Chicago-Kent Law Review

Volume 73
Issue 4 *Symposium on the Internet and Legal Theory*

Article 13

October 1998

The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace

Margaret Jane Radin

R. Polk Wagner

THE MYTH OF PRIVATE ORDERING: REDISCOVERING LEGAL REALISM IN CYBERSPACE

MARGARET JANE RADIN & R. POLK WAGNER*

INTRODUCTION

The legal realists of the 1920s and '30s demonstrated that all law is "public"—that is, dependent upon the state. Contrary to laissez-faire ideology, the "private" legal regimes of property and contract presuppose a "public" regime of enforcement and policing, a baseline of background rights. Private land ownership rights are limited by nuisance law; private contract rights are limited by doctrines of duress, fraud, unconscionability, and public policy.[1] The realist demonstration was repeated by the critical legal theorists of the 1970s and '80s. Sometimes the "crits" used postmodernist methodology—"private" and "public" can be "flipped"—but the insight was the same.[2] Why did the realist demonstration need to be repeated by the crits two generations later? Perhaps because of the persistent mythological force of laissez-faire ideology in our culture.

That mythological force is still with us. In fact, it seems to be waxing. So the demonstration now needs to be repeated in cyberspace. The essays for this symposium by Professors William (Terry)

* Margaret Jane Radin is the William Benjamin Scott & Luna M. Scott Professor of Law at the Stanford Law School and a Co-Director of the Stanford Program in Law, Science and Technology. R. Polk Wagner is a graduate of the Stanford Law School and the University of Michigan. Thanks to Dan L. Burk, William W. Fisher III, Jane C. Ginsburg, Ira V. Heffan, David R. Johnson, Mark A. Lemley, and David G. Post for helpful comments on earlier drafts.

1. *See generally* BARBARA H. FRIED, THE PROGRESSIVE ASSAULT ON LAISSEZ FAIRE: ROBERT HALE AND THE FIRST LAW AND ECONOMICS MOVEMENT (1998).

2. *See* MARK KELMAN, A GUIDE TO CRITICAL LEGAL STUDIES 242-68 (1987); Clare Dalton, *An Essay in the Deconstruction of Contract Doctrine*, 94 YALE L.J. 997, 1010-13 (1985); Duncan Kennedy, *Stages of the Decline of the Public/Private Distinction*, 130 U. PA. L. REV. 1349, 1349-50 (1982); Gary Peller, *The Metaphysics of American Law*, 73 CAL. L. REV. 1151, 1219-59 (1985).

The crits' focus on "flippability" underscored a point that theorists since Hobbes have regularly recognized: the ultimate sovereign authority that lays down rules *itself* rests upon the cooperation of those that accept the rules, so even top-down sovereignty can be "flipped" to show it rests on bottom-up cooperation. The struggle to understand how to think about sovereignty in the global networked environment, we argue in this comment, needs to move beyond such oversimplified opposition, whether propounded by the left or the right.

Fisher and Niva Elkin-Koren set about this task.[3] One more time, there can be no free-standing purely "private" regime of property and contract. One more time, property and contract presuppose limits and enforcement shaped by a sovereign authority.

I. THE AMBIGUOUS IDEAL OF PRIVATE ORDERING

A. Law and Anarchy

The ideal of "private ordering" in cyberspace excites many people. Because the commercial environment is now global, but legal sovereignties are still territorial, it is unclear how (or if) cyberspace will be structured and governed. In these circumstances, because of the continued force of laissez-faire ideology, some people hope to finesse the question of territorial jurisdiction—sovereignty—with global "private ordering." If private ordering means legally enforceable contract, this hope is chimerical. The hope flourishes because the legal realist insight has been suppressed. But once the legal realist insight is revived, we can see there is an urgent question of how the institutions of contract and property in cyberspace will be shaped and patrolled. There is an urgent question of sovereignty: who will do the shaping and patrolling?

There is another way to finesse the question of sovereignty. In a regime of anarchy—as opposed to a regime of "private" law backed by state enforcement and policing—the issue of sovereignty disappears. Insofar as the advocates of private ordering are thinking of regimes of customary norms with no enforcement and policing mechanisms other than people's continuing commitment to them, they are thinking of *anarchy*, not law. In an anarchic regime, there is no guarantee of due process when the group excludes someone, no recourse for fraud, duress, or violence outside the group's own dispute-resolution mechanisms or protection society.[4] Many of those who are excited about private ordering in cyberspace are thinking of regimes held together entirely by customary norms, which evolve on their own

3. *See* Niva Elkin-Koren, *Copyrights in Cyberspace—Rights Without Laws?*, 73 CHI.-KENT L. Rev. 1155 (1998); William W. Fisher III, *Property and Contract on the Internet*, 73 CHI.-KENT L. REV. 1203 (1998); *see also* JAMES BOYLE, SHAMANS, SOFTWARE, AND SPLEENS: LAW AND THE CONSTRUCTION OF THE INFORMATION SOCIETY 144 (1996); Julie E. Cohen, Lochner *in Cyberspace: The New Economic Orthodoxy of "Rights Management"*, 97 MICH. L. REV. 462, 480-515 (1998).

