMS 147 (1989); John F. Shoch, *Inter-Network Naming, Addressing, and Routing*, in PROCEEDINGS OF THE 17TH IEEE COMPUTER SOCIETY INTERNATIONAL CONFERENCE 72 (1978).

<sup>25</sup> See ROSS J. ANDERSON, *SECURITY ENGINEERING – A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS* 125 (2001).

<sup>26</sup> The most computer science research on naming has been conducted in so-called “distributed systems”. 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 (3rd ed. 2001); ANDREW S. TANENBAUM & MAARTEN VAN STEEN, *DISTRIBUTED SYSTEMS – PRINCIPLES AND PARADIGMS* 2 (2002). While

“address” is a special type of name that identifies the location of an object rather than the object itself.<sup>27</sup> The IP address of a computer and the number of a telephone are addresses in this sense. Addresses are not well suited to persistently identify objects. Once the object is moved to another location, its address changes. If a computer connected to the Internet, for instance, is moved to another location, often his IP address has to be changed as well.<sup>28</sup> 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,<sup>29</sup> a phone number does not identify a particular telephone, but its location, i.e. 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.<sup>30</sup> While addresses *locate* resources, location-independent names *identify* them.<sup>31</sup> 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”.<sup>32</sup> Name services allow users and software programs to look up, add, change, and remove names.<sup>33</sup> 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 and altered without any alteration of their name. The aforementioned domain name system (DNS) is a name service which resolves domain names to IP addresses.

---

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, *Naming and Binding of Objects*, in *OPERATING SYSTEMS – AN ADVANCED COURSE* 99-208 (Rudolf Bayer et al. eds., 1978).

<sup>27</sup> COULOURIS ET AL., *supra* note 26, at 354; see also Shoch, *supra* note 24, at 72; TANENBAUM & VAN STEEN, *supra* note 26, at 184.

<sup>28</sup> This problem is most prevalent with mobile computers, see TANENBAUM & VAN STEEN, *supra* note 26, at 184-185. URLs are another example of the shortcomings of addresses as consistent identifiers; see COULOURIS ET AL., *supra* note 26, at 356; see also *infra* note 212.

<sup>29</sup> On number portability, see *infra* note 150.

<sup>30</sup> TANENBAUM & VAN STEEN, *supra* note 26, at 185; Richard W. Watson, *Identifiers (naming) in distributed systems*, in *DISTRIBUTED SYSTEMS – ARCHITECTURE AND IMPLEMENTATION* 191, 196 (Butler W. Lampson et al. eds., 1981).

<sup>31</sup> “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 24, at 72.

<sup>32</sup> COULOURIS ET AL., *supra* note 26, at 357; TANENBAUM & VAN STEEN, *supra* note 26, 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 26, at 371; TANENBAUM & VAN STEEN, *supra* note 26, at 2.

<sup>33</sup> TANENBAUM & VAN STEEN, *supra* note 26, at 194.

Although a computer's IP address may have to be changed when its location is moved, its domain name can remain the same.

The collection of all valid names in a particular system forms a “namespace”.<sup>34</sup> 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 unambiguously resolvable.<sup>35</sup> In such a namespace, names have to be unique.<sup>36</sup>

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).<sup>37</sup> Device namespaces include the domain name system, the telephone number system, ENUM,<sup>38</sup> as well as IP and Ethernet addresses.<sup>39</sup> User namespaces are Microsoft Passport,<sup>40</sup> the Liberty Alliance Project,<sup>41</sup> public key infrastructures<sup>42</sup> as well as user identification systems on eBay, in the AOL network, and in instant messaging systems and networked computer games.<sup>43</sup> Uniform Resource Locators (URLs), peer-to-peer systems,<sup>44</sup> Yahoo! Categories and the different computer file systems available<sup>45</sup> are examples for file namespaces. Service namespaces are created, for instance, by TCP/UDP port numbers<sup>46</sup> and the “Universal Description, Discovery

---

<sup>34</sup> COULOURIS ET AL., *supra* note 26, at 358; Ronald Bourret, *XML Namespaces FAQ*, Answer 2.1, at [http://www.rpbouret.com/xml/NamespacesFAQ.htm#q2\\_1](http://www.rpbouret.com/xml/NamespacesFAQ.htm#q2_1) (last modified Aug. 2002); *see also* TANENBAUM & VAN STEEN, *supra* note 26, at 186. For a helpful proposition of a unified terminology for directories and namespaces, *see* Harald T. Alvestrand, *Definitions for Talking About Directories*, Request for Comments 3254, at <http://www.rfc-editor.org/rfc/rfc3254.txt> (2002).

<sup>35</sup> Saltzer, *supra* note 26, at 121; *see also* MUELLER, *supra* note 9, at 39.

<sup>36</sup> To achieve uniqueness, names are either universally valid, or they are equipped with a representation of the context in which they are unique; *see* Needham, *supra* note 26, at 315.

<sup>37</sup> *See* COULOURIS ET AL., *supra* note 26, at 356; TANENBAUM & VAN STEEN, *supra* note 26, at 184; Cheriton & Mann, *supra* note 24, at 147; Jerome H. Saltzer, *On the Naming and Binding of Network Destinations*, Request for Comments 1498, at <http://www.rfc-editor.org/rfc/rfc1498.txt> (1993); ANDERSON, *supra* note 25, at 131-132.

<sup>38</sup> *See infra* text accompanying notes 81-84.

<sup>39</sup> *See infra* text accompanying notes 170-178.

<sup>40</sup> *See infra* text accompanying notes 65-66.

<sup>41</sup> *See infra* text accompanying notes 139.

<sup>42</sup> *See infra* text accompanying notes 75-76.

<sup>43</sup> For a study of a virtual world computer game (Everquest), *see* Edward Castranova, *Virtual Worlds: A First-Hand Account of Market and Society on the Cyberian Frontier*, *Virtual Worlds: A First-Hand Account of Market and Society on the Cyberian Frontier*, 2 (1) THE GRUTER INSTITUTE WORKING PAPERS ON LAW, ECONOMICS, AND EVOLUTIONARY BIOLOGY (2001), at <http://www.bepress.com/giwp/default/vol2/iss1/art1/>.

<sup>44</sup> *See infra* text accompanying notes 115.

<sup>45</sup> 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 26, at 575-646.

<sup>46</sup> *See infra* text accompanying notes 179-181.

and Integration” (UDDI) service.<sup>47</sup> Some technologies even use several namespaces. Digital rights management (DRM) systems, for example, employ device, user, and file namespaces at the same time.<sup>48</sup> The list of namespaces used by computers and computer networks is endless.<sup>49</sup>

In real space, telephone, credit card, bank account, passport and Social Security numbers as well as tax identifiers are namespaces to 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.<sup>50</sup> The Dun & Badstreet Data Universal Numbering System (D-U-N-S) is used to identify 62 million business entities around the world,<sup>51</sup> while the Thomas Register of American Manufacturers provides unique supplier IDs for over 173,000 U.S. and Canadian manufacturers.<sup>52</sup> The worldwide system of bar codes that is used for product identification is another example how widely namespaces are used today.<sup>53</sup> Traditional media can be identified by different namespaces such as the

---

<sup>47</sup> UDDI.org, <http://www.uddi.org> (last visited Sept. 1, 2002). UDDI enables organizations that develop web services to register these services in a public database so that client applications can locate and use these services. For an overview of UDDI, see DAVID CHAPPELL, UNDERSTANDING .NET – A TUTORIAL AND ANALYSIS 65-71 (2002); THUAN THAI & HOANG Q. LAM, .NET FRAMEWORK ESSENTIALS 155-157 (2nd ed. 2002); ETHAN CERAMI, WEB SERVICES ESSENTIALS 18, 157-199 (2002).

<sup>48</sup> 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, Stefan Bechtold, *From Copyright to Information Law – Implications of Digital Rights Management, in Security and Privacy in Digital Rights Management* 213, 214-216 (Tomas Sander ed., 2002), available at [http://www.jura.uni-tuebingen.de/~s-bes1/pub/2002/DRM\\_Information\\_Law.pdf](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).

<sup>49</sup> Other computer namespaces include variable names in computer languages, character sets, the X.500 directory service, XML namespaces, colorspace 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 modified Apr. 18, 2002).

<sup>50</sup> 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 namespaces in the travel industry are administered by the International Air Transport Association, e.g. the “Travel Industry Designator Service”, see <http://www.iata.org/tids/>. See also Rohit Khare, *Anatomy of a URL (and Other Internet-Scale Namespaces, Part 1)*, 3 (5) IEEE INTERNET COMPUTING 78, 80 (1999).

<sup>51</sup> See Dun & Badstreet, at <http://www.dnb.com/english/duns> (last visited Sept. 1, 2002).

<sup>52</sup> See Thomas Register, at <http://www.thomasregister.com> (last visited Sept. 1, 2002).

<sup>53</sup> For information on the “Universal Product Code” (UPC) and the “European Article Number” (EAN), see UCC, at <http://www.uc-council.org> (2002) and EAN International, at <http://www.ean-ucc.org> (2002). The Auto-ID project at MIT attempts to extend this model by “electronic Product Codes” (ePC) that can be imbedded into smart tags and resolved by an “Object Naming Service”, see Auto-ID Center, at <http://www.autoidcenter.org> (last visited Sept. 1, 2002).

“International Standard Book Number” (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).<sup>54</sup> Bibliographic classification schemes,<sup>55</sup> the frequency spectrum, the various international classification systems for classifying inventions, trademarks and industrial designs,<sup>56</sup> the ISO 3166 list of country codes<sup>57</sup> as well as the names of all chemical compounds<sup>58</sup> may conclude this listing of namespaces. To put it short: namespaces are important and ubiquitous.

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

### **III. DIMENSIONS OF NAMESPACE GOVERNANCE**

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

#### **A. Mechanisms of Namespace Governance**

In general, namespace providers have various interests to regulate 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. Such regulation can be

---

<sup>54</sup> For an overview, see BECHTOLD, VOM URHEBER- ZUM INFORMATIONSRECHT, *supra* note 48, at 39-41.

<sup>55</sup> See *infra* text accompanying note 221.

<sup>56</sup> Four international classification systems are administered by the World Intellectual Property Organization (WIPO), see World Intellectual Property Organization, *International Classifications at WIPO*, at <http://www.wipo.org/classifications/en> (last visited Sept. 1, 2002).

<sup>57</sup> See ISO 3166 Maintenance Agency, at <http://www.iso.org/iso/en/prods-services/iso3166ma/index.html> (last visited Sept. 1, 2002).

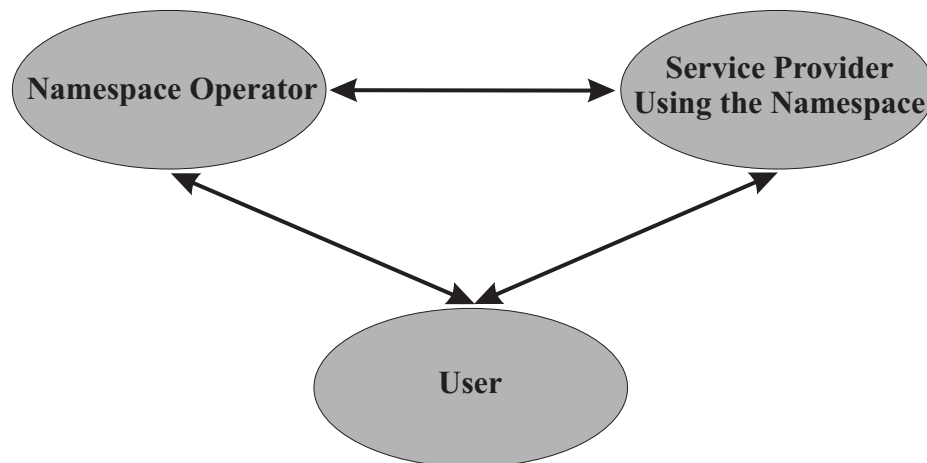
<sup>58</sup> See *infra* text accompanying note 231.

achieved by different mechanisms. 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 on the prior conclusion of a contract. Namespace contracts do not only include agreements about technical issues. They may limit the ways by which a namespace can be accessed. They may also restrict for what purposes and under what conditions it can be accessed. Furthermore, they may restrict in what environments 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 domain name system (DNS),<sup>59</sup> for example, uses such a web of contracts to govern the domain name space. All registrants, registrars and registries of domain names in generic top level domains (gTLDs) such as .com, .biz, .net, and .org have to enter into contractual

---

<sup>59</sup> 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 9; 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 & 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).

agreements that either directly or indirectly originate from the Internet Corporation for Assigned Names and Numbers (ICANN), the entity that currently controls the DNS.<sup>60</sup> In order to solve conflicts between domain name registrations and trademark law, ICANN, after considerable input from the World Intellectual Property Organization (WIPO), created a dispute resolution mechanism. This “Uniform Dispute Resolution Policy” (UDRP)<sup>61</sup> enables trademark holders to challenge the registration of a domain name and potentially gain control over it. In the contracts between ICANN and the gTLD registrars,<sup>62</sup> ICANN requires the registrars to impose the UDRP on everyone who wants to register a domain name.<sup>63</sup> Thereby, on the one hand, ICANN binds all registrars to the UDRP as a condition of their accreditation. On the other hand, every consumer who wants to register a domain name under the .com TLD, for example, will only be able to register it if he agrees to the terms of the UDRP as well. Through a hierarchical web of contracts that originates from ICANN, ICANN has achieved that every registrar and every registrant is bound to the UDRP.<sup>64</sup> ICANN has effectively laid a web of contracts on top of the domain name space that is used to protect, among other things, interests of trademark holders.

Another example of contractual webs as a means of namespace governance is Microsoft Passport.<sup>65</sup> 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

---

<sup>60</sup> See A. Michael Froomkin & Mark A. Lemley, *ICANN and Antitrust* 13-14, at <http://papers.ssrn.com/abstract=291221> (2001). This contractual web does not exist for country-code top level domains (ccTLDs). The relationship between ICANN’s overall governance of the domain name space 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 9, at 205-208; Tamar Frankel, *The Managing Lawmaker in Cyberspace: A New Power Model*, 27 *BROOK. J. INT’L L.* 859, 886-893 (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 9, at 197; Froomkin & Lemley, *ICANN and Antitrust* 11-13; Froomkin, *supra* note 59, at 91, 105-125.

