

LAW AND BORDERS - The Rise of Law in Cyberspace



By [DAVID R. JOHNSON](#) and [DAVID POST](#)

[Breaking Down Territorial Borders](#)

[A New Boundary for Cyberspace](#)

[Will Responsible Self-Regulatory Structures Emerge on the Net?](#)

[Local Authorities, Foreign Rules: Reconciling Conflicts](#)

[Internal Diversity](#)

Introduction

Global computer-based communications cut across territorial borders, creating a new realm of human activity and undermining the feasibility--and legitimacy--of applying laws based on geographic boundaries. While these electronic communications play havoc with geographic boundaries, a new boundary, made up of the screens and passwords that separate the virtual world from the "real world" of atoms, emerges. This new boundary defines a distinct Cyberspace that needs and can create new law and legal institutions of its own. Territorially-based law-making and law-enforcing authorities find this new environment deeply threatening. But established territorial authorities may yet learn to defer to the self-regulatory efforts of Cyberspace participants who care most deeply about this new digital trade in ideas, information, and services. Separated from doctrine tied to territorial jurisdictions, new rules will emerge, in a variety of online spaces, to govern a wide range of new phenomena that have no clear parallel in the nonvirtual world. These new rules will play the role of law by defining legal personhood and property, resolving disputes, and crystallizing a collective conversation about core values.

Breaking Down Territorial Borders

A. Territorial Borders in the "Real World"

We take for granted a world in which geographical borders--lines separating physical spaces--are of primary importance in determining legal rights and responsibilities: "All law is prima facie territorial. [1]" Territorial borders, generally speaking, delineate areas within which different sets of legal rules apply. There has until now been a general correspondence between borders drawn in physical space (between nation states or other political entities) and borders in "law space." For example, if we were to superimpose a "law map" (delineating areas where different rules apply to particular behaviors) onto a political map of the world, the two maps would overlap to a significant degree, with clusters of homogenous applicable law and legal institutions fitting within existing physical borders, distinct from neighboring homogenous clusters.

1. The Trademark Example

Consider a specific example to which we will refer throughout this article: trademark law--schemes for the protection of the associations between words or images and particular commercial enterprises. Trademark law is distinctly based on geographical separations [2]. Trademark rights typically arise within a given country, usually on the basis of use of a mark on physical goods or in connection with the provision of services in specific locations within that country. Different countries have different trademark laws, with important differences on matters as central as whether the same name can be used in different lines of business. In the United States, the same name can even be used for the same line of business if there is sufficient geographic separation of use to avoid confusion [3]. In fact, there are many local stores, restaurants, and businesses with identical names that do not interfere with each other because their customers do not overlap. The physical cues provided by different lines of business allow most marks to be used in multiple lines of commerce without dilution of the other users' rights [4]. There is no global registration scheme [5]; protection of a particularly famous mark on a global basis requires registration in each country. A trademark owner must therefore also be constantly alert to territorially-based claims of abandonment, and to dilution arising from uses of confusingly similar marks, and must master the different procedural and jurisdictional laws of various countries that apply in each such instance.

2. When Geographic Boundaries for Law Make Sense

Physical borders are not, of course, simply arbitrary creations. Although they may be based on historical accident, geographic borders for law make sense in the real world. Their relationship to the development and enforcement of legal rules is logically based on a number of related considerations.

Power.

Control over physical space, and the people and things located in that space, is a defining attribute of sovereignty and statehood [6]. Law-making requires some mechanism for law enforcement, which in turn depends (to a large extent) on the ability to exercise physical control over, and to impose coercive sanctions on, law-violators. For example, the U.S. government does not impose its trademark law on a Brazilian business operating in Brazil, at least in part because imposing sanctions on the Brazilian business would require assertion of physical control over those responsible for the operation of that business. Such an assertion of control would conflict with the Brazilian government's recognized monopoly on the use of force over its citizens [7].

Effects.

The correspondence between physical boundaries and boundaries in "law space" also reflects a deeply rooted relationship between physical proximity and the effects of any particular behavior. That is, Brazilian trademark law governs the use of marks in Brazil because that use has a more direct impact on persons and assets located within that geographic territory than anywhere else. For example, the existence of a large sign over "Jones' Restaurant" in Rio de Janeiro is unlikely to have an impact on the operation of "Jones' Restaurant" in Oslo, Norway, for we may assume that there is no substantial overlap between the customers, or competitors, of these two entities. Protection of the former's trademark does not--and probably should not--affect the protection afforded the latter's.

