REFLECTIONS ON EXCLUSION AND COORDINATION IN CYBERSPACE: *THE CASE OF DOMAIN NAMES*

Margaret Jane Radin* and R. Polk Wagner**

Preliminary Draft, December 1996

I. THE DOMAIN NAMES SYSTEM 4
A. The Distributed, Coordinated Network 4
B. The Internet Addressing Standard 6
C. Domain Naming Conventions and Domain Name Registration Processes 11

II. DISPUTES OVER DOMAIN NAMES: DOMAIN NAMES AS INTELLECTUAL PROPERTY? 15
A. An Evolutionary Perspective on the Propertization of Domain Names 16
B. Mutant Trademarks? Or Something Else? 27

III. TOWARD PRIVATE ORDERING (PROPERTY AND CONTRACT) IN A GLOBAL NETWORKED ENVIRONMENT 33
A. The Internet as a Self-Ordering Legal Environment 36
B. The Limits of Self-Ordering? 41

* William Benjamin Scott & Luna M. Scott Professor of Law, Stanford Law School.

** J.D. candidate 1998, Stanford Law School.

Copyright © 1996 Margaret Jane Radin and R. Polk Wagner. *All Rights Reserved.*

INTRODUCTION

Anyone who has had occasion to look at any commercial websites or to send e-mail to a company has had contact with Internet domain names, of the form [commercial name].com. By now many people are familiar with netscape.com, microsoft.com, yahoo.com, etc. So far these names have been registered on a first-come, first-served basis to those who pay a small fee to an Internet governance organization. As the Internet has burgeoned into a commercial infrastructure, fierce disputes have arisen over domain names. Should "roadrunner.com" belong to an Internet Service Provider (ISP) named Roadrunner, Inc., or to Warner Brothers, the owner of the cartoon character who always bests Wile E. Coyote?[1] Brokering of domain names has sprung up. An enterprising man named

---

[1] Roadrunner Computer Systems offers Internet services. Since December 1995, Warner Brothers, Inc., the owner of the federally-registered trademark "Road Runner" has been seeking to block Roadrunner's use of the domain name "roadrunner.com." After Warner Brother's initial complaints, Roadrunner applied for and received a trademark registration in Tunisia. Memorandum In Support Of Plaintiff's Motion For Preliminary Injunction, Roadrunner Computer Systems, Inc. v. Network Solutions, Inc., No. 96-413-A, (E.D. Va. 1996). *Available at* http://www.patents.com/nsimemo.sht.

Toeppen has registered many domain names corresponding to big companies, apparently with the hope of "selling" them to the companies when those companies "wise up" about the necessity of a presence on the Internet.[2] A Vancouver company, MailBank, has spent U.S. $1,000,000 to register 10,000 domain names relating to popular family names, and is marketing them to those who desire personal domains corresponding to their surnames.[3]

These domain name disputes have caused a flurry of legal skirmishes and drawn forth quite a few commentaries and some policy initiatives. In this essay we will describe some of the skirmishes and initiatives, but our goal here is to focus on a deeper issue that the domain names problem surfaces — the issue of Internet self-organization and self-governance. Perhaps surprisingly to those who do not habitually hang out in Cyberspace, right now it is simply not clear who has the ultimate authority to grant out "ownership" — and revoke "ownership" — of a domain name. A domain name is an address; currently, they are the primary means of

---

[2] Toeppen owns names such as deltaairlines.com, eddiebauer.com, flydelta.com, frenchopen.com, lufthansa.com, neiman-marcus.com, northwestairlines.com, and yankeestadium.com, among many others. Panavision Int"l, v. Toeppen, et. al, _____ F.Supp. _____ , 1996 WL 65372 (C.D.Cal. 1996).

[3] *See* http://www.mailbank.com.

identification in Cyberspace. Questions about how to achieve a stable resolution of the domain names problem flow rather quickly into general questions about "bottom-up" versus "top-down" methods of achieving law, and about sovereignty and its connection to territoriality.

We will begin in Part I by describing some technical features of the Internet and of its governance, just enough to make the following discussion intelligible. Then in Part II we will consider the evolution of a property rights scheme in domain names, and the temptation to consider them a species of mutant trademark. Finally, in Part III we will use the domain names problem as a jumping-off point to reflect on the possibility of the Internet as a self-ordering legal environment. Self-regulation is seen by many Internet partisans as a very attractive possibility, mostly because it is seen as offering a realm of free choice and access to information never before possible. The alternatives involving conflicting and onerous territorial regulations seem unworkable and unattractive. Yet, at least as food for thought for these advocates, we offer cautions about the pitfalls and limitations of self-regulation.

I. THE DOMAIN NAMES SYSTEM

A. THE DISTRIBUTED, COORDINATED NETWORK

The essence of the Internet is its distributed — indeed, net-like — structure. There are an infinite number of possible paths between two points in Cyberspace. Communications are "routed" at each network junction, or "node", depending upon the localized traffic and routing information. The Internet thus does not depend upon any single node, computer, or even network link; it can compensate for problems in real-time.

The Internet's governance is similarly byzantine. In fact, the Internet is not governed — it is coordinated. The top-level coordinating body is the Internet Society (ISOC), an international non-governmental organization with open membership standards.[4] Technical development of the Internet is coordinated by the Internet Engineering Task Force (IETF), a loose group of individuals representing academia, industry, and users. The IETF,

[4] *See* http://www.isoc.org/. Individuals can join the ISOC for $35 per year.

through a series of small "working groups", proposes and establishes standards used across the global network. Standards are established not by decree, but by a quasi-formal process dictated by the slogan: "rough consensus and running code."[5] Standards developed by a Working Group are then considered by the Internet Engineering Steering Group (IESG — the managing body of the IETF), with appeal to the Internet Architecture Board (IAB — the technical group of the ISOC) , and finally promulgated by the Internet Society as international standards. An accepted standard is published in a document known as a "Request for Comment" (RFC — though not all RFCs are standards) — RFCs are published under the joint auspices of the IETF and the ISOC, and are essentially the governing documents for the Internet. The standard under which the Domain Name System operates is published in RFC 1034 and RFC 1035, both dated November 1987.

[5] The complete IETF credo is: "We reject kings, presidents, and voting. We believe in rough consensus and running code." See, John Stewart, *Presentation: IETF Structure and Internet Standards Process* (Sept. 9, 1994). *Available at* http://www.ietf.org/structure.html.

B. THE INTERNET ADDRESSING STANDARD

Each computer connected to the Internet has a unique address. The address, known as the IP (for "Internet Protocol") address, is a series of four numbers separated by periods, such as "36.190.0.136," where each number describes the network, the subnetworks, and the local address, respectively.[6] Communication among computers is achieved by transmitting and receiving a stream of small groups of data, called "packets". In addition to the data, each packet contains a destination address (among other things) — the destination address will be the IP address of the destination computer. At each network junction (or node), electronic devices known as routers read the destination address and pass the packet along a network link according to programmed internal rules. Thus, by "hopping" from router to router, the packet will eventually arrive at the destination computer, where the data will be used. This process will be repeated for each packet sent — typically, many thousands of packets

[6] In common Internet usage, the periods are known as "dots". In the given example, "36" is the network (assigned to Stanford University), "190" and "0" are subnetworks, and "136" is the local address of a computer attached to the Internet from within the Stanford network area.

will be sent and received in a single communication. All packets need not follow the same route: the communication will be divided into packets; the packets will travel the network *individually* according to the easiest path then available; and the communication will be recreated from the reunited packets as they arrive.