<sup>61</sup> See Internet Corporation for Assigned Names and Numbers, *Uniform Domain-Name Dispute-Resolution Policy*, at <http://www.icann.org/udrp/udrp.htm> (last revised Aug. 26, 2001).

<sup>62</sup> For many country-code top-level domains (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 is the case, e.g., in Germany. In other namespaces such as the telephone number space, no UDRP equivalent exists either; see *In the Matter of Toll Free Service Access Codes*, 13 F.C.C.R. 9058 ¶ 22 (FCC 1998).

<sup>63</sup> Internet Corporation for Assigned Names and Numbers, *Registrar Accreditation Agreement* § II.K, at <http://www.icann.org/nsi/icann-raa-04nov99.htm> (Nov. 4, 1999).

<sup>64</sup> See MUELLER, *supra* note 9, at 192.

<sup>65</sup> Microsoft .NET Passport, at <http://www.passport.com> (last visited Sept. 1, 2002).

Passport will provide the participating web site with the necessary authentication information.<sup>66</sup>

In order to ensure that participating web sites do not use this authentication information for data mining and user profiling purposes, Microsoft has laid a web of contracts on top of the technical namespace. 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<sup>67</sup> format.<sup>68</sup>

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 has to agree to the "Microsoft Passport Terms of Use and Notices".<sup>69</sup> In this user contract, Microsoft agrees to use personal information only in accordance with its Passport privacy policy. According to this policy,

---

<sup>66</sup> User namespaces such as Microsoft Passport therefore enable a so-called "single sign-on" (SSO); see Microsoft Corp., *.NET Passport Review Guide – The Why, What, and How of Microsoft .NET Passport* 4-5, at <http://microsoft.com/net services/ passport/passport.asp> (March 2002). With more than 200 million accounts performing more than 3.5 billion authentications each month, Passport is currently the prevailing general authentication system; see <http://www.microsoft.com/net services/ passport/overview.asp>.

<sup>67</sup> The Platform for Privacy Preferences (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 World Wide Web Consortium, *Platform for Privacy Preferences*, at <http://www.w3.org/P3P> (last revised July 10, 2002); Ruchika Agrawal, *P3P – An Objective Overview*, at <http://www.stanford.edu/~ruchika/P3P> (last revised March 11, 2002).

<sup>68</sup> Microsoft Corp., *supra* note 66, at 26-27. 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. 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]", see Margaret J. Radin, *Humans, Computers, and Binding Commitment*, 75 IND. L.J. 1125, 1132 (2000).

<sup>69</sup> Microsoft Corp., *Microsoft Passport Terms of Use and Notices*, at <http://www.passport.com/Consumer/ TermsOfUse.asp> (last revised Aug. 1, 2001). 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 Systems, Inc. v. Wyse Technology*, 939 F.2d 91, 98-100 (3rd Cir. 1991); *Arizona Retail Systems, Inc. v. Software Link, Inc.*, 831 F. Supp. 759, 764-766 (D. Ariz. 1993); see also *Novell, Inc. v. Network Trade Center, Inc.*, 25 F.Supp.2d 1218 (D.Utah 1997), *vacated in part by Novell, Inc. v. Network Trade Center, Inc.*, 187 F.R.D. 657 (D.Utah 1999); *Morgan Laboratories, Inc. v. Micro Data Base Systems, Inc.*, 41 U.S.P.Q.2d 1850 (N.D. Cal. 1997). However, in 1997, Judge Easterbrook of the 7th Circuit Court of Appeals found a shrink-wrap a valid contract, *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1450-1453 (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., Inc. v. Timberline Software Corp.*, 998 P.2d 305, 313 (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 *Lan Systems, Inc. v. Netscout Service Level Corp.*, 183 F.Supp.2d 328, 338-339 (D.Mass. 2002); *Steven J. Caspi, et al. v. The Microsoft Network, L.L.C.*, 732 A.2d 528 (N.J.Super.A.D. 1999); see also *Specht v. Netscape Communications Corp.*, 150 F.Supp.2d 585, 594-595 (S.D.N.Y. 2001); *Groff v. America Online, Inc.*, 1998 WL 307001 (RI Superior Court, May 27, 1998).

Microsoft discloses personal information only if the user has consented or if Microsoft is required to disclose information by law.<sup>70</sup>

As ICANN did in the DNS context, Microsoft has laid a web of contracts on top of its user namespace Passport. This web is used by Microsoft to regulate non-technical, in particular privacy-related aspects of its namespace. This is not to say that privacy is perfectly or even adequately protected in Microsoft Passport.<sup>71</sup> This example merely reinforces the claim that contractual webs are used by namespace providers 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. Digital rights management systems<sup>72</sup> use similar mechanisms. In general, webs of contracts on top of namespaces bind both service providers that depend on the namespace and individual namespace users. They can be used by namespace providers 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 very promising means of namespace governance if the contracts would be hard to enforce in reality. In namespaces, however, it is 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 über-efficient manner. The technical control over a namespace can be used by the namespace provider as leverage for policy and legal control.

This feature can be observed in most namespaces. As was described above,<sup>73</sup> ICANN allows domain name registries, registrars and registrants to enter the domain name space only after

---

<sup>70</sup> 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 revised May 2002).

<sup>71</sup> See *infra* text accompanying notes 119-122.

<sup>72</sup> 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 48, at 217-222, 227.

<sup>73</sup> See *supra* text accompanying notes 60-64.

they have agreed to certain contractual obligations. ICANN's web of contracts can be enforced by the technical control over the domain name space, 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 way: through technology.<sup>74</sup>

Public key infrastructures (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.<sup>75</sup> They are a cornerstone of contemporary computer security architectures. 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.<sup>76</sup> 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.<sup>77</sup> Digital rights management systems use various key revocation techniques to achieve the same goal.<sup>78</sup> In general, technology enables the namespace provider to control which names get assigned, modified and revoked in a namespace. It is the most important governance tool in namespaces.

## **B. Governance by Whom?**

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

---

<sup>74</sup> See MUELLER, *supra* note 9, at 191, 232-234. The combination of technological and contractual protection is a common feature in such diverse areas of Internet law as the DNS, digital rights management, 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 48, at 439-448; Bechtold, *From Copyright to Information Law*, *supra* note 48, at 230.

<sup>75</sup> See Radia Perlman, *An Overview of PKI Trust Models*, 13 (6) IEEE NETWORK 38 (Nov./Dec. 2000).

<sup>76</sup> See RUSS HOUSLEY & TIM POLK, PLANNING FOR PKI 107-124 (2001).

<sup>77</sup> See *supra* text accompanying note 3.

<sup>78</sup> BECHTOLD, VOM URHEBER- ZUM INFORMATIONSRECHT, *supra* note 48, at 26-31; Bechtold, *From Copyright to Information Law*, *supra* note 48, at 215.

The ICANN debate is a prime example of this governance dimension. To what extent ICANN should exercise control over the domain name space and what accountability structures are appropriate, is fiercely contested in Internet policy circles.<sup>79</sup> ICANN's Uniform Dispute Resolution Policy (UDRP) has come under criticism for being biased towards the interests of trademark holders.<sup>80</sup> ICANN, a private non-profit corporation under California law, has been accused of creating a new body of international, but private trademark law that lacks any of the accountability structures under which traditional statutes operate.<sup>81</sup>

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.<sup>82</sup> 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.<sup>83</sup>

---

<sup>79</sup> See MUELLER, *supra* note 9, at 192; Froomkin, *supra* note 59; Froomkin & Lemley, *supra* note 60, at 19-21; Jonathan Weinberg, *ICANN and the Problem of Legitimacy*, 50 DUKE L.J. 187 (2000); Jonathan Zittrain, *ICANN: Between the Public and the Private*, 14 BERKELEY TECH. L.J. 1071 (1999); Kesan & Shah, *supra* note 59; 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](http://www.markle.org/news/ICANN_fin1_9.pdf); Gillian K. Hadfield, *Privatizing Commercial Law: Lessons from ICANN*, 6 J. SMALL & EMERGING BUS. L. 257 (2002); Edward Brunet, *Defending Commerce's Contract Delegation of Power to ICANN*, 6 J. SMALL & EMERGING BUS. L. 1 (2002); 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).

<sup>80</sup> See Michael Geist, *Fair.com? An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP*, 27 BROOK. J. INT'L L. 903 (2002); Milton Mueller, *Rough Justice – An Analysis of ICANN's Uniform Dispute Resolution Policy*, at <http://dcc.syr.edu/roughjustice.pdf> (2000); 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>; but see Annette Kur, *UDRP*, at <http://www.intellecprop.mpg.de/Online-Publikationen/2002/UDRP-study-final-02.pdf> (2002). For general analyses of the UDRP, see 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); Luke A. Walker, *ICANN's Uniform Domain Name Dispute Resolution Policy*, 15 BERKELEY TECH. L.J. 289 (2000); Froomkin, *supra* note 59, at 96-101; 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); A. Michael Froomkin, *ICANN's "Uniform Dispute Resolution Policy" – Causes and (Partial) Cures*, 67 BROOKLYN L. REV. 605 (2002); Elizabeth G. Thornburg, *Fast, Cheap, and Out of Control: Lessons from the ICANN Dispute Resolution Process*, 6 J. SMALL & EMERGING BUS. L. 191 (2002); UDRPlaw.net, at <http://www.udrplaw.net> (last revised Aug. 29, 2002); UDRPinfo.com, at <http://www.udrpinfo.com> (last visited Sept. 1, 2002). For an analysis of the UDRP under antitrust aspects, see Froomkin & Lemley, *supra* note 60, at 50-52.

<sup>81</sup> See Thornburg, *supra* note 80, at 208; Froomkin, *supra* note 80, at 612.

<sup>82</sup> Craig McTaggart, *E Pluribus ENUM: Unifying International Telecommunications Networks and Governance 2*, at <http://www.arxiv.org/ftp/cs/papers/0109/0109091.pdf> (2001). 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 2916, at <http://www.rfc-editor.org/rfc/rfc2916.txt> (Sept. 2000); Internet Engineering Task Force, *Telephone Number Mapping (enum) Charter*, at <http://www.ietf.org/html.charters/enum-charter.html> (last revised May 6, 2002); Washington Internet Project, *ENUM*, at <http://www.cybertelecom.org/dns/enum.htm> (last revised July 23, 2002); International Telecommunication Union, *ENUM*, at <http://www.itu.int/osg/spu/infocom/enum> (last revised Aug. 29, 2002).

<sup>83</sup> ENUM assigns each telephone number a unique domain name. The phone number +1 (555) 497-2815, e.g., 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 IETF ENUM working group determined that ENUM numbers would equal telephone numbers,

The DNS then performs a name lookup and returns personal contact information such as telephone numbers, email addresses, or fax numbers.<sup>84</sup> 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, email, fax, WWW pages, voicemail and instant messaging.<sup>85</sup> With ENUM’s interconnection of the domain names space 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<sup>86</sup> to the International Telecommunication Union (ITU). The discussion how the ENUM device namespace should be governed oscillates between these two extremes.<sup>87</sup>

Whereas the DNS and ENUM device namespaces are governed by hybrid entities, the IP<sup>88</sup> and Ethernet address,<sup>89</sup> Microsoft Passport,<sup>90</sup> P2P,<sup>91</sup> and TCP/UDP port number<sup>92</sup> namespaces

---

Robert Cannon, *ENUM: The Collision of Telephony and DNS Policy* 5, 14-17, at <http://papers.ssrn.com/abstract=287492> (2001). See also 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); Faltstrom, RFC 2916, *supra* note 82, at 2.

<sup>84</sup> Cannon, *supra* note 83, at 4; McTaggart, *supra* note 82, at 5. Therefore, ENUM competes with other discovery services for personal information; one competitor might be Microsoft .NET My Services, *see id.* 23.

<sup>85</sup> Cannon, *supra* note 83, at 2; Autorité de Régulation des Télécommunications, *Principles and Conditions for Implementation of an ENUM Protocol in France* 7, <http://www.art-telecom.fr/publications/syntconsenum-ang.doc> (2001).

<sup>86</sup> See ELI M. NOAM, INTERCONNECTING THE NETWORK OF NETWORKS 204-205 (2001).

<sup>87</sup> 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* Cannon, *supra* note 83, at 7-8, 24-26; *The History and Context of Telephone Number Mapping (ENUM) Operational Decisions*, Request for Comments 3245, at 7-8 (John C. Klensin ed., 2002), at <http://www.rfc-editor.org/rfc/rfc3245.txt>; Hwang et al., *supra* note 83, at 4-5; Autorité de Régulation des Télécommunications, *supra* note 85, at 12-13; Roy Blane, *Liaison to IETF/ISOC on ENUM*, Request for Comments 3026, at 2 (2001), at <http://www.rfc-editor.org/rfc/rfc3026.txt>; 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 83, at 22.

<sup>88</sup> 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 2050, at 4 (1996), at <http://www.rfc-editor.org/rfc/rfc2050.txt>. For an explanation of IP addresses, *see infra* text accompanying notes 170-177.

<sup>89</sup> The 802 Committee of the Institute of Electrical and Electronics Engineers (IEEE) standardized the Ethernet system. IEEE still controls the Ethernet address space. Ethernet addresses – officially called “Ethernet Unique Identifiers” (EUI) – are administered by the IEEE Registration Authority, <http://standards.ieee.org/regauth> (last revised June 4, 2002). For an explanation of Ethernet addresses, *see infra* text accompanying note 178.

<sup>90</sup> 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 that they could develop the passport system in exchange for a piece of every transaction ... there was a recognition of the importance of

all are examples of namespaces that are subject to purely private governance. Bibliographic classification schemes, which are namespaces as well,<sup>93</sup> are usually either sponsored by governments or by private consortiums of interested parties and users.<sup>94</sup> PKI systems are another example of namespaces where the whole spectrum – from publicly governed to hybrid and purely privately governed namespaces – exist. Who is governing a namespace determines in part what values and whose interests are protected by the namespace.