Legitimacy.

We generally accept the notion that the persons within a geographically defined border are the ultimate source of law-making authority for activities within that border [8]. The "consent of the governed" implies that those subject to a set of laws must have a role in their formulation. By virtue of the preceding considerations, the category of persons subject to a sovereign's laws, and most deeply affected by those laws, will consist primarily of individuals who are located in particular physical spaces. Similarly, allocation of responsibility among levels of government proceeds on the assumption that, for many legal problems, physical proximity between the responsible authority and those most directly affected by the law will improve the quality of decision making, and that it is easier to determine the will of those individuals in physical proximity to one another.

Notice.

Physical boundaries are also appropriate for the delineation of "law space" in the physical world because they can give notice that the rules change when the boundaries are crossed. Proper boundaries have signposts that provide warning that we will be required, after crossing, to abide by different rules, and physical boundaries -- lines on the geographical map -- are generally well-equipped to serve this signpost function [9].

B. The Absence of Territorial Borders in Cyberspace

Cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location. The rise of the global computer network is destroying the link between geographical location and: (1) the power of local governments to assert control over online behavior; (2) the effects of online behavior on individuals or things; (3) the legitimacy of the efforts of a local sovereign to enforce rules applicable to global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply. The Net thus radically subverts a system of rule-making based on borders between physical spaces, at least with respect to the claim that cyberspace should naturally be governed by territorially defined rules.

Cyberspace has no territorially-based boundaries, because the cost and speed of message transmission on the Net is almost entirely independent of physical location: Messages can be transmitted from any physical location to any other location without degradation, decay, or substantial delay, and without any physical cues or barriers that might otherwise keep certain geographically remote places and people separate from one another [10]. The Net enables transactions between people who do not know, and in many cases cannot know, the physical location of the other party. Location remains vitally important, but only location within a virtual space consisting of the "addresses" of the machines between which messages and information are routed. The system is indifferent to the physical location of those machines, and there is no necessary connection between an Internet address and a physical jurisdiction. Although a domain name, when initially assigned to a given machine, may be associated with a particular Internet Protocol address corresponding to the territory within which the machine is physically located (e.g., a ".uk" domain name extension), the machine may move in physical space without any movement in the logical domain name space of the Net. Or, alternatively, the owner of the domain name might request that the name become associated with an entirely different machine, in a different physical location [11]. Thus, a server with a ".uk" domain name may not necessarily be located in the United Kingdom, a server with a ".com" domain name may be anywhere, and users, generally speaking, are not even aware of the location of the server that stores the content that they read. Physical borders no longer can function as signposts informing individuals of the obligations assumed by entering into a new, legally significant, place, because individuals are unaware of the

existence of those borders as they move through virtual space.

The power to control activity in Cyberspace has only the most tenuous connections to physical location. Many governments first respond to electronic communications crossing their territorial borders by trying to stop or regulate that flow of information as it crosses their borders [12]. Rather than deferring to efforts by participants in online transactions to regulate their own affairs, many governments establish trade barriers, seek to tax any border-crossing cargo, and respond especially sympathetically to claims that information coming into the jurisdiction might prove harmful to local residents. Efforts to stem the flow increase as online information becomes more important to local citizens. In particular, resistance to "transborder data flow" (TDF) reflects the concerns of sovereign nations that the development and use of TDF's will undermine their "informational sovereignty," [13] will negatively impact on the privacy of local citizens, [14] and will upset private property interests in information [15]. Even local governments in the United States have expressed concern about their loss of control over information and transactions flowing across their borders [16].

But efforts to control the flow of electronic information across physical borders--to map local regulation and physical boundaries onto Cyberspace--are likely to prove futile, at least in countries that hope to participate in global commerce [17]. Individual electrons can easily, and without any realistic prospect of detection, "enter" any sovereign's territory. The volume of electronic communications crossing territorial boundaries is just too great in relation to the resources available to government authorities to permit meaningful control. U.S. Customs officials have generally given up. They assert jurisdiction only over the physical goods that cross the geographic borders they guard and claim no right to force declarations of the value of materials transmitted by modem [18]. Banking and securities regulators seem likely to lose their battle to impose local regulations on a global financial marketplace [19]. And state Attorneys General face serious challenges in seeking to intercept the electrons that transmit the kinds of consumer fraud that, if conducted physically within the local jurisdiction, would be more easily shut down.