The IP address, then, is the street address of Cyberspace, the basic location descriptor of the Internet. It is what allows surety that the communications sent to a particular computer will be received by the destination device. All devices on the Internet must use the IP address system to be recognized by the rest of the Internet — without recognition, the device does not actually "exist" on the Internet. This "enforcement" of the IP address standard is not upheld by government decree, but rather by the "force" of coordination and the desire for network interoperability.[7]

Unfortunately, the IP address system is not very human-friendly, nor it is geographically descriptive. Therefore, in the early 1980s, the Domain Name System (DNS) was developed by the IETF to address the growth of the Internet by imposing a hierarchical naming system that would also be intuitively easier than the (unsystematic) assignment of IP

[7] *See infra*. note 63.

addresses.[8] The DNS overlays the IP address of each computer with a unique series of alphanumeric "words", also separated by dots, called a "fully-qualified domain name", or "domain name". Each domain name address corresponds to exactly one IP address — the domain name associated with 36.190.0.136 is "www.stanford.edu", for example. Each word also (generally) describes the machine's location in the Internet. The most generic term, the "top-level domain" (TLD), is furthest to the right ("edu" in the above example). The second word from the right is called the "second-level domain". Words furthest to the left are called "hostnames" or "hosts" and are the name given to the specific machine.[9]

---

[8] "In the long run, it will not be practicable for every Internet host to include all Internet hosts in its name-address tables. Even now, with over four hundred names and nicknames in the [current Internet] tables, this has become awkward. Some sort of hierarchical name-space partitioning can easily be devised to deal with this problem; however, it has been wickedly difficult to find one compatible with the known mail systems throughout the community. The one proposed here is the product of several discussions and meetings and is believed both compatible with existing systems and extensible for future systems involving thousands of hosts." D. L. Mills, *Internet Domain Names*, Request for Comments: 799 (Sept. 1981). *Available at* http://info.internet.isi.edu:80/in-notes/rfc/files/rfc799.txt

[9] Note that in the Domain Name System, it is possible to have fully-qualified domain names with four (or even more) words, such as "test.www.stanford.edu". In this case, "test" is the hostname, "www" is the "subhost", "stanford" is the domain name, and "edu" is the top-level domain. Similarly, it is also possible to name a computer or device with the domain name — "stanford.edu", for example. The nature of the DNS leads to this flexibility.

The Domain Name System is operated by a vast series of computers containing a database that matches the fully-qualified domain names with their corresponding IP addresses. Like the Internet itself, a key feature of the DNS database is that it is distributed — allowing the size of each sub-database to be manageable, and the entire system to be fast and flexible.

Each computer holding a portion of the DNS database is known as a domain name server, or "nameserver". Each nameserver has its own designated group of machines to keep track of; communication between the various nameservers allows any domain name to be matched with its IP address. The worldwide nameserver network structure is pyramidal, with a small number of "root" nameservers which point towards the "domain" nameservers, which in turn hold the domain name and IP address information for a particular domain.[10] The administrator of a domain is responsible for maintaining the nameserver which locates the hosts within that domain, while the root and other nameservers are

[10] In practice, there are actually several nameservers that create another level between the root nameservers and the domain nameservers — they hold information regarding the domain nameservers for many domains (this controls the load for "populated" top-level domains).

generally maintained voluntarily.[11]

When a domain name is used to establish communications with another computer, perhaps by typing the domain name in the "location" window of a World Wide Web browser, the local computer queries the local nameserver for that domain.[12] The local nameserver will run a "resolver" program that will determine which other nameservers to query for the IP address information; it may have the information stored locally, or it may require a query as "deep" as the root nameserver. The resolver will "resolve" (match) the IP address from the given domain name, and the packets of data will receive their numerical addresses and be sent on their way.

---

[11] As of November, 1996, there were nine root nameservers, hosted by Universities, ISPs, NASA, and the US Military.

[12] Common World Wide Web browsers (or "Web Browsers") are: Netscape Navigator, Microsoft Internet Explorer, Mosaic, and Lynx. Note that the same domain names system is used for all types of Internet communications using the TCP/IP ("Terminal Connection Protocol/Internet Protocol" - the Internet networking standard) protocol, such as FTP, Telnet, electronic mail applications, and HTTP (World Wide Web applications).

C. Domain Naming Conventions and Domain Name Registration Processes

The Domain Name System is hierarchical. The base level consists of a series of top-level domains (TLDs), both generic[13] and allocated according to political geography.[14] Within each TLD is a continuing hierarchy of names, with most second-level domain names directly under their respective TLD.[15] Further structure within the domains (such as hosts) is at the

---

[13] The generic TLDs are: "edu", "com", "net", "org", "gov", "mil", and "int". Each has specific restrictions regarding what organizations can register domain within them. For example, "edu" is (currently) restricted to four-year colleges and universities, "gov" is for the branches and departments of the US government, and "mil" is reserved for the US military. The "com" TLD, intended for commercial entities, is by far the largest. J. Postel, *Domain Name System Structure and Delegation*, Request for Comments: 1591 (Mar. 1994). *Available at* http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1591.txt

[14] See ISO-3166 for a list of current country codes.

[15] Some TLDs have established further structural organization. For example, in the "us" TLD, the structure is based on political geography (locality and state name) — if registered under the "us" TLD instead of under the "edu", Stanford University would likely have the domain name "stanford.santaclara.ca.us". Each state in the "us" TLD is also provided with special designation spaces for schools, governments, libraries, and museums. J. Postel & A. Cooper, *The US Domain*, Request for Comments: 1480 (June 1993). *Available at* http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1480.txt

discretion of the domain name holder.

Operation of the DNS requires close coordination between the administrators of the various nameservers. Without an entry in the DNS database, a domain name (and thus the corresponding device) effectively does not exist on the Internet.[16] Therefore, registration processes have been established for the allocation and use of domain names.

The overall coordinating body for the DNS is the Internet Assigned Numbers Authority (IANA). The IANA is chartered by the ISOC and the Federal Networking Council (FNC) and is operated by the University of Southern California Information Sciences Institute.[17] The IANA is responsible for the delegation of the TLDs, and has designated several regional bodies as the registration authorities for second-level domain

---

[16] Of course, the individual machine's IP address could be used for identification and communication, but the hierarchical organization and descriptive advantages of the Domain Name System would be lost.

[17] The FNC is a multiagency U.S. Government coordination body with the purpose of establishing an effective forum and long-term strategy to oversee operation and evolution of the Internet and other national computer networks in support of research and education. Its members include representatives of the Departments of Commerce, Defense, Education, Interior, and Energy. The FNC was created under the National Science Foundation.

Information regarding the USC ISI can be found at: http://www.isi.edu/

names within particular TLDs.[18] The primary international authority is the InterNIC, which is the registry for second-level domain names within the "com", "edu", org", "net", and "gov" TLDs. Registration administration for InterNIC is handled by Network Solutions, Inc. (NSI), a private for-profit corporation located in Herndon, Virginia.[19]

Registration for a domain name means being assigned a second-level domain name within a TLD.[20] Any organization or individual may register a domain name, provided that the organization can show that two nameservers are available to support the domain.[21] Second-level domain

---

[18] Typically, each country-level TLD has its own registration authority. The generic registrations are handled by InterNIC. Postel, *Domain Name System Structure and Delegation*, *supra* note 13.

[19] InterNIC is a "cooperative activity" between the National Science Foundation, Network Solutions, Inc. and AT&T. *See,* http://rs.internic.net/index.html. Network Solutions, Inc. (NSI) was founded in 1979 and claims to "serve more Internet users than any other company on the planet." *See,* http://www.netsol.com/netsol.html. NSI is a wholly-owned subsidiary of SAIC, a large defense contractor.