4. *See* ROBERT NOZICK, ANARCHY, STATE, AND UTOPIA 200-24 (1974) (arguing that private protection societies organized by participants under anarchy will give way to a monopolistic protection society which will become the state).

in the "self-organizing" networked environment.[5]

B. Top-Down and Bottom-Up: The Motto of the Anarcho-Cyberlibertarians

In "real" space, some areas of social life are governed by law and some by non-legal systems of norms. It seems obvious to suggest that cyberspace will turn out to be the same. Some advocates of private ordering, however, argue that cyberspace must either be governed entirely by state-backed law or entirely by non-legal (anarchic) norms, then vote for the latter.[6] This false dichotomy stems from a resurgence of Friedrich Hayek's stylized distinction between bottom-up and top-down ordering. In Hayek's scheme, top-down ordering, the positivistic, laid-down law of the state, "central planning," is bad; bottom-up ordering, the laissez-faire network of promises among individuals, the growing-up of customary norms, "private ordering," is good.

Cyberlibertarians identify Hayek's top-down central planning with state-backed law and his bottom-up private ordering with regimes of non-legal customary norms. Thus, they should probably be called cyberanarchists rather than cyberlibertarians; a libertarian scheme requires strong state-backed law of property and contract. (Actually they should be called "anarcho-cyberlibertarians" because they are trying to be libertarians and anarchists at the same time. It must be the power of laissez-faire ideology that causes them not to see that one involves no property and one involves strong property). Insofar as anarcho-cyberlibertarians are thinking of bottom-up private ordering as a legal contractual regime, though, they (and Hayek himself) remain subject to the realist critique. Those needed limitations—principles such as duress, fraud, and due process—have to come from somewhere and be enforced somehow. By now we know (or should know) that they do not come from self-enforcing natural law.

The bottom-up "versus" top-down distinction tends to be obfus-

5. *See, e.g.*, David R. Johnson & David G. Post, *And How Shall the Net Be Governed?: A Meditation on the Relative Virtues of Decentralized, Emergent Law*, *in* COORDINATING THE INTERNET 81-90 (Brian Kahin & James H. Keller eds., 1997) (noting the many references to the customary commercial norms of the "law merchant"); Trotter Hardy, *The Proper Legal Regime for 'Cyberspace'*, 55 U. PITT. L. REV. 993, 1051-53 (1994).

6. *See, e.g.*, David G. Post & David R. Johnson, *"Chaos Prevailing on Every Continent": Towards A New Theory of Decentralized Decision-Making in Complex Systems*, 73 CHI.-KENT L. REV. 1055, 1086-88 (1998).

catory in cyberspace, as it is elsewhere. A regime can be characterized as either, depending upon how you look at it. Legislation itself is bottom-up when considered as a good purchased by competing interest groups. To some, nuisance law is unwanted top-down regulation; to others it is a needed inherent limitation on property titles arrived at by bottom-up coordination among neighbors. Top-down legislative regimes are no less the result of social evolutionary processes than are bottom-up regimes of norms. Most regimes are mixed anyway: there are myriad ways for governmental and non-governmental organizations and individuals and groups to be intertwined with each other in social ordering.[7] Sometimes a law laid down seems best (someone has to declare that the speed limit shall be 55); sometimes a customary norm seems best (a validation of a usage of trade); many times a mixture is best.

We ought to be talking about the details of good mixtures, rather than debating top-down "versus" bottom-up. It may make no sense for the Internet to be governed by existing nation-states (or the powerful among them), and it is true that the Internet (at least in its earlier non-commercial stage) has (or had) the potential for ordering a great deal through custom rather than law. That raises interesting questions about the role of custom in the commercialized Internet. It does not mean that a Hayekian free-for-all is the only alternative, or even a viable alternative, to attempted government in detail by nation-states.

II. THE PROBLEM OF SOVEREIGNTY IN CYBERSPACE

A. An Example: Internet Domain Names and Legal Trademark Rights

In exploring the practical and theoretical issues of structuring Internet institutions, it is useful to consider the problem of domain names.[8] Domain names are addresses. In fact, domain names are

7. *See, e.g.*, Henry H. Perritt, Jr., *The Internet is Changing International Law*, 73 CHI-KENT L. REV. 997, 1029-31 (1998).

8. Internet domain names take the form "[host].[domain].[top-level-domain]." For example, "www.stanford.edu," where "www" is known as the hostname, "stanford" is the domain name, and "edu" is the top-level-domain name, or "TLD." Because each Internet domain name corresponds uniquely to what is known as an "IP address," a series of numbers that is the means by which transmissions are routed through the Internet, the domain names themselves are normally used as addresses.

There are a limited number of TLDs, ".com" being the best-known; corporations and individuals wishing to establish an Internet presence "register" their own domain names within par-

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.

The "story" of domain names can be described in evolutionary terms. When the Domain Name System ("DNS") was instituted in the early-to-mid 1980s, the Internet was a non-commercial research and communication tool, originally supported by the Defense Advanced Research Projects Agency 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.[9] As in all commons, the "first-come, first-serve" concept governed use rights—in fact, this continues today, with "first-come, first-serve" being the registration policy for second-level domain names.[10] The designers of the DNS were creating a method of

ticular TLDs. Stanford University, for example, has registered "stanford" within the ".edu" TLD space. Various TLDs are reserved for certain types of organizations: the ".edu" namespace is reserved for institutions of higher education; ".gov" is meant for U.S. government bodies; and ".org" is typically for non-profit groups. The catch-all commercial TLD, ".com," has become extremely popular as commercial entities have discovered the Internet. The hostnames are designated by the domain holder—Stanford may choose the hostnames (such as "www") within the "stanford.edu" namespace.

9. *See* Jon Postel, *The Domain Naming Convention for Internet User Applications* (visited Feb. 28, 1999) <http://www.roxen.com/rfc/rfc819.html>; *see also* P. Mockapetris, *Domain Names—Concepts and Facilities* (visited Feb. 28, 1999) <http://194.52.182.96/rfc/rfc1034.html>.