Faced with their inability to control the flow of electrons across physical borders, some authorities strive to inject their boundaries into the new electronic medium through filtering mechanisms and the establishment of electronic barriers [20]. Others have been quick to assert the right to regulate all online trade insofar as it might adversely impact local citizens. The Attorney General of Minnesota, for example, has asserted the right to regulate gambling that occurs on a foreign web page that was accessed and "brought into" the state by a local resident [21]. The New Jersey securities regulatory agency has similarly asserted the right to shut down any offending Web page accessible from within the state [22].

But such protective schemes will likely fail as well. First, the determined seeker of prohibited communications can simply reconfigure his connection so as to appear to reside in a different location, outside the particular locality, state, or country. Because the Net is engineered to work on the basis of "logical," not geographical, locations, any attempt to defeat the independence of messages from physical locations would be as futile as an effort to tie an atom and a bit together. And, moreover, assertions of law-making authority over Net activities on the ground that those activities constitute "entry into" the physical jurisdiction can just as easily be made by any territorially-based authority. If Minnesota law applies to gambling operations conducted on the World Wide Web because such operations foreseeably affect Minnesota residents, so, too, must the law of any physical jurisdiction from which those operations can be accessed. By asserting a right to regulate whatever its citizens may access on the Net, these local authorities are laying the predicate for an argument that Singapore or Iraq or any other sovereign can regulate the activities of U.S. companies operating in cyberspace from a location physically within the United States. All such Web-based activity, in this view, must be subject simultaneously to the laws of all territorial sovereigns.

Nor are the effects of online activities tied to geographically proximate locations. Information available on the World Wide Web is available simultaneously to anyone with a connection to the global network. The notion that the effects of an activity taking place on that Web site radiate from a physical location over a geographic map in concentric circles of decreasing intensity, however sensible that may be in the nonvirtual world, is incoherent when applied to Cyberspace. A Web site physically located in Brazil, to continue with that example, has no more of an effect on individuals in Brazil than does a Web site physically located in Belgium or Belize that is accessible in Brazil. Usenet discussion groups, to take another example, consist of continuously changing collections of messages that are routed from one network to another, with no centralized location at all; they exist, in effect, everywhere, nowhere in particular, and only on the Net [23].

Nor can the legitimacy of any rules governing online activities be naturally traced to a geographically situated polity. There is no geographically localized set of constituents with a stronger claim to regulate it than any other local group; the strongest claim to control comes from the participants themselves, and they could be anywhere.

The rise of an electronic medium that disregards geographical boundaries also throws the law into disarray by creating entirely new phenomena that need to become the subject of clear legal rules but that cannot be governed, satisfactorily, by any current territorially-based sovereign. For example, electronic communications create vast new quantities of transactional records and pose serious questions regarding the nature and adequacy of privacy protections. Yet the communications that create these records may pass through or even simultaneously exist in many different territorial jurisdictions [24]. What substantive law should we apply to protect this new, vulnerable body of transactional data [25]? May a French policeman lawfully access the records of communications traveling across the Net from the United States to Japan? Similarly, whether it is permissible for a commercial entity to publish a record of all of any given individual's postings to Usenet newsgroups, or whether it is permissible to implement an interactive Web page application that inspects a user's "bookmarks" to determine which other pages that user has visited, are questions not readily addressed

by existing legal regimes--both because the phenomena are novel and because any given local territorial sovereign cannot readily control the relevant, globally dispersed, actors and actions [26].

Because events on the Net occur everywhere but nowhere in particular, are engaged in by online personae who are both "real" (possessing reputations, able to perform services, and deploy intellectual assets) and "intangible" (not necessarily or traceably tied to any particular person in the physical sense), and concern "things" (messages, databases, standing relationships) that are not necessarily separated from one another by any physical boundaries, no physical jurisdiction has a more compelling claim than any other to subject these events exclusively to its laws.