[20] The term "domain name" refers generally to the entire fully-qualified domain name, such as www.stanford.edu. The registration requirement, however, is for the second-level domain name ("stanford"). The TLD ("edu") is not 'selectable' (note the qualifications for registration under each TLD referred to in note 13, *infra*.), and the hostname ("www") is assigned and maintained by the administrator of the second-level domain name (in this case, Stanford University).

[21] This rule was established by the IANA and is administered by the InterNIC. http://rs.internic.net/help/domain/name-service.html

names are no more than 24 alphanumeric characters, and must be unique within the TLD.[22] Once a second-level domain name is registered, NSI places the registrant's nameserver addresses on the root nameservers, thereby "creating' the domain in Cyberspace. Since 1994, NSI has collected registration fees ($100 in November 1996) and maintenance fees ($50 for every year beyond two years) for the registration of second-level domains under its authority.[23]

---

[22] Note, however, that nothing limits the use of the same domain name within different TLDs: "stanford.com' is also registered (but not to Stanford University).

[23] *See*, ftp://rs.internic.net/policy/internic/internic-domain-3.txt: "Seventy percent of the fees collected will be retained by Network Solutions to cover operating costs and will be audited by NSF. The remaining thirty percent will be spent, with guidance from an advisory committee drawn from the Internet community, into the intellectual infrastructure of the Internet and will be publicly accounted for.' http://rs.internic.net/domain-info/billing-FAQ.html#5. NSI reports that "for the period September 14, 1995 through September 30, 1996, $7,072,450.00 has been deposited into the ["intellectual infrastructure'] account. . . [T]here have been no disbursements from the account.' http://rs.internic.net/announcements/iif-update.html.

Other registration authorities (with other TLDs) may offer different pricing schemes — the "us' TLD is generally free. http://www.isi.edu/in-notes/usdnr/usdom-overview.html.

II. DISPUTES OVER DOMAIN NAMES: DOMAIN NAMES AS INTELLECTUAL PROPERTY?

Domain names are addresses. In fact, domain names are simply overlays for addresses — a means by which the complexity of the Internet networking protocols are separated from the user. Domain names require registration, but that registration requirement developed from a need for coordination, rather than a desire to limit the use of the "resource.' Communication could not take place — at least not without massive confusion — without coordination to ensure that no two computers have the same address. Why, then is there such a fracas over the protection and limitation of domain names as a form of property?

A. An Evolutionary Perspective on the Propertization of Domain Names

It is important to recognize first that it is not a foregone conclusion that domain names should be governed by a property regime at all.

Perhaps they should be non-property (part of the public domain or commons). Things that are in the public domain can be appropriated to your own use, but (at least in a theoretical pure commons) you are in a state of nature in which you keep them only as long as you can defend against others' efforts to take them.

There are lots of theories about how one gets from a pre-legal state of nature to a property regime, and indeed more that question the utility of the state of nature theoretical construct. In this essay, we will bypass these questions, interesting as they are, and just talk about the utilitarian/economic framework that is conventionally invoked when discussing intellectual property in this country. One way, then, to think about whether or not something will be or should be treated as property — "propertized' — is to do a cost-benefit analysis. A simple evolutionary economic theory of property holds that property rights come into existence when the enforceable right to exclude others yields a gain, in benefits internalized to owners, which outweighs the costs of implementing the system of exclusion.[24] The costs include not only the cost of the legal system of rights and remedies but also the costs of the profits foregone by

[24] Harold Demsetz, *Toward a Theory of Property Rights*, 57 AM. ECON. REV. PAP. & PROC. 347 (1967).

owners who must respect the boundaries of others' property rights in return for having their own respected; the costs of mutual exclusion. This basic evolutionary theory predicts that when a resource is very plentiful, or not valued highly, or very costly to protect, a property system won't be worth implementing, and the resource will remain in the public domain. When conditions change, and the resource becomes more scarce, more highly valued, or less costly to protect, a property regime will come into being.[25]

Whether or not such a property regime is normatively appropriate — whether there ought to be such property rights — is a separate question. If economic efficiency is to be the benchmark of normative appropriateness, as it is for many theorists of intellectual property, then we need to ask whether evolutionary processes arrive at efficient results. This is a question about which academics intensely dispute, and which is beyond

---

[25] *Id.*; This simple evolutionary model does not play out in practice all of the time, and the circumstances under which practice will turn out differently are an important topic of study. See Elinor Ostrom, *Governing the Commons*; Carol Rose, *Property as Storytelling: Perspectives from Game Theory, Narrative Theory, and Feminist Theory*, 2 YALE J. L. & HUMANITIES 37-57 (1990). The simple theory does appear to fit the facts of the history of domain names, at least at first glance, however. At second glance, it might be more accurate to say that a non-commercial (non-commodified) regime, in which market rhetoric does not well describe incentives and outcomes, gave way to a conventional (commodified) regime, in which it does.

the scope of this essay, although it's important to think about.[26] (If you believe in evolution to efficiency, then you will tend to believe that the status quo is right, and that has important political ramifications.)

The "story" of domain names can be described in evolutionary terms. When the DNS was instituted in the early-to-mid 1980s, the Internet was a non-commercial research and communication tool, originally supported by ARPA and administered by a loose network of researchers and academics. The original concept of the domain name system was as a name-space commons, not as a system of property rights.[27] As in all commons, "the first-come, first served" concept governed use rights[28] — in fact, this continues today, with "first-come, first-served" being the registration policy for second-level domain names. The designers of the DNS were creating a method of administering the name-space commons for the

---

[26] Mark Roe, [Chaos and economics article], HARV. L. REV., Bob Cooter, [Customary Law Article], CAL. L. REV. [?]

[27] J. Postel, *The Domain Naming Convention for Internet User Applications*, Request For Comments: 819 (Aug. 1982); P. Mockapetris, *Domain Names - Concepts And Facilities*, Request For Comments: 1034 (Nov. 1987).

[28] M. Stahl, *Domain Administrators Guide*, Request For Comments: 1032 (Nov. 1987).

convenience of all, not a method of selling names as private property.[29] It wasn't necessary to give serious thought to rights or ownership, or even what might happen if Joe tried to take Mary's domain name. Since Joe could easily (and prior to 1994, freely) get his own domain name that would, given noncommercial purposes, be as good as the one he could take from Mary, there seemed to be "enough and as good" left in common after Mary appropriated hers.[30] Demand for domain names, until recently, was comparatively low: the InterNIC reports that in October 1995, there were 156,943 total domain names registered; by September 1996, that figure had risen to 654,702.[31] There was (and is) little possibility of actually "stealing" a domain name — the technological barriers of the DNS system precluded out-and-out theft. These technological and social circumstances meant — continuing with the market rhetoric of the economic paradigm — that enforceable property rights were not worth the price of implementing them.

Then a few years passed, and the world changed. The Internet came

---

[29] "Concerns about "rights" and "ownership" of domains are inappropriate." Postel, *Domain Name System Structure and Delegation*, *supra* note 13.