10. As of early December 1998, the future of domain name registration was unclear. Spurred by widespread dissatisfaction with the lack of competition among TLDs— ".com," for example, has emerged as the most desired component for an Internet address—and questions about the legitimacy of the registration authority, the United States government established a policy that was intended to encourage transparency in domain name governance and introduce competition between corporations offering registration services. *See* Management of Internet Names and Addresses, 63 Fed. Reg. 31,741 (1998) [hereinafter White Paper]. Months of negotiation resulted in the November 25, 1998 transfer of formal registration authority to a new non-profit oversight corporation, the Internet Corporation for Assigned Names and Numbers ("ICANN"). *See Memorandum of Understanding Between the United States Department of Commerce and Internet Corporation for Assigned Names and Numbers (ICANN)* (visited Feb. 28, 1999) <http://www.ntia.doc.gov/ntiahome/domainname/icann-memorandum.htm>. ICANN intends to establish polices and guidelines for the registration of domain names, dispute procedures, and standards for prospective registrants of additional TLDs, while ensuring order and stability as competition for domain names is gradually introduced. *See, e.g., Internet Corporation for Assigned Names and Numbers* (visited Feb. 28, 1999) <http://www.icann.org/>; Courtney Macavinta, *U.S. to Hand over Net Administration* (visited Feb. 28, 1999) <http://www.news.com/News/Item/0,4,29263,00.html>.

Network Solutions International ("NSI"), the corporation originally charged—under a contract with the National Science Foundation—with handling the registration of individual domain names for the popular "generic" TLDs, such as ".com," ".edu," and ".org" remains

administering the name-space commons for the convenience of all, not a method of selling names as private property.[11] It was not 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.

Demand for domain names until the mid-1990s was comparatively low: Network Solutions International ("NSI"), the corporation presently charged with registering the majority of domain names, reports that in October 1995, there were 156,961 total domain names registered.[12] There was (and is) little possibility of actually "stealing" a domain name: the technological barriers of the DNS system precluded out-and-out theft.[13] These technological and social circumstances meant that enforceable property rights were not worth the price of implementing them.

Then a few years passed, and the world changed. The Internet came to be understood as a commercial infrastructure of very great potential power. Individual domain 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 of them that Internet entrepreneurs came to deem desirable.[14] They started to look very valuable because there is monetiz-

heavily involved. The Commerce Department recently signed an agreement with NSI allowing it to continue to be the sole registrar of the majority of domain names through at least the year 2000, though some competition among registrars may be introduced as early as summer 1999. *See* Courtney Macavinta, *Deal Extends NSI Domain Control* (visited Feb. 28, 1999) <http://www.news.com/News/Item/0,4,27202,00.html>; Network Solutions International (visited Feb. 28, 1999) <http://www.networksolutions.com/>.

11. "Concerns about 'rights' and 'ownership' of domains are inappropriate." Jon Postel, *New Registries and the Delegation of International Top Level Domains* (visited Feb. 28, 1999) <ftp://ftp.ripe.net/rfc/rfc1591.txt>.

12. By early 1998, that figure had risen to 2,057,489. Domain name statistics through 1996 can be found at *What's in a Name?* (visited Feb. 28, 1999) <http://rs.internic.net/nic-support/nicnews/>. More recent statistics can be found at Network Wizards (visited Feb. 28, 1999) <http://www.nw.com/>. The 1998 domain name registration information is provided by Internet.Org. *See Internet Statistics* (visited Feb. 28, 1999) <http://www.internet.org/cgi-bin/genobject/BROWSE/stats/>.

13. In July 1997, however, Eugene Kashpureff, the founder of AlterNIC, an organization promoting competition among TLDs, reportedly managed to route most of the users trying to reach the NSI website (www.netsol.com) to the AlterNIC site. By "redirecting" traffic intended for NSI, Kashpureff in effect "hijacked" the "netsol.com" domain name. *See* Rajiv Chandrasekaran, *Network Solutions Gets Court Order To Halt Redirection of Web Site Users*, WASH. POST, July 24, 1997, at E3.

14. Though some argue that sheer numbers is the root of the scarcity, this seems overly su-

able value in commercial names in a way that there is not in non-commercial names.[15] Demand mushroomed, as did registration.[16] As simple economics would predict, a trade in names grew up; and the expenses of exclusion became worthwhile. Conflicts developed over domain names.[17] Businesses and individuals began advertising domain names for sale; it was rumored that domain names changed hands for sums on the order of $3 million.[18]

In these circumstances, a clear property rights regime, with clear enforcement mechanisms, seemed to be needed to avoid the costly free-for-alls economists predict when non-commercial commons resources suddenly become commercially very valuable. Cyberspace has developed its own form of questionable speculation in the absence of clear property rights called "cybersquatting" or "domain name grabbing." Domain name grabbing refers to the practice of registering a domain name that the registrant 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 effec-

perficial—because second-level domain names can be at least 24 characters long, 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.

15. 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. *See* Postel, *supra* note 11.

16. *See What's in a Name?*, *supra* note 12.

17. A *Wired* and *Newsday* reporter, Joshua 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. *See* Joshua Quittner, *Billions Registered* (visited Feb. 28, 1999) <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. *See* Victoria Slind-Flor, *'Domains' Are There for Taking*, NAT. L.J., June 5, 1995, at A7.