1. The Trademark Example.

The question who should regulate or control Net domain names presents an illustration of the difficulties faced by territorially-based law-making. The engineers who created the Net devised a "domain name system" that associates numerical machine addresses with easier-to-remember names. Thus, an Internet Protocol machine address like "36.21.0.69" can be derived, by means of a lookup table, from "leland.stanford.edu." Certain letter extensions (".com," ".edu," ".org," and ".net") have developed as global domains with no association to any particular geographic area [27]. Although the Net creators designed this system as a convenience, it rapidly developed commercial value, because it allows customers to learn and remember the location of particular Web pages or e-mail addresses. Currently, domain names are registered with specific parties who echo the information to "domain name servers" around the world. Registration generally occurs on a "first come, first served" basis [28], generating a new type of property akin to trademark rights, but without inherent ties to the trademark law of any individual country. Defining rights in this new, valuable property presents many questions, including those relating to transferability, conditions for ownership (such as payment of registration fees), duration of ownership rights, and forfeiture in the event of abandonment, however defined. Who should make these rules?

Consider the placement of a "traditional" trademark on the face of a World Wide Web page. This page can be accessed instantly from any location connected to the Net. It is not clear that any given country's trademark authorities possess, or should possess, jurisdiction over such placements. Otherwise, any use of a trademark on the net would be subject simultaneously to the jurisdiction of every country. Should a Web page advertising a local business in Illinois be deemed to infringe a trademark in Brazil just because the page can be accessed freely from Brazil? Large U.S. companies may be upset by the appearance on the Web of names and symbols that overlap with their valid U.S.-registered trademarks. But these same names and symbols could also be validly registered by another party in Mexico whose "infringing" marks are now, suddenly, accessible from within the United States. Upholding a claim of infringement or dilution launched by the holder of a U.S.-registered trademark, solely on the basis of a conflicting mark on the Net, exposes that same trademark holder to claims from other countries when the use of their U.S.-registered mark on the Web would allegedly infringe a similar mark in those foreign jurisdictions.

2. Migration of Other Regulated Conduct to the Net.

Almost everything involving the transfer of information can be done online: education, health care, banking, the provision of intangible services, all forms of publishing, and the practice of law. The laws regulating many of these activities have developed as distinctly local and territorial. Local authorities certify teachers, charter banks with authorized "branches," and license doctors and lawyers. The law has in essence presumed that the activities conducted by these regulated persons cannot be performed without being tied to a physical body or building subject to regulation by the territorial sovereign authority, and that the effects of those activities are most distinctly felt in geographically circumscribed areas. These distinctly local regulations cannot be preserved once these activities are conducted by globally dispersed parties through the Net. When many trades can be practiced in a manner that is unrelated to the physical location of the participants, these local regulatory structures will either delay the development of the new medium or, more likely, be superseded by new structures that better fit the online phenomena in question [29].

Any insistence on "reducing" all online transactions to a legal analysis based in geographic terms presents, in effect, a new "mind-body" problem on a global scale. We know that the activities that have traditionally been the subject of regulation must still be engaged in by real people who are, after all, at distinct physical locations. But the interactions of these people now somehow transcend those physical locations. The Net enables forms of interaction in which the shipment of tangible items across geographic boundaries is irrelevant and in which the location of the participants does not matter. Efforts to determine "where" the events in question occur are decidedly misguided, if not altogether futile.

A New Boundary for Cyberspace

Although geographic boundaries may be irrelevant in defining a legal regime for Cyberspace, a more legally significant border for the "law space" of the Net consists of the screens and passwords that separate the tangible from the virtual world. Traditional legal doctrine treats the Net as a mere transmission medium that facilitates the exchange of messages sent from one legally significant geographical location to another, each of which has its own applicable laws. Yet, trying to tie the laws of any particular territorial sovereign to transactions on the Net, or even trying to analyze the legal consequences of Net-based commerce as if each transaction occurred geographically somewhere in particular, is most unsatisfying.



A. Cyberspace as a Place

Many of the jurisdictional and substantive quandaries raised by border-crossing electronic communications could be resolved by one simple principle: conceiving of Cyberspace as a distinct "place" for purposes of legal analysis by recognizing a legally significant border between Cyberspace and the "real world." Using this new approach, we would no longer ask the unanswerable question "where" in the geographical world a Net-based transaction occurred. Instead, the more salient questions become: What rules are best suited to the often unique characteristics of this new place and the expectations of those who are engaged in various activities there? What mechanisms exist or need to be developed to determine the content of those rules and the mechanisms by which they can be enforced? Answers to these questions will permit the development of rules better suited to the new phenomena in question, more likely to be made by those who understand and participate in those phenomena, and more likely to be enforced by means that the new global communications media make available and effective.