## C. Namespace Topology

The topology of namespaces may be the most important governance dimension in namespaces.<sup>95</sup> 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 subsection will illustrate.<sup>96</sup>

### 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).<sup>97</sup>

---

neutral, commons-like, infrastructures upon which others could build neutrally”, <http://slashdot.org/article.pl?sid=01/12/21/155221> (Dec. 21, 2001).

<sup>91</sup> See *infra* text accompanying note 145.

<sup>92</sup> See *infra* text accompanying note 179-181.

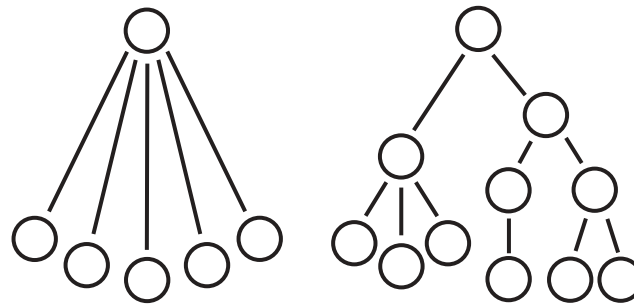
<sup>93</sup> See *infra* text accompanying notes 221.

<sup>94</sup> 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).

<sup>95</sup> In general, the study of a network’s topology is concerned with the manner in which the network nodes are interconnected, ROSHAN L. SHARMA, NETWORK TOPOLOGY OPTIMIZATION 8 (1990).

<sup>96</sup> Parts of the following analysis build upon the overview of different distributed systems topologies by Nelson Minar, *Distributed Systems Topologies*, at [http://www.oreillynet.com/pub/a/p2p/2001/12/14/topologies\\_one.html](http://www.oreillynet.com/pub/a/p2p/2001/12/14/topologies_one.html) (part 1); [http://www.oreillynet.com/pub/a/p2p/2002/01/08/p2p\\_topologies\\_pt2.html](http://www.oreillynet.com/pub/a/p2p/2002/01/08/p2p_topologies_pt2.html) (part 2) (2001-2002). 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, multidrop topology, directed link topology, star topology, ring topology, and bus topology; see DOUGLAS E. COMER, COMPUTER NETWORKS AND INTERNETS 103-105 (3rd ed., 2001); SHARMA, *supra* note 95, at 8-13; see also PRISCILLA OPPENHEIMER, TOP-DOWN NETWORK DESIGN 121-155 (1999).

<sup>97</sup> See Shoch, *supra* note 24, at 75-76.



**Figure 2: Flat versus Hierarchical Namespaces**<sup>98</sup>

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. Flat namespaces can be easily regulated, be it by the namespace provider, by the government, or by hackers.<sup>99</sup> Flat namespaces also have a single point of knowledge:<sup>100</sup> 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.<sup>101</sup> Rather, different parts of the namespace can be managed by different entities,<sup>102</sup> and, occasionally, governed by different policies.<sup>103</sup> Hierarchical namespaces therefore enable some competition to occur within the namespace.

The DNS may exemplify this governance dimension. The DNS is no monolithic system. Rather, it consists of a hierarchically organized network of databases (operated by a network

<sup>98</sup> This figure has been adopted from Minar, *supra* note 96.

<sup>99</sup> 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), at <http://www.cs.dartmouth.edu/~pkilab/papers/vh.pdf> (May 17, 2002).

<sup>100</sup> *Cf.* Watson, *supra* note 30, at 207.

<sup>101</sup> Nevertheless, even in a hierarchical namespace, the root node at the top of the hierarchy retains important regulatory power over the whole namespace. *See also infra* text accompanying notes 258-259.

<sup>102</sup> 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 920 (1984), at <http://www.rfc-editor.org/rfc/rfc1984.txt>.

<sup>103</sup> COULOURIS ET AL., *supra* note 26, at 358; Internet Corporation for Assigned Names and Numbers, *A Unique, Authoritative Root for the DNS*, ¶ 1, at <http://www.icann.org/icp/icp-3.htm> (2001). 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 (2nd ed. 2002); Perlman, *supra* note 75, at 41.

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 country-code top level domain (ccTLD) registries, for example, do not impose ICANN’s UDRP onto domain name registrars and registrants.<sup>104</sup> To some extent, responsibility for assigning domain names and for maintaining the name service is distributed throughout the hierarchical DNS network.<sup>105</sup> Thereby, the decision what policies are appropriate for governing the domain name space is decentralized to some extent. This decentralization in deciding policy issues could only be achieved by making a technical decision at the design stage of the DNS: to choose a hierarchical structure as the DNS’ topology.

ENUM,<sup>106</sup> IP addresses,<sup>107</sup> and the Library of Congress bibliographic classification are further examples of hierarchical namespaces.<sup>108</sup> Conversely, Microsoft Passport and TCP/UDP port numbers are flat namespaces. In PKI systems, both flat and hierarchical namespaces exist.<sup>109</sup>

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.<sup>110</sup> In other namespaces, although different providers occur within the hierarchy, the provider at the top of the hierarchy – the “root” – exercises considerable control over the whole namespace

---

<sup>104</sup> See *supra* note 62.

<sup>105</sup> See MUELLER, *supra* note 9, at 6.

<sup>106</sup> IETF has proposed to structure the ENUM namespace according to a hierarchical model (so-called “golden tree” architecture), see Anthony Rutkowski, *The ENUM Golden Tree*, 3 (2) INFO 97 (April 2001), [http://www.ngi.org/enum/pub/info\\_rutkowski.pdf](http://www.ngi.org/enum/pub/info_rutkowski.pdf); Faltstrom, RFC 2916, *supra* note 82, at 4. On top of this hierarchy lies a single international database (“tier 0”) that points to 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 83, at 7; McTaggart, *supra* note 82, at 8. See also *supra* note 87.

<sup>107</sup> The IP address space is administered by a pyramid of authorities, consisting of IANA at the top and of regional IP registries at the bottom of the pyramid. Namespace responsibility is distributed across this pyramid. See Hubbard et al., *supra* note 88, at 3-4.

<sup>108</sup> For an argument against the popular belief that the telephone system is a strictly hierarchical namespace see Rutkowski, *supra* note 106.

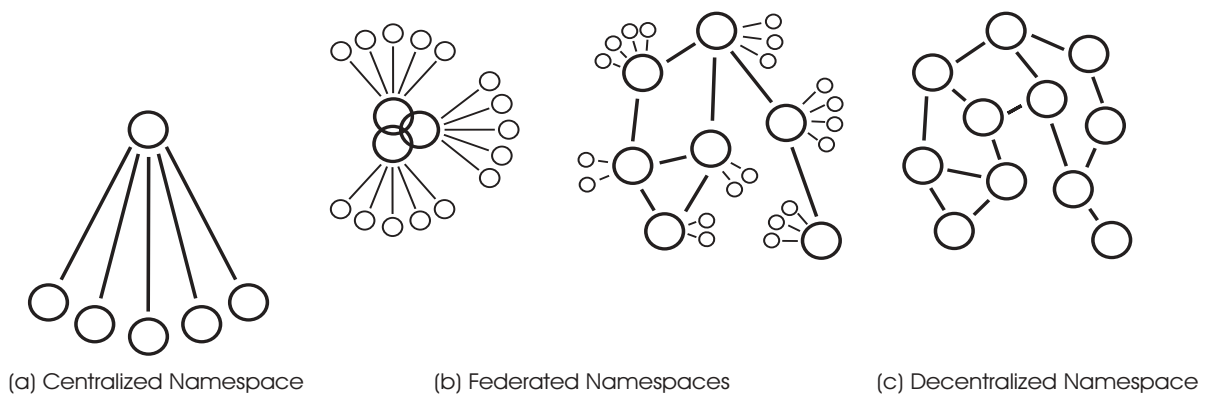
<sup>109</sup> See Perlman, *supra* note 75, at 38-42; HOUSLEY & POLK, *supra* note 76, at 54-55; KAUFMAN ET AL., *supra* note 103, at 372.

<sup>110</sup> In the Library of Congress Classification, e.g., it is the Library of Congress that exercises all the power in this – hierarchical – namespace, see RITA MARCELLA & ROBERT NEWTON, *A NEW MANUAL OF CLASSIFICATION* 87 (1994).

by technological or contractual means. This feature can be found in the domain name space<sup>111</sup> and in hierarchical PKI user namespaces.<sup>112</sup>

## 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 lie various forms of “federated” or interconnected namespaces (see figure 3). 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<sup>113</sup>**

### a) Centralized Namespaces

In a centralized namespace, a single entity provides the name service and thereby operates the full namespace.<sup>114</sup>

---

<sup>111</sup> 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 9, at 47-56. *See also infra* text accompanying notes 258-259.

<sup>112</sup> *See* Perlman, *supra* note 75, at 41.

<sup>113</sup> This figure was inspired by Minar, *supra* note 96.

<sup>114</sup> 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.

## aa) Regulability

Centralized namespaces have a single point of control that can be regulated. This is most obvious in centralized peer-to-peer (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.<sup>115</sup> In a P2P network, files can be shared among the participating peer computers without any intervention by a centralized server. In order to share files, however, the individual peer has to know where files are located in the network. Therefore, P2P networks need a namespace in which each file that is available in the network gets assigned to the address of the peer computer at which the file is located.

Early P2P systems used a centralized namespace for locating files in the network. Until Napster was shut down by a court order in 2001, for example, it used a centralized namespace that was located at a server operated by Napster.<sup>116</sup> P2P systems such as Napster have been criticized for facilitating mass-scale piracy. To suppress such piracy, record companies and other copyright holders have demanded that P2P network 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. For without the namespace, a peer computer can no longer locate any file in the P2P network.<sup>117</sup> A centralized namespace opens the system to regulation of various sorts: the government or courts may order that the namespace be shut down. Also, the namespace may

---

<sup>115</sup> ANDY ORAM, PEER-TO-PEER IX (2001); LESSIG, *supra* note 9, at 134; *see also* Beverly Yang & Hector Garcia-Molina, *Designing a Super-Peer Network 1*, at <http://dbpubs.stanford.edu:8090/pub/2002-13> (Feb. 22, 2002). For an overview of the P2P development, *see* ORAM. For an overview of the innovation enabled by P2P systems, *see* LESSIG, *supra* note 9, at 134-138.

<sup>116</sup> *See, e.g.*, Sylvia Ratnasamy et al., *A Scalable Content-Addressable Network* in: PROCEEDINGS OF THE SIGCOMM SYMPOSIUM 161 (2001). In contrast to the original P2P idea, in such a system some functionality – the name resolution – is centralized. Therefore, such systems are sometimes characterized as “hybrid” P2P systems, *see* Yang & Garcia-Molina, *supra* note 115, at 1; *see also* Lessig, *supra* note 9, at 135.

<sup>117</sup> In the Napster case, record companies achieved this result by prompting a court to order Napster to shut down its central namespace. The court required Napster to exclude files from its network that violated the plaintiff’s copyrights. By exercising control over its central namespace, Napster was able to exclude such files. 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 bare the burden to identify the files Napster should exclude, and what level of accuracy the employed filtering technologies needed to have. *See* A&M Records v. Napster, 239 F.3d 1004 (9th Cir. 2001), *remanded to* 2001 WL 227083 (N.D. Cal. 2001), *aff’d*, 284 F.3d 1091 (9th Cir. 2002).

be shut down by the namespace provider or by hackers.<sup>118</sup> Centralized namespaces are therefore prone to regulability.

## **bb) Privacy**

A centralized namespace is not only easy to regulate, it can also pose privacy risks. In a centralized namespace, all information about the namespace is located within one entity. This entity assigns names, it knows who is accessing the namespace, which names are looked up etc. 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 P2P system. Such information can be valuable data for surveillance, data mining, marketing and personalization purposes.

However, centralized namespaces can have ambivalent implications for privacy protection, as the Microsoft Passport user namespace exemplifies. Microsoft Passport is a centralized namespace as Microsoft is currently<sup>119</sup> the only provider of the namespace. User namespaces can theoretically be used to collect large amounts of personal data.<sup>120</sup> Microsoft Passport does not only store user names and corresponding passwords in its namespace database. If the user so chooses, it can also store the name of the user, credit card information, his address, as well as demographic or preference data such as gender, occupation, state, ZIP code, time zone, birthday, and language preference. Passport does not transmit such data to participating web sites without the user's consent.<sup>121</sup> Rather, as a default, Passport only transmits a 64 bit long unique user identifier to participating web sites.

Thereby, users can access third-party web sites – such as eBay or McAfee – without having to provide the web site any personal information such as the user's name, e-mail address, or phone number. The only service that possesses such information is Passport itself. Passport

---

<sup>118</sup> 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*, 6 (1) IEEE INTERNET COMPUTING 40, 44 (2002).

<sup>119</sup> For announcements of Microsoft to open Passport to competing authentication services, see *infra* text accompanying note 138.

<sup>120</sup> Indeed, after a complaint by privacy advocacy groups led by the Electronic Privacy Information Center (EPIC), the Federal Communication 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 the Matter of Microsoft Corporation*, File No. 0123240, 2002 WL 1836831 (FTC 2002), available at <http://www.ftc.gov/opa/2002/08/microsoft.htm>. In addition, the European Commission is investigating whether Microsoft Passport violates European privacy laws; see *Microsoft Faces European Commission Inquiry on Privacy Concerns*, N.Y. TIMES, May 28, 2002, at C4.

<sup>121</sup> Microsoft Corp., *supra* note 70.

does not transmit such information to any participating web sites without the user's consent.<sup>122</sup> 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. At the same time, centralizing data storage can also threaten privacy interests. 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, Passport is in a unique position to collect personal data. While Microsoft has promised not to engage in such practices, the particular technical design of the user namespace certainly does not prevent them.

Centralized namespaces may therefore 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 himself may misuse the stored information.