18. In 1998, Compaq paid a reported $3 million to secure "altavista.com," the name and address of its popular search engine. *See* Paul Farhi, *A Web 'Squatter' Beats Exxon Mobil to Its Site*, WASH. POST, Dec. 3, 1998, at E1; *see also* "BestDomains" website, styled as "[t]he largest Global Internet Name & Asset Trading Site," (visited Feb. 28, 1999) <http://www.bestdomains.com/domains/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 whatever someone is willing to pay, or sell it for." *Id.*

tively block the corporation from the domain name, then offers to sell the domain name to the corporation.[19]

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 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, NSI will deliver allocation authority to the court.[20] 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.[21]

There has been a great deal of debate about the merits or demerits of the Dispute Policy. At least it is evident from an evolutionary point of view that some such policy would be expected to come into existence when it did. It is also important to bear in mind that

19. A recent case is Panavision Int'l v. Toeppen, 141 F.3d 1316 (9th Cir. 1998). Toeppen registered the domain name "Panavision.com" and demanded $13,000 to relinquish it to Panavision. *See id.* at 1319. (The court noted that "Toeppen's 'business' is to register trademarks as domain names and then sell them to the rightful trademark owners." *Id.* at 1325). Toeppen reportedly registered 240 domain names, most relating to well-known trademarks. *See id.* at 1319. Panavision sued Toeppen in federal court, claiming trademark infringement, state and federal trademark dilution, and federal and state unfair competition, among others. *See id.* at 1318. Panavision prevailed on the dilution claims on summary judgment; Toeppen was enjoined from using the "Panavision.com" name and was required to transfer it to Panavision. *See id.* at 1327.

20. *See Network Solutions' Domain Name Dispute Policy* (visited Feb. 28, 1999) <http://rs0.internic.net/domain-info/internic-domain-6.html>.

21. In *Panavision*, the district court noted: "the policy has not proven effective in resolving domain name conflicts." Panavision Int'l v. Toeppen, 945 F. Supp. 1296, 1302 (C.D. Cal. 1996).

In operation the Dispute Policy allows trademark owners quickly, easily, and cheaply to assert a claim against a domain holder. By complaining to NSI, the trademark owner can get an offending domain name put on hold, with minimal legal costs.

There are several thorough analyses of the Dispute Policy available on the Internet. *See, e.g.*, Dave Graves, *Domain Name Issues & Policies* (visited Feb. 28, 1999) <http://rs0.internic.net/presentations/daveg/ispcon/sld001.html> (presenting the NSI view); Carl Oppedahl, *Analysis and Suggestions Regarding NSI Domain Name Trademark Dispute Policy* (visited Feb. 28, 1999) <http://www.patents.com/nsi/iip.sht> (criticizing the NSI approach).

evolution does not stop. This point is logically anterior to arguing the pros and cons of the NSI 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 seems likely to happen is that domain names are going to become relatively less valuable. The demand for them could ease: more TLDs could be formed;[22] and/or competitors to NSI could become viable.[23] Or the importance of domain names could subside: sophisticated search engines, "smart browsers," agent applications, or other technological innovations may perhaps render them largely irrelevant.[24]

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 do-

22. The Clinton Administration's initiatives towards reform of the domain names system assume increased numbers of TLDs. *See, e.g.*, White Paper, *supra* note 10, at 31,746.

23. The late Jon Postel, one of the founders of the Internet, suggested that the DNS be reformed to allow at least two-dozen new U.S. TLDs and "introduce competition in the top-level domain registration business so that market forces will ensure fair prices for good services." Postel, *supra* note 11. This suggestion has largely been accepted by the current White Paper. *See* White Paper, *supra* note 10, at 31,742.

24. 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) returns a list of pages containing the text, and "indexing" where websites 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. For an example of full-text searching, see Alta Vista (visited Feb. 28, 1999) <http://www.altavista.com> and for an excellent example of a Web index, see Yahoo (visited Feb. 28, 1999) <http://www.yahoo.com>.

Smart browsers would integrate the searching functions into the user's software. Instead of interfacing with a search engine through a website, 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. This feature has been included in Netscape Navigator Version 4.5. *See Netscape Navigator* (visited Feb. 28, 1999) <http://www.netscape.com>.

Agent applications, or "intelligent agents," are software applications that can perform complex tasks independently upon direction from a user. An example is the Anderson Consulting "BargainFinder" agent. BargainFinder "comparison shops among Internet stores to find the best price for a compact disc." *See BargainFinder* (visited Feb. 28, 1999) <http://bf.cstar.ac.com/bf/>; *see also* Dan L. Burk, *Virtual Exit in the Global Information Economy*, 73 CHI-KENT L. REV. 943 (1998).

main names are appropriated out of domain name space.[25] 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.

Trademarks in the United States 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 owners located in different territories could use the same mark. Moreover, trademarks in the United States 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 owners engaged in different lines of business could use the same mark. But 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 cannot share the same name.[26] Domain names are unterritorialized and non-compartmentalized. If Apple Computer is the first to claim "apple.com," then Apple Records must yield.

Additionally, trademark law expressly reserves a large portion of the commons of language—it does not allow the registration of "merely descriptive" terms.[27] "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.[28] 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.

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

25. 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.

26. Unless they are willing to use different TLDs. See White Paper, *supra* note 10, at 31,746, regarding proposals to expand the number of TLDs.

27. *See* 15 U.S.C. § 1052(e)(1) (1994).