1. The New Boundary is Real.

Treating Cyberspace as a separate "space" to which distinct laws apply should come naturally, because entry into this world of stored online communications occurs through a screen and (usually) a "password" boundary [30]. There is a "placeness" to Cyberspace because the messages accessed there are persistent and accessible to many people [31]. You know when you are "there." No one accidentally strays across the border into Cyberspace [32]. To be sure, Cyberspace is not a homogenous place; groups and activities found at various online locations possess their own unique characteristics and distinctions, and each area will likely develop its own set of distinct rules [33]. But the line that separates online transactions from our dealings in the real world is just as distinct as the physical boundaries between our territorial governments--perhaps more so [34].

Crossing into Cyberspace is a meaningful act that would make application of a distinct "law of Cyberspace" fair to those who pass over the electronic boundary. As noted, a primary function and characteristic of a border or boundary is its ability to be perceived by the one who crosses it [35]. As regulatory structures evolve to govern Cyberspace-based transactions, it will be much easier to be certain which of those rules apply to your activities online than to determine which territorial-based authority might apply its laws to your conduct. For example, you would know to abide by the "terms of service" established by CompuServe or America Online when you are in their online territory, rather than guess whether Germany, or Tennessee, or the SEC will succeed in asserting their right to regulate your activities and those of the "placeless" online personae with whom you communicate.

2. The Trademark Example.

The ultimate question who should set the rules for uses of names on the Net presents an apt microcosm for examining the relationship between the Net and territorial-based legal systems. There is nothing more fundamental, legally, than a name or identity--the right to legally recognized personhood is a predicate for the amassing of capital, including the reputational and financial capital, that arises from sustained interactions. The domain name system, and other online uses of names and symbols tied to reputations and virtual locations, exist operationally only on the Net. These names can, of course, be printed on paper or embodied in physical form and shipped across geographic borders. But such physical uses should be distinguished from electronic use of such names in Cyberspace, because publishing a name or symbol on the Net is not the same as intentional distribution to any particular jurisdiction. Instead, use of a name or symbol on the Net is like distribution to all jurisdictions simultaneously. Recall that the non-country-specific domain names like ".com," and ".edu" lead to the establishment of online addresses on a global basis. And through such widespread use, the global domain names gained proprietary value. In this context, assertion by any local jurisdiction of the right to set the rules applicable to the "domain name space" is an illegitimate extra-territorial power grab.

Conceiving of the Net as a separate place for purposes of legal analysis will have great simplifying effects. For example, a global registration system for all domain names and reputationally significant names and symbols used on the Net would become possible. Such a Net-based regime could take account of the special claims of owners of strong global marks (as used on physical goods) and "grandfather" these owners' rights to the use of their strong marks in the newly opened online territory. But a Net-based global registration system could also fully account for the true nature of the Net by treating the use of marks on Web pages as a global phenomena, by assessing the likelihood of confusion and dilution in the online context in which such confusion would actually occur, and by harmonizing any rules with applicable engineering criteria, such as optimizing the overall size of the domain name space.

A distinct set of rules applicable to trademarks in Cyberspace would greatly simplify matters by providing a basis to resist the inconsistent and conflicting assertions of geographically local prerogatives. If one country objects to the use of a mark on the Web that conflicts with a locally registered mark, the rebuttal would be that the mark has not been used inside the country at all, but only on the Web. If a company wants to know where to register its use of a symbol on the Net, or to check for conflicting prior uses of its mark, the answer will be obvious and cost effective: the designated registration authority for the relevant portion of the Net itself. If we need to develop rules governing abandonment, dilution, and conditions on uses of particular types of domain names and addresses, those rules--applicable specifically to Cyberspace--will be able to reflect the special characteristics of this new electronic medium [36].

B. Other Cyberspace Regimes

Once we take Cyberspace seriously as a distinct place for purposes of legal analysis, many opportunities to clarify and simplify the rules applicable to online transactions become available.