### **cc) 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, this single entity can be held responsible for the activities that 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 in the namespace.<sup>123</sup>

### **dd) Competition**

Designing namespaces in a centralized way also influences the competitive framework in which the namespaces operate. Namespaces are subject to network effects.<sup>124</sup> The more users

---

<sup>122</sup> *See id.*

<sup>123</sup> *See* A&M Records v. Napster, 239 F.3d 1004 (9th Cir. 2001), *remanded to* 2001 WL 227083 (N.D. Cal. 2001), *aff'd*, 284 F.3d 1091 (9th Cir. 2002).

<sup>124</sup> 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 (1985). The existence, importance, and impact of network effects is controversial on a theoretical as well

and service providers use a particular namespace, the larger and therefore more valuable the namespace becomes to them.<sup>125</sup> Therefore, in communication markets shaped by network effects, the optimal number of namespaces is often one. Network effects can lead to *de facto* standards, even to monopolies in a market.<sup>126</sup> 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.<sup>127</sup>

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 top level domains.<sup>128</sup> The refusal of AOL to interconnect its instant messaging systems<sup>129</sup> with competing systems can be explained by network effects as well.<sup>130</sup> If, in a market shaped by network effects, a centralized namespace is used, competing namespaces may effectively be driven out of the market.

## **b) Federated Namespaces**

### **aa) 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

---

as an empirical level; see Stan J. Liebowitz & Stephen E. Margolis, *Network Externality: An Uncommon Tragedy*, 8 (2) J. ECON. PERSP. 133, 149 (1994); Lemley & McGowan, *Legal Implications of Network Economic Effects*, 86 CAL. L. REV. 479, 485, 591, 601, 610 (1998); BECHTOLD, VOM URHEBER- ZUM INFORMATIONSRECHT, *supra* note 48, at 351-364. As Gerald Faulhaber correctly points out, in many communication networks, it is not the network itself that is subject to network effects, but rather the namespace that is underlying the network; Gerald Faulhaber, *Network Effects and Merger Analysis: Instant Messaging and the AOL-Time Warner Case*, 26 TELECOMMUNICATIONS POLICY 311, 317 (2002).

<sup>125</sup> 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 the one 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* 175-179 (1999); Lemley & McGowan, *supra* note 124, at 496-497.

<sup>126</sup> Michael L. Katz & Carl Shapiro, *Systems Competition and Network Effects*, 8 (2) J. ECON. PERSP. 93, 105 (1994).

<sup>127</sup> See SHAPIRO & VARIAN, *supra* note 125, at 104; OZ SHY, *THE ECONOMICS OF NETWORK INDUSTRIES* 4 (2001).

<sup>128</sup> For an overview of the debate on alternate DNS roots, see *infra* note 148.

<sup>129</sup> Instant messaging is a service that lets users communicate over the Internet with each other in real time. With its IM and ICQ systems, AOL Time Warner is the largest provider of instant messaging systems. Competitors 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. If an instant messaging provider decides to share access to his NPD with other providers, he makes his IM system interoperable or, in other words, federates his namespace; see *Consent to the Transfer of Licenses and Section 214 Authorizations by Time Warner, Inc. and America Online, Inc., Transferors, to AOL Time Warner, Inc., Transferee*, CS Docket No. 00-30, Memorandum Opinion and Order, 16 F.C.C.R. 6547 ¶ 138-139 (FCC 2001) (hereinafter AOL/TW Merger Order). For general information about instant messaging, see Faulhaber, *supra* note 124; Weiser, *Internet Governance*, *supra* note 20, at 842-846; James B. Speta, *A Common Carrier Approach to Internet Interconnection*, 54 FED. COMM. L.J. 225, 235-238 (2002).

<sup>130</sup> See Faulhaber, *supra* note 124, at 315-316, 324.

efficient than having several competing namespaces, then this is desirable.<sup>131</sup> 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.<sup>132</sup> Rather, namespaces can be opened to competitors. In such a scenario, several competitors offer competing namespace services that all adhere to one common standard. Open standards reduce the lock-in effects produced by network effects.<sup>133</sup> They shift the locus of competition from competing *for* the market to competing *within* the market, using common standards.<sup>134</sup> 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.<sup>135</sup>

Centralized namespaces can be opened to competition by introducing interoperability and interconnection between different namespace providers, i.e. by “federating” the namespace (see figure 3). Federating namespaces introduces competition into the namespace market.<sup>136</sup> It frees namespaces from proprietary control.

In a federated namespace, functions are horizontally distributed across several providers participating in the federation.<sup>137</sup> Microsoft Passport exemplifies the difference between a centralized and a federated namespace. Microsoft used to structure its Passport namespace as a proprietary service. Passport did not interoperate with other competing identification and authentication services. In such a centralized namespace, technical, economic, and policy control are exercised by one single entity. However, in September 2001, Microsoft announced that it would open Passport to other authentication systems. 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. For Passport would accept the authentication from the competing

---

<sup>131</sup> Lemley & McGowan, *supra* note 124, at 497.

<sup>132</sup> *Id.*

<sup>133</sup> *Id.* 516, 600; *see also* MUELLER, *supra* note 9, at 53.

<sup>134</sup> SHAPIRO & VARIAN, *supra* note 125, at 231.

<sup>135</sup> “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 standards ...”, Lemley & McGowan, *supra* note 124, at 599-600.

<sup>136</sup> *See* AOL/TW Merger Order, *supra* note 129, at ¶ 131.

<sup>137</sup> 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.

service and issue a Passport ticket for this user. In other words, Passport would translate the “foreign” identity into a Passport identity.<sup>138</sup> A different proposal for a federated user namespace was made in July 2002 by the Liberty Alliance Project.<sup>139</sup>

Further examples for federated namespaces are various public key infrastructures (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.<sup>140</sup> For centralized namespaces may stifle competition. Such problems can be prevented by using architectural approaches that enable federated PKI user namespaces. Bridge certification authorities,<sup>141</sup> oligarchy models,<sup>142</sup> “mesh architectures”<sup>143</sup> and various means of cross-certification<sup>144</sup> are different approaches to create one large federated PKI namespace.

---

<sup>138</sup> 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. For 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 Version 4, every authentication server had to register with every other authentication server. Due to scalability and performance problems, Kerberos Version 5 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*, 32 (9) IEEE COMMUNICATIONS MAGAZINE 33, 36 (1994); Ken Hornstein, *Kerberos FAQ, v. 2.0*, at <http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html#xrealm> (2000); Brian Tung, *The Moron’s Guide to Kerberos, Version 1.2.2*, at <http://www.isi.edu/gost/brian/security/kerberos.html#crossrealm> (1996); John T. Kohl et al., *The Evolution of the Kerberos Authentication Service*, in DISTRIBUTED OPEN SYSTEMS 78 (Frances M.T. Brazier & Dag Johansen eds., 1994).

<sup>139</sup> 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 for another time. See Liberty Alliance Project, *Liberty Architecture Overview 8-12* (Version 1.0), at <http://www.projectliberty.org/specs/liberty-architecture-overview-v1.0.pdf> (July 11, 2002).

<sup>140</sup> Perlman, *supra* note 75, at 39.

<sup>141</sup> See HOUSLEY & POLK, *supra* note 76, at 64-66; William T. Polk & Nelson E. Hastings, *Bridge Certification Authorities: Connecting B2B Public Key Infrastructures* 8-9, at <http://csrc.nist.gov/pki/documents/B2B-article.pdf> (2000); KAUFMAN ET AL., *supra* note 103, at 378.

<sup>142</sup> 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 Microsoft Corp., *Using Digital Certificates*, at <http://www.microsoft.com/windows/ie/using/howto/digitalcert/using.asp> (Sept. 7, 2001); Perlman, *supra* note 75, at 39; KAUFMAN ET AL., *supra* note 103, at 374; HOUSLEY & POLK, *supra* note 76, at 55-56. 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.

<sup>143</sup> 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 76, at 58-60; Marchesini & Smith, *supra* note 99, at 3-4; Polk & Hastings, *supra* note 141, at 5-7.

<sup>144</sup> In cross certification, one certification authority certifies another certification authority. Thereby, both certification namespaces become interconnected. See KAUFMAN ET AL., *supra* note 103, at 377; HOUSLEY & POLK, *supra* note 76, at 62-64.

Other examples of federated namespaces include interconnected telephone networks,<sup>145</sup> hybrid P2P systems,<sup>146</sup> as well as the discussions about interoperable instant messaging systems<sup>147</sup> and about root zone level competition in both the DNS<sup>148</sup> and ENUM.<sup>149</sup>

By creating interconnections between different namespaces, competition between the federated, interoperable namespaces becomes possible. A competing user authentication service, for example, may 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.

---

<sup>145</sup> Interconnection arrangements and mandates are tools to federate telephone namespaces. See NOAM, *supra* note 86; Mark Armstrong, *Network Interconnection in Telecommunications*, 108 THE ECONOMIC JOURNAL 545 (1998). In the Internet, interconnection between different networks is achieved by peering arrangements between backbone providers. See Jean-Jacques Laffont et al., *Internet Peering*, 91 AM. ECON. REV. PAPERS & PROC. 287 (2001); Stanley Besen et al., *Advances in Routing Technologies and Internet Peering Arrangements*, 91 AM. ECON. REV. PAPERS & PROC. 292 (2001). For a general analysis of interconnection problems on the Internet, see Speta, *supra* note 129.

<sup>146</sup> Hybrid P2P networks use a namespace architecture that lies between the both extremes of a centralized and a decentralized namespace. The FastTrack technology on which Grokster and KaZaA as well as the P2P system eDonkey are based uses such an approach. For more information, see Beverly Yang & Hector Garcia-Molina, *Comparing Hybrid Peer-to-Peer Systems 1*, at <http://dbpubs.stanford.edu:8090/pub/2001-37> (Oct. 8, 2001); Kelly Truelove & Andrew Chasin, *Morpheus Out of the Underworld*, at <http://www.openp2p.com/pub/a/p2p/2001/07/02/morpheus.html> (July 2, 2002); David E. Kendall & Jan B. Norman, *Complaint for Damages and Injunctive Relief for Copyright Infringement in MGM Studios v. Grokster*, ¶ 45, at [http://www.eff.org/IP/P2P/MGM\\_v\\_Grokster/20011002\\_mgm\\_v\\_grokster\\_complaint.pdf](http://www.eff.org/IP/P2P/MGM_v_Grokster/20011002_mgm_v_grokster_complaint.pdf) (2001).

<sup>147</sup> 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 – i.e. not federated – with unaffiliated systems; see AOL/TW Merger Order, *supra* note 129, at ¶ 325; see also Faulhaber, *supra* note 124; Weiser, *Internet Governance*, *supra* note 20, at 842-846; Speta, *supra* note 129, at 235-238. 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*, at [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/DA-02-1772A2.pdf](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*, CS Docket No. 00-30, Public Notice, 2002 WL 1610987 (FCC, July 23, 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) Charter, at <http://www.ietf.org/html.charters/apex-charter.html> (last revised October 12, 2001); Presence and Instant Messaging Protocol (prim) Charter, at <http://www.ietf.org/html.charters/prim-charter.html> (last revised July 31, 2001); SIP for Instant Messaging and Presence Leveraging (simple) Charter, at <http://www.ietf.org/html.charters/simple-charter.html> (last revised July 26, 2002).

<sup>148</sup> For an overview, see Milton Mueller, *Competing DNS Roots: Creative Destruction or Just Plain Destruction?* (2001), at <http://www.arxiv.org/ftp/cs/papers/0109/0109021.pdf>; see also Internet Architecture Board, *IAB Technical Comment on the Unique DNS Root*, Request for Comments 2826 (2000), at <http://www.rfc-editor.org/rfc/rfc2826.txt>; Internet Corporation for Assigned Names and Numbers, *A Unique, Authoritative Root for the DNS*, at <http://www.icann.org/icp/icp-3.htm> (July 9, 2001); Kent Crispin, *Alt-Roots, Alt-TLDs*, at <http://www.icann.org/stockholm/draft-crispin-alt-roots-tds-00.txt> (May 2001). For the history of this debate, see MUELLER, *supra* note 9, at 130-134, 148-149, 152-153.

<sup>149</sup> See Cannon, *supra* note 83, at 17-19; but see RFC 3245, *supra* note 87, at 2-3; McTaggart, *supra* note 82, at 10-14. For an overview of different architectural alternatives for ENUM's design, see Hwang et al., *supra* note 83, at 13-21.

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.<sup>150</sup> Furthermore, a federated namespace architecture only leads to competition if the providers actually do open their namespaces to competitors.<sup>151</sup>

## bb) 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. In a P2P system with such a namespace architecture,<sup>152</sup> for example, 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, in particular the efficiency of centralized namespaces with the robustness and lack of a single point of failure of decentralized namespaces.<sup>153</sup>

---

<sup>150</sup> A user of one federated namespace may have invested considerable time and efforts 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 this information attached to his old identity even though both namespaces are federated. This may deter the user to switch authentication systems in the first place, thereby impeding competition among authentication systems in the federation. 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 the Matter of Telephone Number Portability*, 11 F.C.C.R. 8352 (FCC. 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 (1) TELECOMMUNICATIONS POLICY 73 (1998); Joshua S. Gans et al., *Number to the People: Regulation, Ownership and Local Number Portability*, at <http://papers.ssrn.com/abstract=223189> (2000); Justus Haucap, *Telephone Number Allocation: A Property Rights Approach*, at <http://papers.ssrn.com/abstract=308003> (2002); but see Reiko Aoki & John Small, *The Economics of Number Portability: Switching Costs and Two-Part Tariffs*, at [http://www.crnec.auckland.ac.nz/research/papers/Aoki\\_Small.pdf](http://www.crnec.auckland.ac.nz/research/papers/Aoki_Small.pdf) (1999); NOAM, *supra* note 86, at 206-209.

<sup>151</sup> 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”, interview with Christopher Payne, Microsoft Vice President of the .NET Core Services Platform, at <http://www.microsoft.com/presspass/Features/2001/Sep01/09-20passport.asp> (Sept. 21, 2001). If the authentication system does not adhere to or enforce a comparable privacy policy, Microsoft could cut the connection between both authentication systems, *id.* While this may be a laudable procedure, it is important to note that, in 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 141, at 5. For the legal consequences in the PKI context, see Michael S. Baum & Warwick Ford, *Public Key Infrastructure Interoperation*, 38 JURIMETRICS J. 359 (1998).