28. C|Net, Inc., for example, reportedly paid less than $50,000 for "news.com," yet clearly it is of great value for drawing consumers seeking news. *See* Mike Allen, *Seeing Ad Dollars, C-Net Multiplies Web Sites*, N.Y. TIMES, Sept. 16, 1996, at D4.

and make it possible to have comprehensive rights over a name for all products.[29] Because the concept of dilution tends towards unterritorialization, it is no accident that many domain name cases in this country so far have relied on the new federal anti-dilution statute, the Federal Trademark Dilution Act of 1995 ("Act").[30] This statute does decompartmentalize, but only for "famous" trademarks.[31] The Act, thus, creates a hierarchy: "famous" marks can exclude all others from 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.[32]

If trademark law were to go all the way toward unterritorialization 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 sys-

29. Modern trademark law is moving away from its roots in a common-law tort-like regime based on notions of unfair competition towards a naked—or free-standing—property rights regime. The Ninth Circuit in Panavision International v. Toeppen noted that for a defendant to be liable under the Federal Trademark Dilution Act of 1995, 15 U.S.C. § 1125(c), "[i]t does not matter that he did not attach the marks to a product." 141 F.3d 1316, 1325 (1998). As courts have recognized, whereas traditional trademark law sought to primarily protect consumers, dilution laws place more emphasis on protecting the investment of the trademark owners. *See, e.g.*, Boston Prof'l Hockey Ass'n v. Dallas Cap & Emblem Mfg., Inc., 510 F.2d 1004, 1011 (5th Cir. 1975) (finding infringement in selling unattached trademarked logos, while noting that the decision "may slightly tilt the trademark laws from the purpose of protecting the public to the protection of the business interests of plaintiffs."). *But cf.* Illinois High Sch. Ass'n v. GTE Vantage, Inc., 99 F.3d 244, 247 (7th Cir. 1996) (arguing that "antidilution statutes . . . do not elevate a trademark all the way to property").

30. *See* 15 U.S.C. § 1125(c) (Supp. II 1994); *see also Panavision*, 141 F.3d at 1316; Avery Dennison Corp. v. Sumpton, 999 F. Supp. 1337, 1339 (C.D. Cal. 1998); Intermatic, Inc. v. Toeppen, 947 F. Supp. 1227, 1236 (N.D. Ill. 1996).

31. 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." 141 CONG. REC. S19,312 (daily ed. Dec. 29, 1995) (statement of Sen. Leahy).

The criteria established for determination of a "famous" mark are: (a) the degree of inherent or acquired distinctiveness of the mark (i.e., its strength); (b) the duration and extent of use of the mark; (c) the duration and extent of advertising/publicity of the mark; (d) the geographical area in which the mark is used; (e) channels of trade for the goods or services with which the mark is used; (f) the fame of the mark in the trading areas; (g) the nature and extent of use of similar marks by third parties; and (h) whether the mark is federally registered. *See* 15 U.S.C. § 1125(c)(1).

32. Traditional (non-dilution) infringement analysis requires a showing of "likelihood of confusion." *See, e.g.*, Interstellar Starship Servs., Ltd. v. Epix, Inc., 983 F. Supp. 1331, 1334 (D. Or. 1997). In contrast, the dilution standard requires only a claim that the value of the mark is lessened. *See* 15 U.S.C. § 1127 (definition of dilution); *see also Panavision*, 141 F.3d at 1316; *Intermatic*, 947 F. Supp. at 1227 (finding dilution, but not finding traditional infringement).

tem to enforce them. That, of course, brings us back to the question of sovereignty.

B. Turning to the Ideal of Self-Ordering

The domain name issue draws attention to 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 it, what is a permissible use, who will sanction transgressions, etc. immediately arise. These issues permeate the nascent 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 it become obsolete? (Next year, or forty 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 sovereign nor subject to rules centrally laid down, unless one nation becomes powerful enough to assert sole control, or unless we develop world government. It seems safe to say that we are not going to have world government with a supreme legislative 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.[33]

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, including rules about access to domain names.[34] But this authority would only be authoritative if its decrees were accepted by every national sovereign, and that might require a full-scale network of treaties or at least unanimity of official acquiescence. We could also imagine a piecemeal process of treaty-making, issue-by-issue—a Domain Names Property Rights Enforcement Treaty, and similar accords for other kinds of intellectual prop-

33. Witness the European Union: decades after the common market was instituted, there has been substantial development of overarching community law but the process is far from complete. *See, e.g.*, Oscar Schachter, *The Decline of the Nation-State and its Implication for International Law*, 36 COLUM. J. TRANSNAT'L L. 7, 11 (1997).

34. *See supra* notes 9-12 and accompanying text.

erty rights on the Internet. Some international accords dealing with intellectual property rights 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.

These difficulties give impetus to the idea of considering the Internet as its own *sui generis* jurisdiction, with its own self-governance and enforcement mechanisms. Many who are interested in the Internet, including quite a few anarcho-cyberlibertarians, are thinking about spontaneous ordering (self-organization) rather than rules laid down.[35] They are thinking about laws, customs, and technological standards which are not laid down but instead grow up.[36] One important, indeed urgent, question for study is whether open technological standards can grow up as the result of market interactions, that is, without a governmental regulatory structure other than a general state-backed background regime of property and contract.[37] For anarcho-cyberlibertarians, there is a more basic question: whether a state-independent background regime of property and contract can grow up as customary "law." That is, under what social, economic, and technological circumstances might customary regimes of property and contract grow up on the Internet? On the other hand, under what social, economic, and technological circumstances will the Internet need a sovereign to legislate or adjudicate for it, at least in some respects?

In this regard, it is interesting to ask why almost everyone in the world seems to have largely accepted NSI's authority to dole out do-

35. *See* Hardy, *supra* note 5, at 1025-28; Johnson & Post, *supra* note 5, at 81-84; Post & Johnson, *supra* note 6 (advocating self-ordering and coordination over sovereign-introduced legal rules).