[30] Locke [cite incomplete]

[31] http://rs.internic.net/nic-support/nicnews/nov96/demo.html

to be understood as a commercial infrastructure of very great potential power. The individual names started to look both scarce and very valuable. They started to look scarce not because of the numbers of them available, but because of the much smaller numbers that Internet entrepreneurs came to deem desirable.[32] They started to look very valuable because there is monetizable value in commercial names in a way that there isn't in noncommercial names.[33] Demand mushroomed, as did registration.[34] As the simple economic model would predict, a trade in names grew up; and the

---

[32] Though some argue that sheer numbers is the problem, this seems overly superficial — since second-level domain names can be at least 24 characters, potential names are amply numerous. Indeed, if a particular TLD's domain space is near capacity, one would suspect that new registrants would use alternative TLDs. The real problem is two-fold: first, businesses want to use the flexible nature of the domain names to describe their business accurately ("apple.com" is much better than "aapl.com" or some other such combination); second, businesses believe that the "com" TLD space is the only feasible "address" to have. Thus, since domain names must be unique, demand for "good" domain names (as defined by each potential registrant) is high, but demand for less good domain names is much lower.

[33] By analogy to physical space, businesses understood an important factor in the success or failure of their on-line venture to be *location*. "Location" in Cyberspace means domain names. Just as a premium location in physical commercial space commands high prices, the high-rent district of the Internet is the "com" TLD. This rush to "stake out" valuable domain name space is driving the exponential growth in domain name registrations.

[34] In September 1996, 75,213 new domain names were registered, an increase of over 375 percent from October 1995. http://rs.internic.net/nic-support/nicnews/nov96/demo.html

expenses of exclusion became worthwhile. Conflicts developed over domain names.[35] Businesses and individuals began advertising domain names for sale; it was rumored that domain names changed hands for sums on the order of $100,000.[36]

In these circumstances, a clear property rights regime, with clear enforcement mechanisms, seemed to be needed to avoid the typical costly free-for-alls when non-commercial commons resources suddenly become commercially very valuable. An example of this is the problem of "squatting". Cyberspace has its own form, predictably called "cybersquatting" or "domain name grabbing". Domain name grabbing refers to the practice of registering for a domain name that the registrant

---

[35] A Wired and Newsday reporter, Josh Quittner, registered the domain name "mcdonalds.com" after trying unsuccessfully to prod McDonalds into a comment on the subject. Quittner then asked readers to send in suggestions for the domain. Quittner, *Billions Registered*, WIRED 2.10. *Available at*: http://www.hotwired.com/wired/2.10/departments/electrosphere/mcdonalds.html) McDonalds eventually complained to NSI, claiming trademark infringement. Quittner relinquished the domain in exchange for the donation of computer equipment (including an Internet connection) to a New York public school. Victoria Slind-Flor, *Domains are there for the Taking*, NAT. L. J., June 5, 1995, page A7.

[36] *See* "BestDomains" web site, styled as "the largest Global Internet Name & Asset Trading Site". http://www.nasa.org/buysell/index.html. The BestDomains site has this to say regarding the price of domain names: "The short answer is, an Internet Domain Name is worth what ever some one is willing to pay, or sell it for. Domain names have sold for prices ranging from $250 to over $95,000."

speculates will be of value. The typical case involves the registering of a domain name corresponding to a major corporation or product (almost always a recognized trademark). The domain name "grabber", who can effectively block the corporation from the domain name, then offers to "sell" the domain name to the corporation.[37]

Suddenly, in July 1995, NSI, in response to several cases of domain name disputes leading to legal action (including against NSI), promulgated the Domain Name Dispute Policy. Broadly speaking, the Policy (which has been amended three times since) allows trademark holders to file a complaint with NSI regarding violations of "legal rights" by a domain name. After receiving a proper complaint, NSI will encourage the domain-holder to relinquish the domain name. The domain-holder then has the burden of

---

[37] A recent case is Panavision Int"l v. Toeppen, et. al, ___ F.Supp. ___, 1996 Westlaw 653726 (C.D. Cal. 1996). Toeppen registered the domain name "panavision.com" and demanded $13,000 to relinquish it to Panavision. (The court noted that "Toeppen's "business" is to register trademarks as domain names and then sell the domain names to the trademarks" owners." Id. at *6.) Toeppen reportedly has registered approximately 240 domain names, most relating to well-known trademarks. Panavision sued Toeppen in Federal Court, claiming trademark infringement, state and federal trademark dilution, and federal and state unfair completion, among others. Panavision prevailed on the dilution claims on summary judgment; Toeppen was enjoined from using the "panavision.com" name and required to transfer it to Panavision.

proving ownership of its own trademark corresponding to the domain name within 30 days to avoid a "hold" status. If the disputing parties cannot reach a resolution, NSI will place the domain name on "hold" pending further action. When a lawsuit is filed over the allocation of a domain name, the NSI will deliver allocation authority to the court.[38] Whether the Policy is a good one is open to serious question. The policy allows trademark registration from foreign jurisdictions to trump senior use rights under U.S. law. It allows trademark holders to get the equivalent of an injunction before the merits have been heard. In practice, it may be making matters worse rather than better.[39]

---

[38] InterNIC, *Domain Name Dispute Policy*, http://rs0.internic.net/domain-info/internic-domain-6.html.

[39] In Panavision, the court noted: "the policy has not proven effective in resolving domain name conflicts." Panavision, *supra* note 37, FN 2, *10.

It's important to understand that the NSI essentially abandons the policy established by RFC 1591, which allocates the authority for Internet Registration to InterNIC (and who in turn has contracted with NSI for the registration services). While the policy purports to avoid interjecting NSI into disputes between trademark owners and domain-holders, it effectively places NSI in the position of analyzing (at least in a preliminary manner) the competing claims of a domain registrant and a trademark owner.

The NSI policy appears to have two interrelated intentions. The first seems sensible: preventing NSI (and InterNIC and the NSF) from being impleaded into every domain name-trademark litigation. Second, the policy is clearly a response to complaints from trademark owners that domain name registrants were violating their "rights" — complaints fueled by the enthusiastic media coverage of the "David

A great deal of debate is going on right now about the merits or demerits of the Dispute Policy. At least it's evident from an evolutionary point of view that some such policy would be expected to come into existence when it did. It's also important to bear in mind that evolution doesn't stop. This point is logically anterior to arguing the pros and cons of the current NSI/InterNIC approach. History could move on from here, changing the social, technological and economic parameters, and cause the perceived need for property rights in domain names to subside.

One thing that could happen is that domain names could become less valuable. The demand for them could ease: the IANA could create more

---

and Goliath" situations such as McDonalds. Thus, NSI (and its lawyers) must have determined that a policy which supports the interests of the trademark holders was the wisest course, though they did maintain the registration policy of "first-come, first-served".

The Dispute Policy thus allows trademark owners to quickly, easily, and cheaply assert a claim against a domain holder. By complaining to NSI, the trademark owner can get an offending domain name put on hold, without legal costs. In fact, given the territorial and compartmentalized nature of trademark law, one wonders if the claims to NSI are motivated by fear of public confusion or simply by a desire to procure the most appropriate domain name.

There are several thorough analyses of the Dispute Policy available on the Internet. See, e.g., D, Graves, *Domain Name Issues & Policies*, http://rs0.internic.net/presentations/daveg/ispcon/sld001.html (presenting the NSI view); C. Oppedhal, *Analysis and Suggestions Regarding NSI Domain Name Dispute Policy*, (unpublished manuscript dated August 8, 1996, *avaialbe at* http://www.patents.com/nsi/iip.sht) (criticizing the NSI approach).

TLD's;[40] and/or competitors to InterNIC could become viable.[41] Or the importance of domain names could subside: sophisticated search engines, "smart browsers", agent applications, or other technological innovations could perhaps render them largely irrelevant.[42]

---

[40] The recent formation of the Internet International Ad-Hoc Committee (IAHC) signals impetus towards reform. See, K. Hart, *New setup takes hold of Net*, COMMUNICATIONSWEEK INT"L, October 21, 1996, Pg. 8. *See* http://www.iahc.org/ for details.