<sup>152</sup> See *supra* note 146.

<sup>153</sup> Yang & Garcia-Molina, *supra* note 115, at 1-2.

## cc) Privacy

The partial decentralization in federated namespaces can be used to enhance the protection of privacy interests. In a centralized user namespace such as the current 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,<sup>154</sup> no globally unique ID exists that is tied to a particular identity provider.<sup>155</sup> 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 his identities can be linked together.<sup>156</sup> Even if two identities are linked together, however, no common identity exists. Both services remember the other's handle for the user and communicate with each other only with these handles.<sup>157</sup> This architecture enables the user to decide in a very fine-grained way which identities become linked together and which should stay separate. Thereby, the user can control which providers can exchange information about the user.<sup>158</sup>

Federated user namespaces can also be architected differently. One alternative approach would be to federate all namespaces in 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, he can control the dissemination of personal information across the namespace in a fine-grained way. Federating namespaces can enhance privacy protection as the overall namespace is effectively modularized.

---

<sup>154</sup> See *infra* text accompanying note 139.

<sup>155</sup> Liberty Alliance Project, *supra* note 139, at 22, 26.

<sup>156</sup> 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.* 23.

<sup>157</sup> See Liberty Alliance Project, *Liberty Protocols and Schemas Specification* 17 (Version 1.0), at <http://www.projectliberty.org/specs/liberty-architecture-protocols-schemas-v1.0.pdf> (July 11, 2002).

<sup>158</sup> 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 still are not able to exchange information about him. For the user has not created a federation between the two service provider identities. See Liberty Alliance Project, *supra* note 139, at 24, 26.

### c) Decentralized Namespaces

Whereas in a federated namespace, a small number of interconnected namespaces exists, in a totally 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.<sup>159</sup> 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.<sup>160</sup> The P2P system Gnutella<sup>161</sup> uses such architecture.<sup>162</sup> Other decentralized namespaces include encryption systems – such as the original PGP – that do not employ a structured PKI architecture, but rather a more anarchical model in which public keys are certified on a peer-to-peer basis.<sup>163</sup> Decentralized namespace possess interesting features regarding their regulability, privacy protection and the liability of the namespace “providers”.

#### aa) Regulability

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

---

<sup>159</sup> Arguably, the individual peers do not even need a distinct namespace as they can just search their hard disk; see Crespo & Garcia-Molina, *supra* note 146, at 2.

<sup>160</sup> 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 1960's, randomly selected individuals were asked to direct letters to a target person in another, distant city in the U.S. whom they did not know by forwarding the letter to a single friend. In 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 *SOCIOLOGY* 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, Peter S. Dodds & M. E. Newman, *Identity and Search in Social Networks*, 296 *SCIENCE* 1302 (2002).

<sup>161</sup> <http://www.gnutelliums.com> (last visited Sept. 1, 2002); Clip2, *The Gnutella Protocol Specification v0.4 Document Revision 1.2*, at [http://rfc-gnutella.sourceforge.net/Development/GnutellaProtocol0\\_4-rev1\\_2.pdf](http://rfc-gnutella.sourceforge.net/Development/GnutellaProtocol0_4-rev1_2.pdf) (2001); Gene Kan, *Gnutella* in: PEER-TO-PEER 94 (Andy Oram ed., 2001); Matei Ripenau et al., *Mapping the Gnutella Network*, 6(1) *IEEE INTERNET COMPUTING* 50 (2002).

<sup>162</sup> 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 161, at 105-106, 110; see also Fernando R. Bordignon & Gabriel H. Tolosa, *Gnutella: Distributed System for Information Storage and Searching* 5, at [http://www.gnutella.co.uk/library/pdf/paper\\_final\\_gnutella\\_english.pdf](http://www.gnutella.co.uk/library/pdf/paper_final_gnutella_english.pdf) (2001).

<sup>163</sup> In such a system, no trusted certification authority certifies the identity or integrity of any public key or individual person. Rather, the individual 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 Perlman, *supra* note 75, at 40; KAUFMAN ET AL., *supra* note 103, at 569.

## bb) Liability and Privacy

As no single entity exists that operates the namespace, liability for actions occurring within the namespace is scattered as well.<sup>164</sup> For there are only the individual users who could be held liable for any actions occurring within the namespace, but no central entities, as no such entities exist.

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.<sup>165</sup> Some of these networks are even designed with the explicit purpose to preserve privacy for information producers and consumers and resist censorship.<sup>166</sup> Surveillance of P2P systems with a fully decentralized namespace is an intricate task.<sup>167</sup> 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 harder, more expensive and more inefficient it becomes to make somebody liable for the actions occurring on the namespace, and the more competition it allows 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.

---

<sup>164</sup> See Kan, *supra* note 161, at 99; LESSIG, *supra* note 9, at 137.

<sup>165</sup> “With Gnutella, every router and cable on the Internet would need to be tapped to learn about transactions between Gnutella hosts or peers”, Kan, *supra* note 161, at 119.

<sup>166</sup> See Ian Clarke et al., *supra* note 118, at 41; 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). For other P2P systems that attempt to preserve anonymity, see Andrei Serjantov, *Anonymizing Censorship Resistant Systems*, at <http://www.cs.rice.edu/Conferences/IPTPS02/120.pdf> (2002); Qin Lv et al., *Can Heterogeneity Make Gnutella Scalable?*, at <http://www.cs.rice.edu/Conferences/IPTPS02/165.pdf> (2002).

<sup>167</sup> “... the only way to monitor what is happening on the Gnutella network is to monitor what is happening on the entire Internet”, Kan, *supra* note 161, at 118.

## 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, i.e. if it is a scarce namespace,<sup>168</sup> mechanisms have to exist to assign names in an efficient and resource-saving manner.<sup>169</sup> 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, not technical reasons.

A namespace that illustrates the difference in degree between control and coordination is the IP address space. As described above,<sup>170</sup> the DNS resolves domain names into IP addresses. IP addresses form a distinct namespace that is administered by the “Internet Assigned Numbers Authority” (IANA).<sup>171</sup> Traditionally, IP addresses had been assigned entirely on a first-come/first-served principle.<sup>172</sup> Although the IANA coordinated the IP address space, it exercised almost no policy control over the address space. In the early 1990’s, however, it became evident that the IP address space would be used up in a few years.<sup>173</sup> The IP address space turned out to be a scarce resource. To cope with this scarcity, IP address registries started to impose policies that assigned IP addresses based on demonstrated need and made

---

<sup>168</sup> The telephone number space is a scarce namespace. Although only 5 percent of the 6.4 billion telephone numbers supported by the U.S. numbering plan had been assigned in the mid-90’s, the telephone number space was already in danger of becoming exhausted; *see* MUELLER, *supra* note 9, at 20-21. A similar problem occurs in the IP address space. To remove the artificial size limitation of the current IP version 4 address space, IP version 6, the next generation of a core protocol underlying Internet communications, will expand the size of the IP address space from 32 bits to 128 bits; *see id.* 38. Scarcity also exists in the namespace of generic top level domains (gTLDs). The current ICANN-administered DNS recognizes only a limited number of generic top level domains (.com, .net, .org, .aero, .biz, .coop, .info, .museum, .name, and .pro). For other scarce namespaces, *see infra* text accompanying notes 219-220.

<sup>169</sup> Various ways exist to allocate scarce namespaces. Names can be assigned on a first-come/first-served basis (assignment based on priority), they can be auctioned or traded as a regular good (assignment based on market forces), they can be 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 (by, e.g., trademark law or dispute resolution policies). Some of these assignments procedures work better in some namespaces than in others; *see id.* 24-26.

<sup>170</sup> *See infra* text accompanying notes 12, 33.

<sup>171</sup> Hubbard et al., *supra* note 88, at 3. IANA’s website can be found at <http://www.iana.org> (last revised Aug. 25, 2002).

<sup>172</sup> MUELLER, *supra* note 9, at 36.

<sup>173</sup> 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 although only a small fraction of the address space was actually used; *see id.* 36.

them subject to annual fees.<sup>174</sup> Thereby, the registries attempted to prevent stockpiling of IP addresses and to conserve the current address space as long as possible.<sup>175</sup> They increasingly used their technical control over the IP address space to facilitate rationing and policy enforcement.<sup>176</sup> 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 other policy issues that would be worth mentioning.<sup>177</sup> A similar development can be observed with Ethernet addresses.<sup>178</sup>

Name scarcity therefore can 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

If the coordination problems described are solved by the sheer size of a namespace, no central authority has to coordinate the assignment of names. 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

---

<sup>174</sup> It was even discussed whether IP address blocks should be auctioned or traded in a market, *see id.* 37.

<sup>175</sup> *See* Hubbard et al., *supra* note 88, at 2-3, 5, 6, 7-8. The more restrictive assignment of IP addresses is not the only way to cope with the scarce address space. One relief was the introduction of more new routing algorithms (classless inter-domain routing) that used up fewer IP addresses. Another solution is the expansion of the IP address space, a goal pursued by IPv6; *see* MUELLER, *supra* note 9, at 37-39; *supra* note 168.

<sup>176</sup> MUELLER, *supra* note 9, at 35-36. For an overview of the IPv6 address assignment policy, *see* Internet Corporation for Assigned Names and Numbers, *IP Address Assignment and Allocation Policy*, at <http://www.icann.org/aso/ipv6-statement-11jul02.htm> (July 11, 2002).

<sup>177</sup> *See* Kim Hubbard et al., *supra* note 88; MUELLER, *supra* note 9, at 32-39. Besides the scarcity constraint, the assignment of IP addresses also needs to take the Internet routing architecture into account; *see id.* 33-34.

<sup>178</sup> Ethernet addresses – officially called “Ethernet Unique Identifiers” (EUI) – are administered by the IEEE Registration Authority, *see* <http://standards.ieee.org/regauth>. Ethernet addresses used to be 48 bits long. As with IP addresses, the Ethernet address space gradually became a scarce resource. Therefore, the IEEE Registration Authority responded by imposing address space conservation policies. Apart from measures to preserve the address space, the IEEE Registration Authority exercises no considerable policy control over the Ethernet address space. *See* MUELLER, *supra* note 9, at 27-28. Furthermore, to alleviate the scarcity problem, the Ethernet address space was enlarged to support 64 bit long addresses. *See id.* 28.

communication among a wide variety of applications, a standardized mechanism has to exist how applications can contact and communicate with remote applications. The TCP and UDP port number space provides such standardized mechanism.<sup>179</sup> They are namespaces for identifying “channels” over which programs can 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.<sup>180</sup> Therefore, port numbers provide a service namespace that identifies applications running on networked computers.<sup>181</sup>

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, they had to agree which port to use. Therefore, the network provides an *ex ante*, standardized agreement about which programs can be contacted on which ports: the “Internet Assigned Numbers Authority” (IANA) maintains a list of TCP ports that are pre-assigned to specific programs or processes.<sup>182</sup> According to this list, web servers can be contacted on port 80, for example. This means that a web browser can simply contact a remote computer on port 80. If a web server is running on the remote computer, it will most likely listen to and respond on port 80.

Port 80 is not the only such “standardized” port. In fact, the first 1,024 of the 65,535 ports all are so-called “well-known ports” which are assigned to processes that are widely used across the Internet.<sup>183</sup> Port numbers in the range from 1,024 to 49,151 are called “registered ports”. They are assigned to less common programs and are listed in IANA’s list of port numbers “as

---

<sup>179</sup> 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 User Datagram Protocol (UDP) is a connection-less transport layer protocol which uses port numbers just as the Transmission Control Protocol (TCP) does. While there are important technical differences between UDP and TCP, they are of no importance for this paper and are therefore not addressed. For a more detailed description, see PETE LOSHIN, *TCP/IP CLEARLY EXPLAINED* 181-210 (3d ed. 1999); ERIC A. HALL, *INTERNET CORE PROTOCOLS* 274 (2000).

<sup>180</sup> In the TCP port number space, this combination with IP addresses are called “sockets”. See LOSHIN, *supra* note 179, at 184-185 (who also provides an explanation of server daemons which complicates this description slightly); CRAIG HUNT, *TCP/IP NETWORK ADMINISTRATION* 46 (2d ed. 1998).

<sup>181</sup> See HALL, *supra* note 179, at 274-286.

<sup>182</sup> The list is available at <http://www.iana.org/assignments/port-numbers> (last revised Aug. 28, 2002). It lists ports for both the UDP and the TCP protocol. From 1977 until 1994, the list was contained in a series of Request for Comments (RFCs), the most current being RFC 1700. In January 2002, however, it was officially acknowledged that RFC 1700 was outdated and that IANA’s website should be consulted instead, see Reynolds, Joyce K. ed., *Assigned Numbers: RFC 1700 is Replaced by an On-line Database*, Request for Comments 3232 (2002), at <http://www.rfc-editor.org/rfc/rfc3232.txt>. A copy of the list is stored on most computers connected to the Internet (e.g. /etc/services on Unix systems) in whole or part, see HUNT, *supra* note 180, at 43-44.

<sup>183</sup> FTP (port 21), SSH (22), telnet (23), SMTP (25), the 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.

a convenience to the community”.<sup>184</sup> While IANA exercises some control over the assignment of ports 0 through 49,151,<sup>185</sup> 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, 25% of the TCP port number space are not only uncontrolled, they are 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.<sup>186</sup> 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. The technical architecture of namespaces is not neutral. Rather, it is based on design choices that embody particular values. To see the value embedded in the port number space, imagine a different design. *First*, imagine that IANA would assign every port number to specific programs so that no private ports would exist. *Secondly*, imagine that IANA would assign 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 also auction ports or charge an administrative fee for assignment. It could choose to assign no 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 these criteria. The scenario becomes more plausible, however, if you imagine, *thirdly*, that it was not IANA that assigned the port

---

<sup>184</sup> See <http://www.iana.org/assignments/port-numbers> (last revised Aug. 28, 2002).