As we mentioned, these dichotomous categories (spontaneous ordering versus centralized planning) seem to be derived from the work of Friedrich Hayek. While the categories tend to oversimplify the understanding of real-world institutions, we do not claim that these categories are useless as a first cut at describing features of desirable approaches to law in Cyberspace, as long as the realist insight that baselines are needed for a legal (as opposed to anarchic) regime is kept in mind. Nevertheless, we want to suggest that the second (and subsequent) cuts should be more fine-grained.

36. *See* Hardy, *supra* note 5, at 1019-22. Hardy, among others, notes the rise of the Law Merchant in the medieval trade context—a growth of customs and practices consisting of certain principles of equity and usage of trade which benefited the merchants as a whole. *See id.*

37. Of course, such a general background regime becomes contentious whenever one zeroes in on it. For example, what is the extent of property rights in information, with respect to (say) a database consisting of a merchant's catalogue? The fact that the background regime becomes contentious so often when it must come into play in order to enforce a contested interaction is the reason why the libertarian "minimal state" cannot be put uncontroversially into practice in order to create a background scheme of certain and strong property rights.

main names until quite recently.[38] No world government or treaty granted it this power, nor confirmed in it the sovereign ownership of the name space.[39] Indeed, in the early days of this country there was more question about the authority of the United States 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."[40] It would be unimaginable to suppose that our government could validly grant land somewhere else in the world. Yet, it appears that a private body, NSI, located in the U.S. and operating under U.S. auspices, has been able to dole out "virtual land" in Cyberspace (in the form of domain name space).

It could be the case that the .com and the other unterritorialized top level domains have been held together by tacit coordination which all understand to be profitable.[41] Alternatively, it could be the case that the wide acceptance of NSI's authority was an artifact of the earlier non-commercial Internet, and that it will now unravel under market pressures. Achievement of stability in a self-regulated commons is often thought to be dependent upon whether the cooperators are a close-knit social group. Earlier users of the Internet may have belonged to a close-knit social group but this is not true of Internet users today.[42]

Under the tacit coordination hypothesis, the system administrators choose to point their nameservers at the "official" 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. According to this hypothesis, the unplanned yet systematic coordination among the widely varied parties using the Internet has firmly established the international

38. *See* Chandrasekaran, *supra* note 13. To be sure, there have been dissenters, such as AlterNIC, but their impact has been limited.

39. United States government funds certainly contributed to the initial research and development of the Internet, and government funds support the initial registration efforts—the cooperative agreement which established NSI's registration authority stipulated a grant of $42 million over fifty-seven months. *See NSF Cooperative Agreement No. NCR-9218742* (visited Feb. 28, 1999) <http://rs0.internic.net/nsf/agreement/agreement.html>.

40. Johnson v M'Intosh, 21 U.S. (8 Wheat.) 543, 588 (1823).

41. Yet, the realization by commercial actors of the magnitude of NSI's authority, as well as displeasure with its practices, has led to calls for additional TLDs, competition among registration authorities, and calls for legislation to regulate domain names and trademarks. Recent developments in the control and distribution of domain names feature such market-oriented reforms. *See, e.g.*, Jeri Clausing, *Control of Domain Names Draws Alternative Proposal: Planning the Internet's Final Privatization*, N.Y. TIMES, Oct. 5, 1998, at C3.

42. *See* discussion at text accompanying *infra* notes 44-45.

TLDs (especially the ".com" TLD) and NSI as *de facto* the sole authoritative body regarding domain names.

Similarly, a process of tacit coordination 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 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.[43]

If tacit coordination is the right way to think about what gave NSI its authority, then we need to consider what types of issues are amenable to tacit coordination. That is, what kinds of problems involving necessary cooperation—mutual exclusion and forbearance, uniform standardization—can be solved through sovereignless self-organizing coordination? And, perhaps more importantly, what kind of problems cannot?

III. THE LIMITS OF SELF-ORDERING

A. Conditions of Coordination

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 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.[44]

The old noncommercial Internet was such a group, but the new

43. Johnson & Post, *supra* note 5, at 74.

44. *See, e.g.*, ROBERT C. ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES 156-66 (1991).

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.[45] 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 order on the Internet in general—a case in which external 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?

B. Self-Ordering Through Contract?

Many Internet observers are adopting the view that networks of contracts among participants can substitute for external regulation. For example, Johnson and Post suggest that many of the enforcement mechanisms will be laid down by the on-line system operators, "sysops," with users contracting freely to move easily among on-line "spaces" (whether those "spaces" are Internet providers, particular sites, or entire areas of the Internet)—thereby "voting" for the rules and environments that they prefer.[46] Sysops would hold the ultimate power: banishment. 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."[47] He suggests that such self-regulation should also include commitment to arbitration as a means of enforcement of these top-level rules.[48]

45. *See, e.g.*, THOMAS C. SCHELLING, THE STRATEGY OF CONFLICT 67-74 (1960).

46. *See* Johnson & Post, *supra* note 5, at 75.

47. *See* David R. Johnson, *The Price of Netizenship* (visited Feb. 28, 1999) <http://www.cli.org/pon.html>. "Force" in this context would be, for example, launching computer viruses against one's competitors.

48. *See id.*

Professor William Fisher in this symposium also proposes a regime of contractual self-ordering to govern digital content on the Internet.[49] He suggests that courts and legislators should by and large stand aside as content creators supplant copyright-based entitlements with contract-based entitlements. Fisher sees societal benefit in the flexibility of contract. Contracting out of copyright will enable price discrimination by content creators, resulting in a transfer of wealth from consumers to content producers, and, thus, in a net increase in production of content, whose social value Fisher presumably believes will offset the net loss to consumers.[50] Fisher proposes imposition of a list of mandatory terms and default rules.[51] (By whom they should or could be imposed is not part of his project). He suggests that coordination around this scheme of mandatory terms and default rules will create a stable regime for protecting digital content and thus encourage its production.