[41] John Postel, one of the "founders" of the Internet, recently suggested that the DNS be reformed to allow at least "two-dozen" new US TLDs and "introduce competition in the top-level domain registration business so that market forces will ensure fair prices for good services." J. Postel, *New Registries and the Delegation of International Top Level Domains* (Oct. 1996). *Available at* ftp://ftp.isi.edu/in-notes/iana/administration/new-registries.

There already are unofficial competitors to InterNIC. An organization named AlterNIC has established 39 "alternative" TLDs. However, since InterNIC does not include these TLDs on the root nameservers, connection to these TLDs through the DNS is sporadic, and their use limited. http://www.alternic.net/

[42] In this context, "search engines" refers to both "full-text searching", where the user inputs key words or phrases and the engine (usually through a Web page interface) return a list of pages containing the text, and "indexing" where web sites are categorized. A physical space analogy to full-text searching would be a phone book's white pages; an index is more similar to the "yellow pages". See "AltaVista" at www.altavista.com for an example of full-text searching. "Yahoo", at www.yahoo.com, is an excellent example of a Web index.

Smart browsers would integrate the searching functions into the user's software. Instead of interfacing with a search engine through a Web site, a user would simply type the search terms or phrases into the browser itself. This effectively adds a software layer between the user and the address, and subtracts a layer of tasks for the user.

Agent applications, or "intelligent agents" are software applications that can perform complex tasks independently upon direction from a user. An example is the

When we think about the "propertization" of domain names, we should not conflate physical address and intellectual "address." Trademarks are needed for the latter, not the former. Companies and individuals in the real (non-virtual) world don't necessarily have to use trademarks as a physical address. Customers can find a Bloomingdale's store without its being located on Bloomingdale Street. In physical space we have inexpensive techniques for matching locations to companies, so it isn't cost effective for Bloomingdale's to try to see to it that its physical location is named after it, perhaps by spending big bucks lobbying for enforceable street name guidelines to be made mandatory for city planners or the like. We might expect the same kind of thing to happen with virtual locations in Cyberspace. If so, domain names will be superseded by other methods of identification. If so, domain names aren't going to be a valuable piece of intellectual property worth investing in.

Anderson Consulting "BargainFinder" agent. BargainFinder "comparison shops among Internet stores to find the best price for a compact disc." B. Krulwich, *An Agent of Change*, http://www.ac.com/cstar/hsil/agents/framedef_art_bf.html. *See generally*, S. Lohr, *New Internet Search Engine Said to Ease Hunt for Sites*, N. Y. TIMES, May 21, 1996 Section D; Page 6; Column 5.

B. MUTANT TRADEMARKS? OR SOMETHING ELSE?

It has been tempting for the various players in the commercial transformation of the Internet to consider domain names a species of mutant trademark. A domain name that matches a trademark does have at least one similar function: to identify the service or product of the owner. And it can have value to the owner in the same way that the goodwill attaching to any other commercial name can have value: the value is the commodified propensity of customers to choose the named product over competing products. Moreover, trademarks are in a sense appropriated out of the commons of language just as domain names are appropriated out of domain name space. [43] An additional advantage of a domain name is that it can be valuable both in the sense of trademark-type "recognition" (conceptual location) and address implementation (operational location). The consumer can choose products based on the value of the mark, and use the mark to find information about the product.

---

[43] Traditionally, in this country, trademarks have been "appropriated" from the language commons by using the words in commerce, gaining a commercially valuable meaning for the user. Registration has been seen as a mechanism of confirmation, not a mechanism of establishment of property rights.

The temptation to consider domain names as mutant trademarks has unfortunately been troublesome. There are important features of domain names that aren't analogous to traditional trademarks. We will call these non-analogous features territorialization and compartmentalization. Trademarks traditionally have been territorially-based, meaning that the property right is only good in the territory in which the user's rights have been established, so firms located in different territories could own the same mark. Moreover, trademarks traditionally have been compartmentalized, meaning that the property right is only good in the industry in which the user's rights have been established, so that firms engaged in different lines of business could own the same mark.[44] But

[44] Trademark infringement analysis uses a several-factor test, including: the strength of the infringed mark, the degree of similarity between the two marks, the proximity of the products, the area and manner of consistent use, the strength of the infringed mark, actual confusion, intent by the infringer to confuse, and the sophistication of the buyers. See, e.g. Polaroid Corp. v. Polaroid Electronics Corp., 287 F.2d 492 (2d Cir. 1961), *cert. denied*, 368 U.S. 820 (1961); Forum Corp. of North Am. v. Forum Ltd., 903 F2d 434, 439 (7th Cir. 1990). Note that the above analysis explicitly does not preclude concurrent use, a fact recognized by the statute: if the Commissioner determines that confusion, mistake, or deception is not likely to result from the continued use by more than one person of the same or similar marks under conditions and limitations as to the mode or place of use of the marks or the goods on or in connection with which such marks are used, concurrent registrations may be issued to such persons when they have become entitled to use such marks as a result of their concurrent lawful use in commerce . . . 15 U.S.C. 1052(d) (1994).

fully-qualified domain names are unique: there is only one Internet, one "com" TLD, and one IP address corresponding to any given name in that domain. Therefore, under the current regime, different companies in different places can't share the same name.[45] Domain names are unterritorialized and non-compartmentalized. If Apple Computer is the first to claim "apple.com," then Apple Records is out of luck.

Additionally, trademark law expressly reserves large portion of the commons of language — it does not allow the registration of "merely descriptive" terms.[46] "Computer" cannot be a registered mark for a computer product. In contrast, domain name space has no such limitations — therefore, the most valuable domain names are clearly the most generic.[47] Moreover, trademarks that become generic can lapse back into commons, but an appropriated domain name (as long as the servers supporting it are maintained) cannot.

---

[45] Unless they are willing to use different TLDs. *See supra* notes 40 and 41 regarding proposals to expand the number of "official" TLDs.

[46] 15 U.S.C. § 1052(e)(l) (1994)

[47] C|Net, Inc. reportedly paid about $50,000 for "news.com" M. Allen, Seeing Ad Dollars, C-Net Multiplies Web Sites, The New York Times, September 16, 1996 Section D; Page 4; Column 1. Also see, BestDomains, offering "classifieds.net" for $175,000,000. http://www.nasa.org/domains/special.html.

Traditional trademark law is in flux right now. There is pressure to "unterritorialize" it — harmonize national regimes and make it possible to have worldwide rights. At the same time there is pressure to "decompartmentalize" it — eliminate industry compartmentalization and make it possible to have comprehensive rights over a name for all products. Because the concept of dilution tends towards unterritorialization, it is no accident that most domain names cases in this country so far have relied on the new federal anti-dilution statute, the Federal Trademark Dilution Act of 1995.[48] This statute does decompartmentalize, but only for "famous" trademarks.[49] The Act thus creates a hierarchy: "famous" marks can exclude all others from

---

[48] *See, e.g.*, Panavision, *supra* note 37.; Intermatic, Inc. V. Toeppen, No. 96 C 1982, 1996 U.S. Dist. LEXIS 14878 (N.D. TX 1996); American Std. Inc. V. Toeppen, 1996 U.S. Dist. LEXIS 14451 (C.D. IL 1996).

[49] Senator Leahy, in remarks just prior to the passage of the act, stated that he hoped the Act would help "stem the use of deceptive Internet addresses taken by those who are choosing marks that are associated with the products and reputations of others." Cong. Rec. Dec. 29, 1995, S19312.