<sup>185</sup> 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 Internet Assigned Numbers Authority, *Application for System (Well-Known) Port Number*, at <http://www.iana.org/cgi-bin/sys-port-number.pl> (last revised Nov. 21, 2000); Internet Assigned Numbers Authority, *Application for User (Registered) Port Number*, <http://www.iana.org/cgi-bin/usr-port-number.pl> (last revised Nov. 21, 2000).

<sup>186</sup> 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 as 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.

numbers, but 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.<sup>187</sup>

In regulating the port number space, however, 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 running over the Internet that uses a private port. This particular regulation of the port number space played a large role in the phenomenal innovation occurring on the Internet. Since nobody exercised control over the port number space, everybody was 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&T's or Microsoft's 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 fostered 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.<sup>188</sup> First described by Saltzer, Reed and Clark in a seminal paper

---

<sup>187</sup> This scenario may seem far-fetched. However, in other communication networks, this application discrimination is already happening. Over the last 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 18. 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, “if 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, *supra* note 9, at 172; see also Hans Kruse, William Yurcik & Lawrence Lessig, *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). 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 & Kjeld B. Egevang, *Traditional IP Network Address Translator (Traditional NAT)*, Request for Comments (RFC) 3022, at <http://www.rfc-editor.org/rfc/rfc3022.txt> (January 2001); Pyda Srisuresh & Matt Holdrege, *IP Network Address Translator (NAT) Terminology and Considerations*, Request for Comments (RFC) 2663, at <http://www.rfc-editor.org/rfc/rfc2663.txt> (August 1999). For an overview of the architectural implications of NATs, see Tony Hain, *Architectural Implications of NAT*, Request for Comments (RFC) 2993, at <http://www.rfc-editor.org/rfc/rfc2993.txt> (November 2000). For an explanation of the related concept of “Realm Specific IP” (RSIP), particularly “Realm Specific Address and Port IP” (RSAP-IP), see Srisuresh & Holdrege, RFC 2663, *id.*, 15, 18-21.

<sup>188</sup> “... the [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*,

dating from 1984,<sup>189</sup> the e2e argument claims that as much intelligence as possible should reside at the “edges” of the network, i.e. at applications running on networked computers, not in the network itself.<sup>190</sup> It vests power in end users and disables control by a central actor within the network.<sup>191</sup> E2e thereby ensures that the network is a neutral platform that does not discriminate between different applications or services.<sup>192</sup>

Concerning innovation,<sup>193</sup> e2e implies that “innovators with new applications need only connect their computers to the network to let their applications run”.<sup>194</sup> 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.<sup>195</sup>

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 what kind of applications will be run over the network. It is one of the goals of e2e “to support the widest possibly variety of services and functions, to permit applications that cannot be anticipated”.<sup>196</sup> Network architectures that violate the e2e design principle tend to build “complex function into a network [which] implicitly optimizes

---

Request for Comments 1958, 2 (Brian E. Carpenter ed., 1996), at <http://www.rfc-editor.org/rfc/rfc1958.txt>; 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): “... the 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.”

<sup>189</sup> Jerome H. Saltzer & David P. Reed & David D. Clark, *End-to-End Arguments in System Design*, 2 (4) ACM TRANSACTIONS ON COMPUTER SYSTEMS 277-288 (1984). For an overview of e2e, see *Architectural Principles of the Internet*, RFC 1958, *supra* note 188, at 3-4. For an analysis of the challenges to the e2e design principle posed by new technologies and new demands, see Blumenthal & Clark, *supra* note 188, at 70; *Recent Changes in the Architectural Principles of the Internet* 3-5 (Brian E. Carpenter & Rob Austein eds., 2002), at <http://www.rfc-editor.org/internet-drafts/draft-iab-arch-changes-00.txt>; see also Brian E. Carpenter & Scott W. Brim, *Middleboxes: Taxonomy and Issues*, Request for Comments 3234, at <http://www.rfc-editor.org/rfc/rfc3234.txt> (Febr. 2002).

<sup>190</sup> See Saltzer & Reed & Clark, *supra* note 189, at 286; LESSIG, *supra* note 9, at 34; Lemley & Lessig, *supra* note 18, at 930-931; Blumenthal & Clark, *supra* note 188, at 71. In its purest forms, 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 & Reed & Clark, *supra* note 189, at 277; see also David P. Reed & Jerome H. Saltzer & David D. Clark, *Commentaries on “Active Networking and End-to-End Arguments”*, 12 (3) IEEE NETWORK 69 (1998); Blumenthal & Clark, *supra* note 188, at 71.

<sup>191</sup> Kruse, Yurcik & Lessig, *supra* note 187, at 150.

<sup>192</sup> LESSIG, *supra* note 9, at 37; Lemley & Lessig, *supra* note 18, at 931.

<sup>193</sup> The e2e argument has also many implications for the security, integrity, performance and other aspects of communications. In fact, e2e should be regarded as an umbrella for different, but related system design principles; see Saltzer & Reed & Clark, *supra* note 189; Brian E. Carpenter, *Internet Transparency*, Request for Comments (RFC) 2775, at 3-5 (2000), at <http://www.rfc-editor.org/rfc/rfc2775.txt>.

<sup>194</sup> LESSIG, *supra* note 9, at 36.

<sup>195</sup> Kruse, Yurcik & Lessig, *supra* note 187, at 150.

<sup>196</sup> Reed & Saltzer & Clark, *supra* note 190, at 70.

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.”<sup>197</sup>

Although in a network, no single entity may exist that can anticipate all possible uses of the network, this knowledge may indeed exist, but 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.<sup>198</sup> If it is not predictable what kind of innovation will occur on a network, e2e argues, the network should not be biased by its very architecture towards any specific kind of innovation.<sup>199</sup>

The connection between e2e design and innovation is not a novel observation.<sup>200</sup> 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 25 % of all port numbers uncoordinated, thereby enabling decentralized innovation.<sup>201</sup> This openness of the TCP/UDP port number space is the Internet’s implementation of the end-to-end argument.<sup>202</sup>

---

<sup>197</sup> *Id.*

<sup>198</sup> 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, *Competition as a Discovery Procedure*, in *NEW STUDIES IN PHILOSOPHY, POLITICS, ECONOMICS AND THE HISTORY OF IDEAS* 179 (Friedrich A. Hayek 1978); FRIEDRICH A. HAYEK, *THE POLITICAL ORDER OF A FREE PEOPLE* 67-70 (1979); FRIEDRICH A. HAYEK, *THE MIRAGE OF SOCIAL JUSTICE* 70-71, 114-115 (1976); Manfred E. Streit, *Cognition, Competition, and Catallaxy*, 4 CONST. POL. ECON. 223, 234-238 (1993). More generally, the claimed importance of the e2e argument for innovation is part of the larger debate what the optimal market structure for innovation is and what the implications of centralized control for innovation are; *see* Lemley & Lessig, *supra* note 18, at 960-962; John E. Lopatka & William H. Page, *Internet Regulation and Consumer Welfare: Innovation, Speculation, and Cable Bundling*, 52 HASTINGS L.J. 891, 914-917 (2001); *see also* LESSIG, *supra* note 9.

<sup>199</sup> *See* LESSIG, *supra* note 9, at 39; Lemley & Lessig, *supra* note 18, 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 some particular support by the network architecture to reach their full potential.

<sup>200</sup> It was clearly formulated by Reed & Saltzer & Clark, *supra* note 190, at 70. Lawrence Lessig builds much of his analysis in his book “The Future of Ideas” on the impact of e2e on innovation. *See also* Blumenthal & Clark, *supra* note 188, at 72, 74; Kruse, Yurcik & Lessig, *supra* note 187, at 141.

<sup>201</sup> *See supra* text accompanying notes 185-187.

<sup>202</sup> 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 paper does not attempt to provide a full assessment of the relationship between e2e, innovation, and the governance over the Internet.

Uncoordinated namespaces can enable decentralized innovation. If the port number space would be 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 not complied with the e2e design principle, the development of HTTP, HTML, and the web revolution might never have taken place.<sup>203</sup>

## **E. Scope of Namespace Governance**

The governance of namespaces can not only differ in intensity, but also in scope. Namespaces can be designed to store large or small amounts of information. They can be architected to be accessible for a single or for multiple purposes. They can 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 can lead to privacy concerns, information-poor namespaces can become a tool for privacy protection.

As was described above,<sup>204</sup> Microsoft Passport creates a user namespace in which much personal information is stored in one location.<sup>205</sup> 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 by 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.<sup>206</sup>

---

<sup>203</sup> Reed & Saltzer & Clark, *supra* note 190, at 70.

<sup>204</sup> *See supra* text accompanying notes 119-122.

<sup>205</sup> 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 – employers, Internet portals, various communities, and business services. Authentication systems attempt to reduce this friction; *see* Liberty Alliance Project, *supra* note 139, at 8-12.

<sup>206</sup> For this argument in the Microsoft Passport context, *see supra* text accompanying notes 119-122.

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 database. In contrast, no global public databases exist that reveal personal information about every telephone subscriber. From an outside perspective, the telephone network is therefore an information-poor namespace.<sup>207</sup>

## **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. As the following discussion will show, 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 a P2P 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 therefore a multi-purpose namespace.

Single-purpose namespaces are more prone to regulation than multi-purpose namespaces. As soon as a court had determined that the Napster namespace was mainly used 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.

### **b) Innovation around Namespaces**

Whether a namespace serves a single or multiple purposes, also determines to a large extent whether the namespace fosters or hinders innovation.

---

<sup>207</sup> 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. ENUM potentially stores a large amount of private contact information. Since such information is stored in a DNS-like database, it is questionable whether the traditionally lax privacy approach of the DNS should also apply to ENUM; see Cannon, *supra* note 83, at 35; Hwang et al., *supra* note 83, at 22-23; see also the documents of the Security & Privacy Working Group within the ENUM Forum, at <http://www.enum-forum.org/workingdocs.html> (last visited Sept. 1, 2002); Electronic Privacy Information Center, *ENUM*, at <http://www.epic.org/privacy/enum> (last revised Aug. 14, 2002).

### **aa) Horizontally Innovation-friendly Namespaces**

A multi-purpose namespace does not control for what purposes 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 purposes for which it is used. The IP address space therefore enables new applications to be created that use the IP address space for whatever purposes. The same is true for the Ethernet address space, the domain name space 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. Thereby, the application would 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.<sup>208</sup> Single-purpose namespaces that are not horizontally innovation-friendly allow only certain authorized applications to access their namespaces and control for what purposes the namespace is accessed. They can impede innovation by non-affiliated innovators.

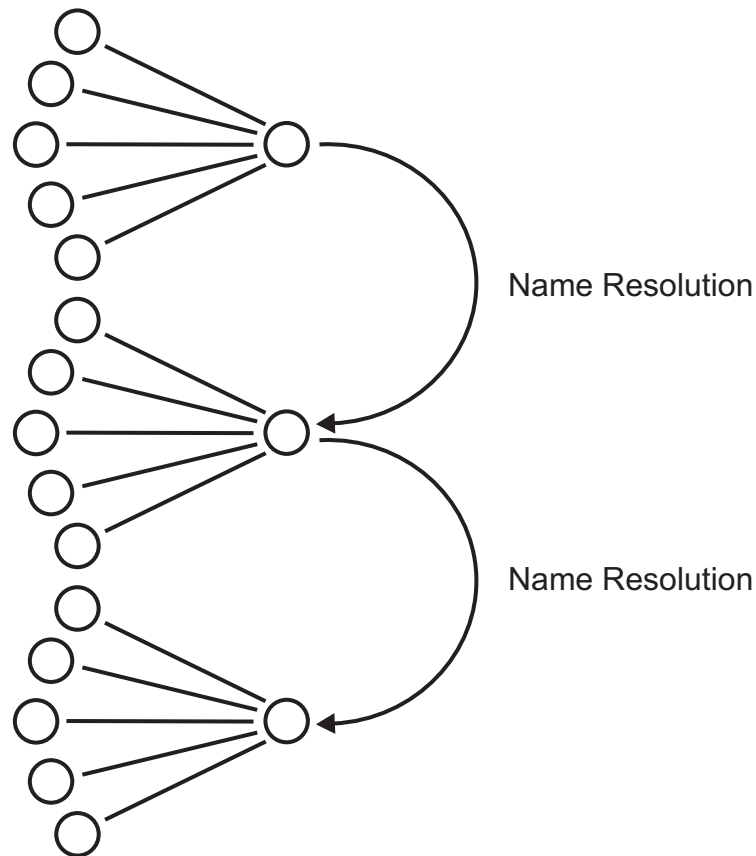
### **bb) Vertically Innovation-friendly Namespaces**

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

---

<sup>208</sup> See Faulhaber, *supra* note 124, at 317-318. For information about the FCC’s requirement to open AOL’s instant messaging systems to competing systems, see *supra* note 147.

namespaces on top of them. A vertically innovation-friendly namespace allows the creation of a distinct name service on top of its own name service (see figure 4).



**Figure 4: Vertically Innovation-friendly Namespaces**

Such multi-purpose namespaces facilitate innovation in software applications that need their own namespaces. For such applications can use the existing namespace infrastructure and build their own namespaces on top of it. A single-purpose, not vertically innovation-friendly namespace prevents such namespace creation by contractual or technological means.

A prime example for vertically innovation-friendly namespaces is the intertwining among the Ethernet address, IP address, and domain name spaces. 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 addressed by Ethernet addresses.<sup>209</sup> The “Address Resolution Protocol” (ARP) enables the network to resolve IP addresses into Ethernet addresses. While the DNS connects the domain name space with the IP address space, ARP in a similar way connects the IP address space with the Ethernet address space.<sup>210</sup>

Other examples of layered namespaces include many P2P systems that create a proprietary namespace on top of the IP address space<sup>211</sup> as well as “Uniform Resource Names” (URNs), a location-independent namespace that is created on top of the namespace for identifying web pages.<sup>212</sup> Also, many instant messaging services build user namespaces on top of the IP address or the domain name space.<sup>213</sup> On top of such instant messaging user namespaces, even other namespaces can be created. The Madster network,<sup>214</sup> for example, creates a “virtual private network” on top of the America Online Instant Messenger (AIM) user namespace: a distinct file namespace is created on top of the AIM user namespace. This Madster file namespace enables music and other files to be shared among the users identified by the underlying AIM user namespace.<sup>215</sup> 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 whether a namespace allows other namespaces to be built on top of it is an application of the e2e

---

<sup>209</sup> This is not the only addressing scheme, however. If a computer is connected to the Internet by a network different from Ethernet (such as ATM, e.g.), the addressing scheme differs as well.