C. Contracts of Adhesion

How can we determine whether such a contractual ordering is possible or desirable? Note that the examples above—the agreements with the domain registries, sysops, and the content creators—are at best contracts of adhesion.[52] A conventional approach to adhesion contracts validates them only if the terms are reasonable and/or are foreseeable by the adhering party. In the context of mass-market uniform adhesion contracts, a conventional economic analysis would validate those contracts in which the package of terms won out in a free market, indicating that the terms were preferred by consumers, and would invalidate those that were arrived at by collusion or market power. Under this economic analysis, adhesion contracts cannot be deemed valid without investigating their market context.

One easy observation is that sysops and content creators may

49. *See* Fisher, *supra* note 3, at 1219.

50. *See id.* at 1249-50.

51. *See id.* at 1220, 1241. Unlike some proponents of contractual self-ordering, Fisher is well aware of the realist point that the scope of contract as an institution must be defined and policed by an enforcement authority. One may infer that he supposes that content producers, being profit-maximizers, will willingly trade off the costs to them of the limits imposed by that authority in the form of mandatory and prohibited terms against the gains to be reaped from enforceable property rights including price discrimination.

52. *See* Johnson & Post, *supra* note 5, at 81-84. Even if evolutionary theory supposes such contracts will all exist only by consumer choice in the long run, a theory seemingly adopted by Johnson and Post, for example, there is no reason to suppose *a priori* that we are looking at a long-run equilibrium in any given case.

find a way tacitly to standardize on onerous "take-it-or-leave-it" terms, under threat of exclusion in the sysop case, or denial of access to digital information in the content creation case. The optimistic view is that the adhesive character is of no moment because exit is easy; thousands of flowers will bloom (and only those that users choose to pollinate will continue to exist). But a more pessimistic view is that sysops will find a way to coordinate on onerous take-it-or-leave-it terms, under the threat of exclusion.[53] Such coordination on uniform take-it-or-leave-it terms amounts to imposition of a rigid entitlement structure.

Externalities are another problem with these sorts of contracts. It is possible, for example, as Professor Niva Elkin-Koren and others note, that there are more and broader-ranging externalities with information than with physical goods.[54] Indeed, this commodified mode of thought—looking solely at the economic impact on third parties—does not fully capture what is at stake here, such as the formation of self and its characteristics and preferences in the context of groups. Contracts which concern privacy, for example, touch on a range of issues beyond the economic transaction, including personal identity and freedom. Who will decide to what extent firms may gather and use information about customers? Will it be sufficient to validate these practices that the consumer "clicks" on a box in an on-line form contract?[55]

A third important point about contractual ordering is the distinction between contracts between immediate parties and those that "run with" the object. Contracts that run with the object change the entitlement structure—not just between the immediate parties but for all parties in a chain of distribution. When contracts that "run with" the object are also mass uniform contracts of adhesion, then we *do* have a change in the overall social entitlement structure. In the realm

53. *See* Fisher, *supra* note 3, at 1245-46. Fisher suggests that this problem can be addressed by imposing limits on the terms of the contracts—primarily by refusing to enforce agreements outside the permissible range. *See id.* at 1250. Of course, it is entirely reasonable to suppose that if moving the terms of the agreements towards these limits is a profit-maximizing trend, then the content creators will have strong incentives to standardize upon the limits, resulting in a *de facto* regime of private legislation.

54. *See* Elkin-Koren, *supra* note 3, at 1197-99. For the most thorough and insightful treatment of the issue of externalities in the context of information content, focusing on media, see C. Edwin Baker, *Giving the Audience What It Wants*, 58 OHIO ST. L.J. 311, 372-83 (1997).

55. *See, e.g.*, Mark E. Budnitz, *Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate*, 49 S.C. L. REV. 847, 849-51, 869-74 (1998) (describing the concerns of online privacy advocates and industry responses); *Privacy Online: A Report to Congress* (visited Feb. 28, 1999) <http://www.ftc.gov/reports/privacy3/>.

of information content, we are seeing "running" contracts both that attempt to expand background intellectual property rights (e.g., by forbidding reverse engineering) and to cut them back (e.g., the copyleft General Public License).[56] Given that schemes of "running" adhesion contracts, like adhesion contracts generally, cannot be *ipso facto* valid, how will we determine which of them will be enforceable (whoever is doing the enforcing)?

The analogy of "residential private government," drawn from the context of social ordering through land ownership, is instructive.[57] 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, primarily for three reasons: (1) they are imposed on would-be residents on a take-it-or-leave-it basis; (2) they have tended to standardize on exclusionary sets of rules that reinforce patterns of social power detrimental to poor and minority persons (and anyone heterodox in lifestyle); and (3) their "private" character means there is little or no constitutional check on the power of developers to set their own rules as the market (i.e., the tastes of those with money) dictates. Judge-made doctrines such as the requirement that running covenants "touch and concern land" have served to weed out some systems of "running" contractual arrangements, arguably those that are most vulnerable to these kinds of criticisms. It is true that Internet users can more easily exit the rules created by one sysop or content provider than condominium or subdivision dwellers can exit the rules created by the developer. The possibility of exit will not be of much use, however, if all of the desirable sites or content have similar rules.