The criteria established for determination of a "famous" mark is: (1) the degree of inherent or acquired distinctiveness of the mark (i.e., its strength); (2) the duration and extent of use of the mark; (3) the duration and extent of advertising/publicity of the mark; (4) the geographical area in which the mark is used; (5) channels of trade for the good or services with which the mark is used; (6) the fame of the mark in the trading areas; (7) the nature and extent of use of similar marks by third parties; and (8) whether the mark is federally registered. 15 U.S.C. § 1125(c)(l) (1994).

duplicating their names, whereas others can exclude only those in their own and related product markets. Owners of "famous" marks can use this statute to capture the domain name they want, even if someone else got it first, but owners of non-famous marks seem to be out of luck.[50]

If trademark law were to go all the way toward un-territorialization and de-compartmentalization, then it would clearly be less procrustean for application to domain names. It's unlikely, however, that this could happen. It would require both unterritorialized scope of validity of trademarks and an unterritorialized background legal system to enforce them.[51] If trademark law could somehow become un-territorialized and de-compartmentalized it would become almost useless for all but the McDonald's and Disney's of this world. The widespread scope and recognition of major brands would allow them to be enforced in all commercial settings worldwide, at the expense of local firms. It is hard to

---

[50] Traditional (non-dilution) infringement analysis requires a showing of "likely confusion"; the dilution standard requires only a claim that the value of the mark is lessened. *See*, Panavision, id.; Toys "R" Us, Inc., v. Akkaoui, 1996 U.S. Dist. LEXIS 17090 (CD Cal, 1996) (declining to consider infringement claims after finding dilution). *See also*, Intermatic, Inc. v. Toeppen, 1996 U.S. Dist. Lexis 14878, ND Ill., Oct. 3, 1996) (finding dilution, but not finding traditional infringement).

[51] The prospects of world government seem weak. See *infra*. note 53 and accompanying text.

imagine a regime in which every firm in the world could have a different name and make it commercially viable, especially if we want most business owners to be free to use their own surnames if they want to. If we still want to be able to protect the goodwill of local firms" marks against unfair competition, then either trademark law has to somehow stop short of going all the way down the road toward un-territorialization and de-compartmentalization, as the Trademark Dilution Act of 1995 does, or some other regime has to be implemented. But as long as trademark law does stop short of going all the way down this road, it won't truly fit the current facts of domain names.

III. TOWARD PRIVATE ORDERING (PROPERTY AND CONTRACT) IN A GLOBAL NETWORKED ENVIRONMENT

It is obvious that the Internet forces us to ask questions about un-territorialization. This question arises any time we try to think about enforceable rights of any kind in Cyberspace, not just when we try to think

about domain names.[52] The domain names issue is a good point of entry into the problem of sovereignty in Cyberspace. Whoever wants to establish a commercial presence on the Internet must acquire a domain name, and the questions of who has the authority to grant them, what is a permissible use, who will sanction transgressions, etc., immediately arise. These issues permeate the nascent law (or "law") of Cyberspace. The Internet, almost by definition, collapses our traditional notions of location and the significance of geography for sovereignty and regimes of law. Who will decide what rights there are and who will enforce them? Will territorially-based jurisdiction and choice of law as we have known them become obsolete? (Next year, or 40 years from now?)

It is possible to make some basic conjectures. First, the internet is transnational. It will not be "within" the territorial jurisdiction of any

---

[52] Addressing the challenges of copyright, Jane Ginsburg noted:

> "A key feature of the [Internet] is its ability to render works of authorship pervasively and simultaneously accessible throughout the world.
>
> The principle of territoriality becomes problematic if it meas that posting a work on the [Internet] calls into play the laws of every country in which the work may be received when . . . these laws may differ substantively."

Jane C. Ginsburg, Global Use/Territorial Rights: Private International Law Questions of the Global Information Infrastructure, J. COPY. SOC. 318, 319-320 (1995), *quoted in* David R. Johnson and David G. Post, *Law and Borders: The Rise of Law In Cyberspace*,

sovereign nor subject to rules centrally laid down, unless we develop world government. It seems safe to say that we are not going to have world government with a central planning authority any time soon. The Internet is at least potentially a global market infrastructure of tremendous value, and we can postulate a general tendency of transnational markets to bring social and political coalescence in their wake. But that process is slow.[53] Second, in the meantime, we might look to international organizations and treaties to accomplish something similar on a piecemeal basis. Imagine an international Internet governance authority that would be charged with laying down rules about access to domain names. But this authority would only be authoritative if its decrees were accepted by every national sovereign, and that would require a full-scale "network" of treaties. We could also imagine a piecemeal process of treaty-making, issue-by-issue — a Domain Names Property Rights Enforcement Treaty,[54] and similar accords for other kinds of intellectual

---

[53] Witness the European Union: [30?] years after the common market was instituted there has been substantial development of overarching community law but the process is far from complete. [Cite]

[54] Such a treaty could be either directed at trademarks in general or domain names in particular. It might provide for enforcement by referring disputes to the judicial processes of the signatories. For example, Ann Gundelfinger, Trademark Counsel to Sun Microsystems, proposes that domain name registries require, as a condition of registration, that holders agree to jurisdiction in the courts of the

property rights on the Internet. These other kinds of accords are in process — chiefly the Berne Convention and the TRIPS provisions of GATT. Their history shows at minimum that the process is uneasy and incomplete.[55]

A. THE INTERNET AS A SELF-ORDERING LEGAL ENVIRONMENT

Another possibility is to consider the Internet as its own sui generis

country in which the registry is located for the purposes of resolving disputes. [Cite: Gundelfinger, Remarks at Fenwick & West Symposium] Virtually all trademark/domain name disputes relate to the "com" TLD, whose registration authority InterNIC, is located in the United States, so such a proposal might be favored by U.S. companies. However, approximately 30 percent of recent registrations in this TLD are non-U.S. entities, so it is unclear whether their respective sovereigns would enter into an arrangement that cedes jurisdiction in this way. [Cite: Radcliffe, remarks at Digital Content Conference]

[55] *See, e.g.*, David Nimmer, *The End of Copyright*, 48 VAND. L. REV. 1385 (noting the "end of the [American] experiment" in autonomous copyright law with the passage of GATT/TRIPS.); R. Krupka, P. Swain, R. Levine, *Section 337 And The Gatt: The Problem Or The Solution?*, 42 AM. U.L. REV. 779 (Spring, 1993) (Arguing that GATT/TRIPS provisions limit the ability of US corporations to protect intellectual property domestically.)

Johnson and Post assert that international treaties are unlikely to be successful in regulating the Internet, primarily because of "regulatory arbitrage" — counties not adhering to a treaty could become the "locations" for those who wish to avoid the treaty rules, or such countries could be virtually excluded from the commercial aspects of the Internet altogether. Johnson & Post, *supra* note 52.

jurisdiction, with its own self-governance and enforcement mechanisms. Given the apparent difficulties of using top-down processes to accomplish un-territorialization, many who are interested in the Internet are thinking about spontaneous ordering (self-organization) rather than planning.[56] They are thinking about laws, customs, and technological standards which are

---

[56] *See*, Johnson & Post, *supra* note 52; I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace"*, 55 U. PITT. L. REV. 993, 1051-1053; David R. Johnson and David G. Post, *And How Shall the Net Be Governed? A Meditation on the Relative Virtues of Decentralized, Emergent Law*, (draft dated 9/5/96, *available at* http://www.cli.org/emdraft.html). (advocating self-ordering and coordination over sovereign-introduced legal rules).