<sup>210</sup> For an overview of ARP, see HALL, *supra* note 179, 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-04.txt> (June 30, 2002).

<sup>211</sup> This is done, e.g., in the P2P system Overnet, see Overnet, *How it Works*, <http://www.overnet.com/documentation/how.html> (last visited Sept. 1, 2002).

<sup>212</sup> On the WWW, web pages are identified by “Uniform Resource Locators” (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 Larry Masinter & Karen Sollins, *Functional Requirements for Uniform Resource Names*, Request for Comments (RFC) 1737, at <http://www.rfc-editor.org/rfc/rfc1737.txt> (Dec. 1994); Ryan Moats, *URN Syntax*, Request for Comments (RFC) 2141, at <http://www.rfc-editor.org/rfc/rfc2141.txt> (May 1997); Leslie L. Daigle et al., *URN Namespace Definition Mechanism*, Request for Comments (RFC) 2611, at <http://www.rfc-editor.org/rfc/rfc2611.txt> (June 1999). For an overview of all registered URN namespaces, see Internet Assigned Names Authority, *URN Namespaces*, at <http://www.iana.org/assignments/urn-namespaces> (last revised Aug. 16, 2002).

<sup>213</sup> See Jeff Tyson, *How Instant Messaging Works*, at <http://www.howstuffworks.com/instant-messaging.htm> (last visited Sept. 1, 2002); Michael Gowan, *How it Works: Instant Messaging*, at <http://www.cnn.com/2000/TECH/computing/05/25/how.messaging.works.idg/> (May 25, 2000); Speta, *supra* note 129, at 236; see also Faulhaber, *supra* note 124, at 317.

<sup>214</sup> <http://www.madster.com> (last visited Sept. 1, 2002). Madster was formerly known as Aimster.

<sup>215</sup> For an analysis of the copyright liability of Aimster, see Haydn J. Richards, *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>.

argument. As was described above, the e2e argument states that system functions should be located at upper rather than lower levels of a layered system.<sup>216</sup> 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 a single or multiple purposes is a question that relates to how a namespace interacts with surrounding applications. Yet, from a governance perspective, the way in which namespaces are structured internally matters as well. 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 the use of the namespace 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 changes over time. Building a comprehensive, rigid namespace structure at one time does not mean that this structure will be the best possible in future times.

#### 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,<sup>217</sup> the size of the IP and the Ethernet address spaces was enlarged over time in order to accommodate more addresses.<sup>218</sup> Similar problems arose in the domain name space<sup>219</sup> and the Social Security number space.<sup>220</sup> 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.

---

<sup>216</sup> See *supra* note 190.

<sup>217</sup> See *supra* text accompanying notes 168-178.

<sup>218</sup> Another namespace that is expanded 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.

<sup>219</sup> Until the 1980's, each computer connected to the Internet stored a single list of all the names and IP addresses of all other connected computers. As the Internet increased in size, a more scalable namespace architecture was needed. The current DNS hierarchy is the result of this evolutionary process. For a detailed history of the DNS, see MUELLER, *supra* note 9, at 73-208; Froomkin, *supra* note 59, at 50-92; Kesan & Shah, *supra* note 59, at 169-176.

<sup>220</sup> Originally, Social Security numbers were used to administrate potential retirement and survivor benefit payments under the Social Security Act of 1935. Today, Social Security numbers are used by a wide variety of federal, state, and local authorities as well as private companies for identification purposes. Nevertheless, the small size of the number space, the lack of a check digit, and other disadvantages severely impede the usability of Social Security numbers for many purposes. For an overview, see SIMSON GARFINKEL, DATABASE NATION 18-25 (2000).

## b) Changing Kinds of Names

In some cases, namespaces do not only have to cope with a larger number of names that have to be addressed by the namespace. They also have to deal with new kinds of names. This is especially important in a particular class of namespaces: bibliographic classification schemes.

In libraries, bibliographic classification schemes are used to place books in book shelves in a particular order as well as to create classified catalogues and bibliographies.<sup>221</sup> For a long time, classification schemes organized knowledge in a strictly hierarchical manner. The Library of Congress Classification (LCC), one of the largest in the world, continues to do so up to the present day.<sup>222</sup> 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 built-in obsolescence.<sup>223</sup> New classifiers have then to be added to enumerative classification scheme by the editors of the scheme (so-called “classificationists”). 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 to integrate new subjects into their existing structure. Such classification difficulties impede the organization and processing of new knowledge which, in its turn, can have detrimental impact on scientific progress.<sup>224</sup> This example demonstrates that

---

<sup>221</sup> For a general overview of the theory and problems of classification, see MARCELLA & NEWTON, *supra* note 110. An overview of the history and present examples of classification schemes is given in MARCELLA & NEWTON, *supra* note 110, at 65-112. A comprehensive account of the history of library classification systems can be found in the standard work Evgenij I. Samurin, *GESCHICHTE DER BIBLIOTHEKARISCH-BIBLIOGRAPHISCHEN KLASSIFIKATION* [The History of Librarian Bibliographic Classification] (1964, 2 vols.).

<sup>222</sup> “LCC is fundamentally and irrevocably an enumerative scheme, with perhaps the least synthesis of all the general schemes”, MARCELLA & NEWTON, *supra* note 110, at 85. The LCC is used by over 62% of U.S. university libraries used LCC, *id.* 80. It boasts over 60,000 distinct classification numbers. For an overview of the LCC, see *id.* 79-89.

<sup>223</sup> *Id.* 30.

<sup>224</sup> “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

information about the kinds of names being assigned in a namespace can be encoded in the very structure of namespace. As the kinds of names changes over time, the structure of such namespaces can become outdated. Using such an approach in dynamically changing environments is therefore not advisable.<sup>225</sup>

Regarding bibliographic classification systems, library and information science has invested large efforts to get rid of these structural, innovation-hostile shortcomings. Over the last few decades, various forms of “self-perpetuating” classification scheme have been proposed to solve these problems. The basic idea, developed by the Indian librarian Shiyali R. Ranganathan in the 1930’s, 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 of knowledge without waiting for the classificationist to give the number.”<sup>226</sup>

As it is beyond the scope of this paper to describe this so-called “faceted analytico-synthetic” approach in detail, suffice it to say that such classification schemes do not list all specific subjects of knowledge, but rather the fundamental constituent concepts (or: “facets”) of knowledge by the combination of a few of which the specific subjects can be formed.<sup>227</sup> By using these facets and digits with mnemonic values,<sup>228</sup> 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 yet achieve identical results.<sup>229</sup> By providing

---

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*, 43 (3) LIBRI 179, 183 (1990). See also Gerhard J. A. Riesthuis, *Sociological Aspects of Classification*, 24 (2) INTERNATIONAL CATALOGUING AND BIBLIOGRAPHIC CONTROL 35, 36 (1995); Shiyali R. Ranganathan, *Self-Perpetuating Scheme of Classification*, 4 (4) THE JOURNAL OF DOCUMENTATION 223, 231 (1949).

<sup>225</sup> Such problems can be observed in other namespaces as well. The IP address space may exemplify this problem. Initially, the IP address space was hierarchically structured in “classes” of different sizes (“classful IP addressing”). The information expressed by this hierarchy was used by the network routers to route traffic efficiently over the Internet; see COMER, *supra* note 96, at 283-285; MUELLER, *supra* note 13, at 33-35. As the Internet grew larger, this mechanism proved inefficient. Therefore, new routing mechanisms (such as “subnet addressing” and “classless inter-domain routing”) were developed. However, for these mechanisms, the information expressed in the hierarchical structure of the IP address space was not only unnecessary. The fixed hierarchical structure itself was obstructive to the new routing mechanisms. Therefore, the assignment procedure of IP addresses and the internal structure of the namespace had to be adapted. For a more detailed overview, see MUELLER, *supra* note 9, at 36-38; COMER, *supra* note 96, at 289-292.

<sup>226</sup> Ranganathan, *supra* note 224, at 224; see also MARCELLA & NEWTON, *supra* note 110, at 30.

<sup>227</sup> Ranganathan, *supra* note 224, at 232. For an introduction into faceted classification schemes, see BRIAN C. VICKERY, FACETED CLASSIFICATION – A GUIDE TO THE CONSTRUCTION AND USE OF SPECIAL SCHEMES (1968).

<sup>228</sup> For an overview of the concept of seminal mnemonics as used in Colon Classification, see RAGHUNATH S. PARKHI, DECIMAL CLASSIFICATION AND COLON CLASSIFICATION IN PERSPECTIVE 461-473 (1964); see also MARCELLA & NEWTON, *supra* note 110, at 58.

<sup>229</sup> Ranganathan, *supra* note 224, 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

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.<sup>230</sup> It is not the goal of this paper to write about the details of 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 *kind* of names that has to be identified changes 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.

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 the facets in analytico-synthetic classification schemes, the periodic system provides a modularized tool set by which the

---

class number; see MARCELLA & NEWTON, *supra* note 110, at 25. Similar ideas are used in other namespaces as well. For attempts to build a facet-oriented search layer on top of the DNS, see Klensin, *supra* note 210. An example for creating a new classification number with the faceted analytico-synthetic approach is given by PARKHI, *supra* note 228, at 469-470. A comparison between enumerative and faceted classification scheme is provided in MARCELLA & NEWTON, *supra* note 110, at 20-28. A general description can be found as well in MARCELLA & NEWTON, *supra* note 110, at 19-20: "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 the form of presentation, place and time. To classify an item, we analyse 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."

<sup>230</sup> 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; see Clare Beghtol, 'Facets' as *Interdisciplinary Undiscovered Public Knowledge: S.R. Ranganathan in India and L. Guttman in Israel*, 51 JOURNAL OF DOCUMENTATION 194, 201 (1995); MARCELLA & NEWTON, *supra* note 110, at 28-30. However, the best-known self-perpetuating classification scheme is the Colon Classification (CC), developed by the aforementioned Indian librarian Shiyali R. Ranganathan in the 1930's. In the CC, the faceted analytico-synthetic approach is realized to the largest extent. For an assessment of the self-perpetuating feature of the Colon Classification, see Arthur Maltby, SAYERS' MANUAL OF CLASSIFICATION FOR LIBRARIANS 199-201 (5th ed., 1975); Abdul M. Baba, DEWEY DECIMAL CLASSIFICATION, UNIVERSAL DECIMAL CLASSIFICATION AND COLON CLASSIFICATION 336-337, 449 (1988); see also Malur A. Gopinath, *The Colon Classification*, in CLASSIFICATION IN THE 1970'S 53, 56 (Arthur Maltby ed., 1972); SHIYALI R. RANGANATHAN, PROLEGOMENA TO LIBRARY CLASSIFICATION (3rd ed. 1967). For a general overview of the Colon Classification, see also ELAINE SVENONIUS, THE INTELLECTUAL FOUNDATION OF INFORMATION ORGANIZATION 174-176 (2000). CC is not used by many libraries worldwide and is considered to fade away slowly for various reasons; see MARCELLA & NEWTON, *supra* note 110, at 103-104.

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).<sup>231</sup> Modularization and decentralization can enable innovation within the namespace itself.

## IV. IMPLICATIONS OF GOVERNANCE DIMENSIONS

This paper has hitherto identified several dimensions along which namespace governance can be studied. Choosing a particular design for a namespace has numerous legal and policy consequences. Although these consequences 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. Secondly, it also influences the allocation of knowledge, control, and responsibility within the namespace.

### A. Namespace Architectures Protect and Express Values

As this paper has illustrated, 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.<sup>232</sup> It can decide what personal information a domain name registrant has to provide and who can access such information afterwards.<sup>233</sup> It can regulate the domain name registration industry by imposing price controls and enforcing market structures.<sup>234</sup> It can decide what top level domains (TLDs) should exist.<sup>235</sup> Whether to introduce a .biz TLD for businesses, a .ps TLD for Palestina,<sup>236</sup> a

---

<sup>231</sup> Ranganathan, *supra* note 224, at 232.

<sup>232</sup> ICANN discussed to introduce such a fee in 1999; *see* MUELLER, *supra* note 9, at 7, 188, 189-190; Froomkin, *supra* note 59, at 87.

<sup>233</sup> MUELLER, *supra* note 9, at 8. The current design of the domain namespace allows everyone to identify the name as well as the physical and email address of every domain name registrant, *see id.* 219, 235-238.

<sup>234</sup> *See id.* 219.

<sup>235</sup> *See Name.Space, Inc. v. Network Solutions, Inc.*, 202 F.3d 573 (2nd Cir. 2000).

.eu TLD for the European Union,<sup>237</sup> a .xxx TLD for web sites with sexually explicit material, or a .kids TLD for web sites which are suitable for children – all these are policy decisions that involve issues of international politics, freedom of speech, and content regulation.<sup>238</sup>

Other examples how the namespace architecture determines the values protected by the namespace include federated namespaces that enable competition between different namespace providers,<sup>239</sup> centralized P2P user namespaces that protect the interests of copyright owners,<sup>240</sup> decentralized P2P user namespaces that are specifically designed to preserve the privacy of information producers and consumers and resist censorship,<sup>241</sup> and uncoordinated namespaces such as the TCP/UDP port number space that create an open platform for decentralized, uncoordinated innovation.<sup>242</sup>

At the same time, by protecting certain values, many namespaces communicate a particular *Weltanschauung*. This is particularly noticeable in bibliographic classification schemes.<sup>243</sup> In library and information sciences, it is a well-known fact that classification schemes often show structural biases of gender, sexuality, race, age, ability, ethnicity, language, culture, and religion.<sup>244</sup> The Dewey Decimal Classification class for religion is biased towards – or, more gently spoken: heavily focused on – Christianity.<sup>245</sup> The Library of Congress Classification exhibits distinct biases “towards the social structure, history, law and cultural concerns of the

---

<sup>236</sup> This TLD was created in 2000, *see* Internet Assigned Names Authority, *Root-Zone Whois Information, .ps – Palestinian Territories*, at <http://www.iana.org/root-whois/ps.htm> (last revised March 22, 2000); *see also* Froomkin, *supra* note 59, at 47-48.