D. The Issue of Enforcement

It is 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

56. *See, e.g.*, Ira V. Heffan, *Copyleft: Licensing Collaborative Works in The Digital Age*, 49 STAN. L. REV. 1487, 1492-1504 (1997); *Netscape Communicator Open Source Code White Paper* (visited Feb. 28, 1999) <http://sitesearch.netscape.com/browsers/future/whitepaper.html>.

57. The term "residential private government" was coined by Uriel Reichman. *See* Uriel Reichman, *Toward a Unified Concept of Servitudes*, 55 S. CAL. L. REV. 1177, 1238 (1982).

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; 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.[58] An analogy is the incorporation competition among states, with the attendant gradual decrease in corporate legal liability standards in past decades.[59] 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.[60] 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 their own rules, in which case self-regulation will fail.

Enforcement mechanisms are difficult to establish spontaneously and maintain through self-organized cooperation. Even if tacit coordination has held almost everyone to standardization on ".com," for example, why did not 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?

58. *See* Johnson & Post, *supra* note 5, at 87. 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. *See id.* at 82-84. Rules imposed by sysops would be avoided by simply changing ISPs. *See id.* at 84-89.

59. *See* William L Cary, *Federalism and Corporate Law: Reflections Upon Delaware*, 83 YALE L.J. 663, 702-05 (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* FRANK H. EASTERBROOK & DANIEL R. FISCHEL, THE ECONOMIC STRUCTURE OF CORPORATE LAW 213-18 (1991) (noting that empirical studies "fatally undermine" Cary's view that shareholders are victimized by incorporation in Delaware).

60. This argument, of course, assumes that a large proportion of Internet users have a similar orientation with respect to a significant issue. There is a strong counter-argument 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 Internet-specific taxation, for example, can be expected to be widely unpopular, thus, generating regulatory arbitrage, that is, tax havens in cyberspace.

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 will not agree to arbitrate or who fail to accept the terms of the arbitration body is the only ultimate remedy that can be reliably executed by self-ordering.

E. Technological Self-Help

This conclusion seems to be challenged, however, by the advent of trusted systems. Trusted systems are sophisticated rights-management programs. They can be programmed to prevent delivery of a piece of content until payment is received and credited, to prevent all copying of a piece of content or the making of more than *n* copies, to prevent printing a copy or more than *n* copies, to prevent reading it more than once or more than *n* times, to destroy the content if the user attempts to do something prohibited, and so on.[61] Many of the theories for self-ordering in the information context—the shift from copyright to contract, for example—rest on the assumption that all of the details of these contracts will be rendered self-enforcing through the use of trusted systems.[62]

Trusted systems are a species of technological self-help. They are more like building high fences than relying on nuisance law; more like moving out the tenant's furniture and changing the lock than relying on landlord-tenant law; and more like sending over a committee of one's friends to intimidate a storekeeper into paying a debt than relying on legal enforcement of contract.

A regime of technological self-enforcement by trusted systems is, in other words, anarchic rather than legal. For anarcho-cyberlibertarians,[63] this distinction is hard to see, but it should be clear to the rest of us. If trusted systems are the only way to "contract," there will be no such thing as "fair use" or "efficient breach." Indeed, there will be no way to use breach to police purported agreements; that is, if nobody can breach the offending contract, then the primary means of testing the legality of the bargain will disappear. Those who

61. *See* MARK J. STEFIK, INTERNET DREAMS: ARCHETYPES, MYTHS, AND METAPHORS 391-94 (1996).

62. For example, Fisher notes that "[s]uch devices . . . should be sufficient to keep the leakage [of content to unauthorized users] to a tolerable level." Fisher, *supra* note 3, at 1225.

63. *See supra* text accompanying notes 6-7.

desire not to accede to the strictures of a trusted system will be banished from access to the content it protects. So technological self-help regimes return us to the issue of banishment.

CONCLUSION: WHERE ARE WE HEADED?

A final point, then, about public or hybrid enforcement necessary to support a network of contractual self-ordering. Those who are banished will no doubt resort to the courts in their own countries or elsewhere in physical space, appealing to legal limitations on such banishment. So one suspects that enforcement mechanisms will evolve on the Internet into a hybrid of internal self-regulation and external sovereignty. But what if the Internet becomes a sovereign jurisdiction of its own, with its own constitution, courts, and police force?

A first step in that direction would be for courts in physical space 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. But what happens when someone appeals banishment? If cyberspace really acquired its own sovereignty, perhaps other sovereignties would not question its authority to de-nationalize (banish) its citizens. But perhaps it is 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 de-nationalization 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 do not 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 it 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 on-line contracts of adhesion are valid and enforceable.

As we suggest, the external courts might stop short of abstention in certain cases of banishment. Yet, if banishment is the only cyberspace enforcement mechanism with "teeth," external courts would have to accept even banishment in most cases if Internet self-regulation is to be stable. Moreover, the guidelines for the exceptional cases in which banishment would not be acceptable, so that an external court would find it appropriate to step in, would have to be consistent among all external sovereigns. That requires a lot more global agreement about due process and public policy limits on contract than we now have. Yet, the apparent alternative—a welter of conflicting local regulations—threatens to be either ineffective or to kill the promising commercial goose.

Internet proponents' best hope is for a process of evolution toward a regime in which there is enough harmony about the minimal standards of background due process and public policy limits so that all players, on and off the Internet, will understand and accept them. If such harmony could emerge, it would allow stable self-enforcement on the Internet, in the shadow of possible appeal to territorial sovereigns. We certainly have not reached such harmony yet. The needed background baseline of due process and public policy limits has a better chance of developing if participants do not obscure the understanding that contractual ordering cannot exist without it.