These dichotomous categories (spontaneous ordering versus centralized planning) seem to be derived from the work of Friedrich Hayek. The categories tend to oversimplify the understanding of real-world institutions, since many of them represent spontaneous ordering from one perspective and top-down rule-making from another. For example, Hayekians tend to see governmental regulation as central planning (a poor substitute for the spontaneous ordering of contracts in a laissez faire market). Yet public choice theorists, who are at least intellectual cousins of Hayek, tend to see regulation itself as the output of a market (and hence a form of spontaneous ordering). Moreover, the network of contracts necessary for the market to work its spontaneous ordering depends, of course, on pre-existing tradeable entitlements and the availability of reliable enforcement mechanisms; and those, in turn, depend upon at least a minimal state that can lay down rules. These considerations are cautions for those "Netizens" who seem to advocate anarchic self-regulation through contract in Cyberspace while presupposing enforceable alienable entitlements. They do not -- we think -- render these categories useless as a first cut at describing features of efficient approaches to law in Cyberspace.

not "laid down" but instead "grow up".[57] One important, indeed urgent, question for study is whether open technological standards can grow up as the result of market interactions without governmental intervention.[58] The question we are drawing attention to here is analogous. It is important to study how — under what social, economic, and technological circumstances — un-territorialized regimes of property and contract might grow up on the Internet.

In this regard it is interesting to ask why almost everyone in the world seems to be accepting InterNIC's authority to dole out domain names.[59] No world government or treaty granted it this power, nor

---

[57] Hardy notes the arise of the "Law Merchant" in the medieval trade context — a growth of customs and practices consisting of certain principles of equity and usages of trade which benefitted the merchants as a whole. Hardy, *supra* note 56.

[58] Renaissance Committee, National Academy of Science, *Realizing the Information Future: The Internet and Beyond* (1994), *available at* http://www.nap.edu/nap/bookstore/0309050448.html. Also available in condensed form in Marjory S. Blumenthal, *Realizing the Information Future: Technology, Economics, and the Open Data Network*, in TOWARD A COMPETITIVE TELECOMMUNICATION INDUSTRY 275 (Gerald W. Brock ed., 1995).

[59] To be sure, there are dissenters, such as AlterNIC, but their impact to date has been limited. See *supra* note 41.

confirmed in it the sovereign ownership of the name space.[60] Indeed, in the early days of this country there was more question about the authority of the U.S. government to grant out land within its own territory, until Chief Justice Marshall held that "[c]onquest gives a title that the courts of the conqueror cannot deny[.]"[61] It would be unimaginable to suppose that our government could validly grant land somewhere else in the world. Yet it appears that a quasi-private body, InterNIC, is able to dole out "virtual land" in Cyberspace (in the form of a domain name space).

We can usefully conjecture that the ".com" and the other un-territorialized top level domains are held together by tacit coordination which all understand to be profitable.[62] The system administrators choose

---

[60] To be sure, U.S. government funds certainly contributed to the initial research and development of the Internet, and government funds still support InterNIC — the cooperative agreement which established InterNIC stipulated a grant of $4.2 million over 57 months. *NSF Cooperative Agreement No. NCR-9218742*, *available at* http://rs0.internic.net/nsf/agreement/agreement.html. But the U.S. government has never implicitly or explicitly granted the authority of the IANA, the InterNIC, or other Internet quasi-governance bodies.

[61] Johnson v. M"Intosh, 21 U.S. (8 Wheat) 543 (1823).

[62] Alternatively, it could be the case that the wide acceptance was an artifact of the earlier non-commercial Internet, and that it will now unravel under market pressures. It could be the realization by commercial actors of the magnitude of InterNIC's authority, as well as displeasure with its practices, that has led to the calls for additional TLDs, competition among registration authorities, and calls for legislation to regulate domain names and trademarks. Note the recent creation of a formalized international body (IAHC) to generate proposals for the reform of the DNS

to point their nameservers at the "official" InterNIC root nameservers in order to gain the most reliable connection to the broadest array of other domains. The businesses and individuals registering new domain names follow the conventional perception that the "com" TLD is the most valuable one. The unplanned yet systematic coordination among the widely varied parties using the Internet has firmly established the international TLDs (especially the "com" TLD) and InterNIC as de-facto the sole authoritative body regarding domain names.

This is the same process that can create and maintain technological standards, when the conditions — which we don't fully understand and must study — are right. As David Johnson and David Post note:

> The [Internet] itself solves an immensely difficult collective action problem: how to get large numbers of individual computer networks, running diverse operating systems, to communicate with one another for the common good. And, yet, the net is really nothing more than a set of voluntary standards regarding message transmission, routing, and reception. There is not now and never was a central governmental body that decreed or voted to adopt a law stating that TCP/IP is required to be used by those wishing to communicate electronically on a global scale, or that HTTP is required to be used if you wish to communicate

system. J. Postel, *New Registries and the Delegation of International Top Level Domains*, *supra* note 41.

> over a particular portion of the global network (the World Wide Web). If you connect to a neighboring host and send out packets of data that conform to the protocol, your messages can be heard by others who have adopted the protocol. All are free to decline to follow the standard and to obey some other protocol, and they will communicate only to those who, literally, speak their language.[63]

If tacit coordination is the right way to think about what gives InterNIC its authority, then we need to consider what types of issues are amenable to tacit coordination. What kinds of problems involving necessary mutual exclusion and forbearance can be solved through sovereignless, un-territorialized, self-organizing coordination, and perhaps even more importantly, what kind of problems can't? What kinds of problems involving necessary cooperation and standardization can (and cannot) be solved in this way?

B. THE LIMITS OF SELF-ORDERING?

We are not aware of any algorithm that describes the circumstances under which a regime of exclusion rights and mutual forbearance — an entitlement regime — is likely to come into being through self-organizing

---

[63] Johnson & Post, *And How Shall the Net Be Governed*, *supra* note 56.

coordination. Achievement of stability in self-regulated commons is often thought to be dependent on the degree to which the cooperators are a close-knit, homogeneous cultural group.[64] The old noncommercial Internet was such a group, but the new commercial Internet is not. Additionally, stable coordination is often thought to be easier to achieve when the possible points of agreement are stable and obvious, and when deviance by any player is very difficult and/or readily apparent.[65] It seems that the existence of the domain names scheme at least roughly fits these parameters. It was developed by a close-knit homogeneous cultural group (which might loosely be characterized as the "techie-educational community"); its protocols were (and are) easy to adhere to; and deviance was (and is) difficult.

Once a scheme of exclusion rights and mutual forbearance comes about, it is still a question whether the scheme can be stably enforced through internal self-organizing mechanisms or whether it will degenerate unless uniform enforcement mechanisms are laid down from above. Is the domain names scheme — and ordering on the Internet in general — a case

---

[64] *See, e.g.*, Robert C. Ellickson, ORDER WITHOUT LAW (19__).

[65] *See, e.g.*, Thomas Schelling, STRATEGY OF CONFLICT (19--); [add cite on Tit-for-Tat]

in which regulation is now required, or one in which the development of protection schemes can instead be left to the same coordination process that gave rise to the exclusion rights themselves? Many Internet commentators are adopting the view that networks of contracts among participants — spontaneous free-market ordering — can substitute for external regulation. For example, Johnson and Post suggest that the enforcement mechanisms will be laid down by the "sysops", with users contracting freely to move easily among online "spaces" (whether they be Internet providers, particular sites, or entire areas of the Internet) — thereby "voting" for the rules and environments that they prefer.[66] Sysops would hold the ultimate power: banishment.[67] Johnson further suggests that the domain name registration authorities should coordinate to condition domain name use (and thus access to Cyberspace) by sysops on certain basic prohibitions of fraud and "force".[68] He suggests that such self-regulation should also include commitment to arbitration as a means of

---

[66] *See also* Bob Dunne; *but cf.* reply by Mark Lemley . Those who advocate governance by a network of free contract seem to have been influenced by the works of Friedrich Hayek; see *supra* note 56.