<sup>237</sup> *See* Regulation (EC) No. 733/2002 of the European Parliament and of the Council of April 22, 2002, on the Implementation of the .eu Top Level Domain, 2002 O.J. (L 113) 1.

<sup>238</sup> *See also* MUELLER, *supra* note 9, at 9; Froomkin & Lemley, *supra* note 60, at 19-21.

<sup>239</sup> *See supra* text accompanying notes 131-151.

<sup>240</sup> *See supra* text accompanying notes 116-117.

<sup>241</sup> *See supra* text accompanying note 166.

<sup>242</sup> *See supra* text accompanying notes 179-203.

<sup>243</sup> Wilson, *supra* note 94, at 392. Wilson writes on p. 395: “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 (ie European), Party member.”

<sup>244</sup> 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 (2) CATALOGING & CLASSIFICATION QUARTERLY 61 (2001). A database surveying this literature is located at <http://www.ualberta.ca/~holson/marginal/database.htm> (last visited Sept. 1, 2002). *See also* Hope A. Olson, *Mapping Beyond Dewey's Boundaries: Constructing Classificatory Space for Marginalized Knowledge Domains*, 47 (2) LIBRARY TRENDS 233 (1998); Wilson, *supra* note 94.

<sup>245</sup> In the 21st 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). For other biases in the DDC, *see* Wilson, *supra* note 94, at 394-395; *see also* Olson, *supra* note 244, at 253 note 1. Over the last years, DDC has undertaken great efforts to reduce systematic biases in its classification scheme.

United States.”<sup>246</sup> The major Russian classification system has been criticized for reflecting Socialist ideology.<sup>247</sup> 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.<sup>248</sup> The plasticity of bibliographic classification schemes can also be used strategically: Chinese classification systems have been deliberately shaped to reflect particular political and ideological beliefs.<sup>249</sup>

This is not the place to criticize particular classification schemes. Indeed, some biases in classification schemes may be unavoidable.<sup>250</sup> Biased bibliographic classification schemes merely illustrate that namespaces are social constructs which reflect the same biases as the culture that creates them.<sup>251</sup> All these problems do not only occur in bibliographic classification schemes. The structure of other namespaces, such as web directories, can express values in similar worrisome ways.

---

<sup>246</sup> MARCELLA & NEWTON, *supra* note 110, at 88.

<sup>247</sup> Tamara S. Goltvinskaya & Eduard S. Sukiasyan, *Library-Bibliographical Classification: On the Path of Renovation*, 20 (2) KNOWLEDGE ORGANIZATION 77, 78-79 (1993) (on 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 94, at 394-395. Other classification and subject heading schemes suffer from similar shortcomings. Classic biases in schemes used in the U.S. include the treatment of Native Americans as well as of African cultures and religions; see Olson & Schlegel, *supra* note 244, at 67-68.

<sup>248</sup> See Wilson, *supra* note 94, at 393, 395.

<sup>249</sup> See William E. Studwell, Hong Wu & Rui Wang, *Ideological Influences on Book Classification Schemes in the People’s Republic of China*, 19(1) CATALOGING & CLASSIFICATION QUARTERLY 61, 62, 63-64 (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)*, 9 (2) INTERNATIONAL CATALOGUING 21 (1980).

<sup>250</sup> Unavoidable biases may result from the fact that their users are not be 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 (2/3) CATALOGING & CLASSIFICATION QUARTERLY 125, 126 (1982). Furthermore, many scholars argue that it is simply impossible to design a totally objective, unbiased classification scheme; see Olson, *supra* note 244, at 252. However, other scholars propose that due to their ability to construct themselves, faceted, analytic-synthetic classification schemes such as the Colon Classification exhibit less inherent biases than other schemes, see Wilson, *supra* note 94, at 393.

<sup>251</sup> Olson, *supra* note 244, at 233-234; Riesthuis, *supra* note 224; see also Eric de Grolier, *Classifications as Cultural Artefacts*, in UNIVERSAL CLASSIFICATION I – SUBJECT ANALYSIS AND ORDERING SYSTEMS 19 (Ingetraut Dahlberg ed., vol. 1, 1982).

## B. Allocation of Knowledge, Control, and Responsibility

While this paper has identified several distinct governance dimensions, most of them can be reduced to a single, more abstract dimension. Most governance dimensions described hitherto differ in the allocation of knowledge, control, and responsibility within a namespace.

A flat namespace, for example, has a single point of *knowledge*.<sup>252</sup> 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 thereby 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.

In vertically distributed, i.e. hierarchical, namespaces, on the other hand, different parts of the namespace can be managed by different entities, and, occasionally, different policies.<sup>253</sup> Hierarchical namespaces distribute knowledge, control, and responsibility over different hierarchies of the namespace.<sup>254</sup>

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 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,<sup>255</sup> an uncoordinated namespace is fully “democratized” in the sense that no entity in the namespace

---

<sup>252</sup> See also Watson, *supra* note 30, at 207.

<sup>253</sup> COULOURIS ET AL., *supra* note 26, at 358.

<sup>254</sup> Minar therefore writes that hierarchical systems are more “fault-tolerant and lawsuit-proof than centralized systems”, see Nelson Minar, *Distributed Systems Topologies, Part 2*, *supra* note 96.

<sup>255</sup> See *supra* text accompanying note 179.

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 paper.

| Namespace Architecture  |                             | Allocation of    |         |                |
|-------------------------|-----------------------------|------------------|---------|----------------|
|                         |                             | Knowledge        | Control | Responsibility |
| Vertical Distribution   | Flat                        | c <sup>256</sup> | 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 a merely technical matter. It entails decisions about legal and policy questions. Structure has consequences. At this point, the gentle reader might ask “so what?”. While the paper so far has analyzed the close intertwining between

<sup>256</sup> c = fully centralized; m = intermediate between centralized and decentralized; d = fully decentralized.

technology, law and policy in namespaces, it has not addressed the question what the consequences of this analysis are. Should namespaces be designed according to certain principles? How should lawyers think about namespaces? This section attempts to provide some answers to such questions. In particular, it describes what the consequences for lawyers and technologists, who have to deal with namespaces, are.

Unfortunately, providing such answers – and thereby developing a full-fledged theory of namespace governance – is complicated by four factors:

1. First, namespaces are used in many different areas, ranging from network authentication and communication to bibliographic classification issues. While this paper 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 in general. What may represent a wise regulatory decision for one particular namespace may be totally erroneous for another one. After all, authenticating users in a public key infrastructure is not the same as developing a method to place books in library shelves in some reasonable order.
2. Secondly, developing a theory of namespace regulation is complicated by the fact that it should be based on a sound general theory of regulation. Although technology is plastic and, therefore, values such as freedom, competition, copyright, and privacy can be “engineered” into technology,<sup>257</sup> one first has to determine whether that is actually the best solution. Solving social problems by technological design is normally 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 of lacking predictability: if it is unclear what kind of problems will emerge in the future, how could an *ex ante* regulation by 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 lacking predictability and path dependency could lead to an answer what kind of values should be

---

<sup>257</sup> Cf. LESSIG, *supra* note 8.

implemented by an *ex ante* regulation (i.e. by engineering them into technology), and what kind of values should be left to *ex post* regulation (by the legislator, the courts and other regulators). Such a normative theory of namespace governance could provide guidelines which legal and policy considerations should be taken into account during the technical design of a namespace. It could also prompt lawyers to become more involved in the thinking about designing 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. As it is beyond the scope of this paper to even outline such a theory, the paper has to a large extent restricted itself to a descriptive and empirical approach in analyzing the governance in namespaces.

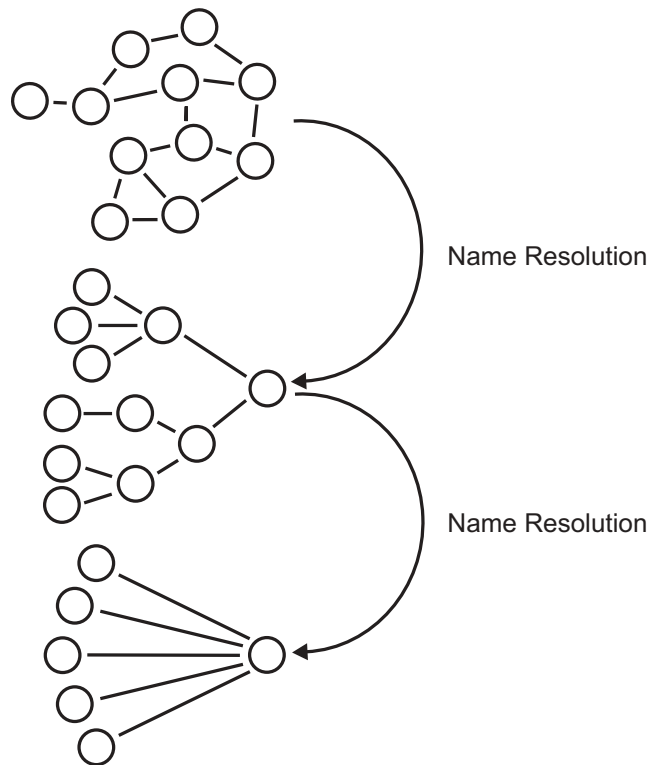
3. A complete theory how namespaces should be governed is thirdly complicated by the fact that it is not enough to look at individual namespace governance dimensions. Rather, the interaction between different governance dimensions has to be taken into account as well. Consider, for example, the DNS. As was described above, the hierarchical structure of the DNS leads to a certain decentralization: different parts of the namespace can be governed by different entities.<sup>258</sup> 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.<sup>259</sup> Different dimensions of namespace governance (here: contractual webs and topology) are not always used to achieve the same goal.
4. Finally, not only the interactions between different governance dimensions in a namespace, but also between different namespaces have to be taken into account. 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. Regularly, 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

---

<sup>258</sup> See *supra* text accompanying notes 102-103.

<sup>259</sup> The author is indebted to Milton Mueller for this remark.

tried to shut down the “channel” over which Napster communicated. In other words, it could have tried to shut down the TCP port 6699. The e2e-compliant TCP port number space made such regulation impossible, however. 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).<sup>260</sup>



**Figure 6: Interaction Between Namespaces**

<sup>260</sup> Another example where the interaction between different namespaces becomes important is digital rights management. 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, often a proprietary, centralized, intense namespace governance structure is 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 have to ensure the proper and secure interaction and communication among them.

Despite all these reservations, in the following the paper attempts to outline what the implications of a normative theory of namespace governance could be. In general, namespaces should be designed in ways that enable competition within the namespace, between different namespaces as well as around and on top of namespaces. Namespaces should be designed as open platforms on top of which innovation can occur. The paper has demonstrated several tools that can be used to achieve these ends. Both a vertical and horizontal distribution of namespaces facilitates competition. Furthermore, governance structures in namespaces should be as lightweight as possible. As the end-to-end argument demands, control and intelligence should not be placed in namespaces themselves, but in applications and other components that lie on top of them. Minimizing control structures in namespaces also means adapting modular design principles.<sup>261</sup> This can be exemplified in the privacy area. A user authentication system such as Microsoft Passport, for example, should reveal as little personal information as possible each time a user is authenticated. If the personal information stored in the user namespace is stored in modularized components, the namespace is able to transmit only those authentication modules which are needed for a particular authentication.<sup>262</sup>

In general, therefore, the technical design of namespaces should engineer openness, competition, modularization, decentralization and innovation-friendliness into the namespace. They should, in other words, be designed to cope with uncertainty: uncertainty, how a namespace will develop and uncertainty how a namespace will be used. Namespaces should enable, not control. Due to the general lack of predictability described above, remaining problems that occur in namespaces should be left to an *ex post* regulation, be it by law or technology. Yet, in some cases it may be clear from the outset that certain other values should be protected by the namespace. Such values may include the protection of privacy or

---

<sup>261</sup> For a general account of the importance of modularity in system design, see CARLISS Y. BALDWIN & KIM B. CLARK, *DESIGN RULES – THE POWER OF MODULARITY* (2000).

<sup>262</sup> Suppose, for example, that in an authentication system, information about the real name of the user, his age, address and preferences all are stored in one string of bits, which is the user's name in the authentication system. If a participating web site used this system as its authentication mechanism, it could receive much information about the user by merely receiving the name which the authentication system has assigned to the user. If, conversely, the user's attributes are not stored in the name itself, but in modularized components which are only linked to the name, the authentication system can transmit the user name to the participating web site without revealing the user's address, age and preferences. With modularization, even the transmission of globally unique user names can be avoided, as the Liberty Alliance project shows; *see supra* text accompanying notes 154-158.

copyright interests. In such cases, namespaces can be architected much more precisely to protect these interests.

These remarks are more of a call for light-weight namespace governance than an actual theory how namespaces should be designed. At any rate, ICANN's broad and intense control of the domain name space seems hard to justify under this line of thought.

## VI. CONCLUSION

Namespaces are an overlooked facet of governance both in real and cyberspace. Although we are surrounded by namespaces, policy discussions have regularly not taken any attention to general policy problems of namespaces. This paper has shown that the technical design of namespaces in general has numerous legal and policy implications. As analytical tools, the paper has developed several dimensions that prove useful in analyzing governance questions in 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. This taxonomic structure developed in the paper could be useful to legal scholars who think about the implications of various namespaces. It could also be useful to designers of namespaces who have to think about the legal and policy implications of what they are doing. Finally, it could assist lawyers and policymakers in becoming involved in governance discussions at the time of the technological design of namespaces. While the paper has focused mainly on namespaces in cyberspace, many of its findings can be applied to namespaces in real space as well.<sup>263</sup> As we are literally surrounded by namespaces both in cyberspace and real space, governance in namespaces could be a ubiquitous theme as well.

---

<sup>263</sup> The P.O. box system, for example, can be thought of 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; UPS, for example, does not offer P.O. box numbers that are compatible 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.