[67] Johnson & Post, *And How Shall the Net Be Governed*, *supra* note 56.

[68] David R. Johnson, *The Price of Netizenship*, (unpublished manuscript, on file with authors). "Force" in this context would be, for example, launching computer viruses against one's competitors.

enforcement of these top-level rules.[69]

How can we determine whether such a contractual ordering is possible or desirable? The general rules imposed by such registries in the first instance and the more detailed rules imposed by sysops in the second instance are at best contracts of adhesion. The optimistic view is that the adhesive character is of no moment because exit is too easy; thousands of flowers will bloom (and only those that users choose to pollinate will continue to exist). But the pessimistic view is that sysops will find a way to coordinate tacitly to standardize on onerous "take-it-or-leave-it" terms, under the threat of exclusion.

Perhaps the analogy of "residential private government" will be instructive in this regard. Systems of private covenants, in subdivisions or condominiums, have been praised as a method of choice-based community creation. But they have also been criticized because they are imposed on would-be residents on a take-it-or-leave-it basis; because they have tended to standardize on an exclusionary set of rules that reinforce patterns of social power detrimental to poor and minority persons (and anyone heterodox in lifestyle); and because their "private" character means there is little or no constitutional check on the power of developers to set

[69] *Id.*

their own rules as the market (i.e. the tastes of those with money) dictates. It is true that Internet users can more easily exit the rules created by one sysop than condominium or subdivision dwellers can exit the rules created by the developer. The possibility of exit won't be of much use, however, if all of the desirable sites have similar rules.

Right now, it's not clear that "decentralized" contractual law-making on the Internet for enforcement purposes would result in the desired ends of diversity and choice. Under the current economic model of the Internet, Internet service providers (ISPs), the home of most sysops, are for-profit commercial entities. One can guess, therefore, that fiscal concerns will be a factor in the establishment of policies. In fact, various forms of profit-maximizing myopia might be expected. One possibility suggested by the residential private government analogy is oppressive over-regulation. Sysops will prefer those who pay the most and cause the least "hassle", excluding others; and it will be difficult to impose standards of due process or equal treatment because this is a "private" ordering. In this scenario, the remedy of exclusion (banishment) will not be reserved for force and fraud, but rather will serve to consolidate power and profit. Another, opposite, possibility is destructive under-regulation— a "race to the bottom" among sysops, registration authorities, or other sub-units of

Internet authority, resulting in a "lowest-common denominator" enforcement scheme.[70] An analogy is the incorporation competition among states, with the attendant gradual decrease in corporate law liability standards in past decades.[71] If users can arbitrage their choice of ISP, for example, then ISPs can in turn switch their registration authority or TLD. The easy "exit" option of the citizen of Cyberspace may result in weaker or nonexistent enforcement, and the speed at which inhabitants of Cyberspace can "cross borders" may accelerate any trends.[72] A race to the bottom might cause Internet self-regulation to be too minimal (with respect to fraud, for example) to keep territorial sovereigns from imposing

---

[70] The "regulatory arbitrage" described by Johnson and Post as making top-down ordering impractical might also have unpleasant effects when it comes to self-regulation. Johnson & Post, *And How Shall the Net Be Governed*, *supra* note 56.

[71] *See*, William L. Cary, *Federalism and Corporate Law: Reflections on Delaware*, 83 YALE L. J. 663 (1974) (stating the "traditional" view that the competition for state benefits resulting from incorporation gives states incentives to choose "loose" legal rules — those which allow managers to exploit investors). *But see*, Easterbrook and Fischel, THE ECONOMIC STRUCTURE OF CORPORATE LAW 213-218 (1991) (noting that empirical studies "fatally undermine" Cary's view that shareholders are victimized by incorporation in Delaware).

[72] This argument, of course, assumes that a large proportion of net users have a similar orientation with respect to a significant issue. There is a valid counter that diversity reigns on the Internet in similar (if not greater) proportion than in physical space. Some issues, however, may result in substantial uniformity — the imposition of "net-taxes", for example, can be expected to be widely unpopular, thus generating regulatory arbitrage.

their own rules, in which case self-regulation will fail.

Enforcement mechanisms are more difficult than rule-making. Even if tacit coordination has held almost everyone to standardization on ".com", for example, why didn't the same process arrive at a customary procedure for resolving tussles over domain names, without the necessity for NSI (or someone) to promulgate mandatory dispute policies? Perhaps, as Johnson suggests, the registration authorities can now coordinate on a set of minimal conditions for entry into Cyberspace, and for continued existence there, and perhaps they can impose an "agreement" to arbitrate in the case of disputes. It seems, however, that unilateral banishment of those who won't agree to arbitrate or who fail to accept the terms of the arbitration body, is the only ultimate remedy that can be achieved by self-ordering.

Those who are banished will no doubt resort to the courts in their own countries or in the country in which the registration authority is "located". So one suspects that enforcement mechanisms will evolve on the Internet into a hybrid of internal self-regulation and external sovereignty — unless (or until) the Internet becomes a sovereign jurisdiction of its own, with its own constitution, courts, and police force. A first step in this direction is for physical space courts to recognize the Internet's own

jurisdictional space. That is, courts could develop a kind of comity between the Internet and the territorialized non-virtual world, abstaining from Internet disputes in favor of the Internet's own processes, at least until someone is appealing banishment. Of course, if Cyberspace really acquired its own sovereignty, perhaps other sovereignties would not question its authority to de-nationalize (banish) its citizens. But perhaps it's more likely that such an eventuality would cause the world's sovereigns not to recognize any sovereign's general right to de-nationalize its citizens, at least where denationationalization would deny the ability to engage in meaningful commerce.

It seems far-fetched to be talking about whether Cyberspace could become a sovereign jurisdiction of its own. People don't physically live there; its government would not organize economic and social life in a physical space. The premises of sovereignty in physical space have been territorial; the Internet is unterritorial. Yet is seems that intermediate regimes might be unstable. Even a regime of comity between the Internet's own dispute-resolution processes and enforcement mechanisms and those of the territorialized non-virtual world will serve to attenuate the territoriality (and territorial diversity) of sovereignty. In order for a regime of internal arbitration to work, every territorial sovereign to whom

a disappointed “resident” of Cyberspace might appeal must cede a considerable part of its precious jurisdiction, because every territorial sovereign to whom a disappointed resident of Cyberspace might appeal must agree that all those contracts of adhesion are valid and enforceable. Perhaps the external courts might stop short in certain cases of banishment. Yet if banishment is the only Cyberspace enforcement mechanism with “teeth”, external courts must accept it in most cases if Internet self-regulation is to be stable; and the guidelines for when it would not be acceptable would have to be consistent among all external sovereigns. That requires a lot more global agreement about due process than we now have. Yet it seems the likely alternative — a welter of conflicting local regulations — will either be ineffective or kill the promising commercial goose. Internet proponents” best hope is an evolution toward a regime in which there is enough agreement about the minimal standards of background due process so that all players will understand and accept them, allowing stable self-enforcement on the Internet.