1. Defamation Law

Treating messages on the Net as transmissions from one place to another has created a quandary for those concerned about liability for defamation: Messages may be transmitted between countries with very different laws, and liability may be imposed on the basis of "publication" in multiple jurisdictions with varying standards [37]. In contrast, the approach that treats the global network as a separate place would consider any allegedly defamatory message to have been published only "on the Net" (or in some distinct subsidiary area thereof)--at least until such time as distribution on paper occurs [38]. This re-characterization makes more sense. A person who uploads a potentially defamatory statement would be able more readily to determine the rules applicable to his own actions. Moreover, because the Net has distinct characteristics, including an enhanced ability of the allegedly defamed person to reply, the rules of defamation developed for the Net could take into account these technological capabilities --perhaps by requiring that the opportunity for reply be taken advantage of in lieu of monetary compensation for certain defamatory net-based messages [39]. The distinct characteristics of the Net could also be taken into account when applying and adapting the "public figure" doctrine in a context that is both global and highly compartmentalized and that blurs the distinction between private and public spaces.

2. Regulation of Net-Based Professional Activities

The simplifying effect of "taking Cyberspace seriously" likewise arises in the context of regimes for regulating professional activities. As noted, traditional regulation insists that each professional be licensed by every territorial jurisdiction where she provides services [40]. This requirement is infeasible when professional services are dispensed over the Net and potentially provided in numerous jurisdictions. Establishing certification regimes that apply only to such activities on the Net would greatly simplify matters. Such regulations would take into account the special features of Net-based professional activities like tele-medicine or global law practice by including the need to avoid any special risks caused by giving online medical advice in the absence of direct physical contact with a patient or by answering a question regarding geographically local law from a remote location [41]. Using this new approach, we could override the efforts of local school boards to license online educational institutions, treating attendance by students at online institutions as a form of "leaving home for school" rather than characterizing the offering of education online as prosecutable distribution of disfavored materials into a potentially unwelcoming community that asserts local licensing authority.

3. Fraud and Antitrust

Even an example that might otherwise be thought to favor the assertion of jurisdiction by a local sovereign--protection of local citizens from fraud and antitrust violations--shows the beneficial effects of a Cyberspace legal regime. How should we analyze "markets" for antitrust and consumer protection purposes when the companies at issue do business only through the World Wide Web? Cyberspace could be treated as a distinct marketplace for purposes of assessing concentration and market power. Concentration in geographic markets would only be relevant in the rare cases in which such market power could be inappropriately leveraged to obtain power in online markets--for example by conditioning access to the net by local citizens on their buying services from the same company (such as a phone company) online. Claims regarding a right to access to particular online services, as distinct from claims to access particular physical pipelines, would remain tenuous as long as it is possible to create a new online service instantly in any corner of an expanding online space [42].

Consumer protection doctrines could also develop differently online--to take into account the fact that anyone reading an online ad is only a mouse click away from guidance from consumer protection agencies and discussions with other consumers. Can Minnesota prohibit the establishment of a Ponzi scheme on a Web page physically based in the Cayman islands but accessed by Minnesota citizens through the Net? Under the proposed new approach to regulation of online activities, the answer is clearly no. Minnesota has no special right to prohibit such activities. The state lacks enforcement power, cannot show specially targeted effects, and does not speak for the community with the most legitimate claim to self-governance. But that does not mean that fraud might not be made "illegal" in at least large areas of Cyberspace. Those who establish and use online systems have a interest in preserving the safety of their electronic territory and preventing crime. They are more likely to be able to enforce their own rules. And, as more fully discussed below, insofar as a consensually based "law of the Net" needs to obtain respect and deference from local sovereigns, new Net-based law-making institutions have an incentive to avoid fostering activities that threaten the vital interests of territorial governments.

4. Copyright Law

We suggest, not without some trepidation, that "taking Cyberspace seriously" could clarify the current intense debate about how to apply copyright law principles in the digital age. In the absence of global agreement on applicable copyright principles, the jurisdictional problems inherent in any attempt to apply territorially-based copyright regimes to electronic works simultaneously available everywhere on the globe are profound. As Jane Ginsburg has noted:



A key feature of the GII [Global Information Infrastructure] is its ability to render works of authorship pervasively and simultaneously accessible throughout the world. The principle of territoriality becomes problematic if it means that posting a work on the GII calls into play the laws of every country in which the work may be received when . . . these laws may differ substantively. Should the rights in a work be determined by a multiplicity of inconsistent legal regimes

when the work is simultaneously communicated to scores of countries? Simply taking into account one country's laws, the complexity of placing works in a digital network is already daunting; should the task be further burdened by an obligation to assess the impact of the laws of every country where the work might be received? Put more bluntly, for works on the GII, there will be no physical territoriality . . . Without physical territoriality, can legal territoriality persist [43]?

But treating Cyberspace as a distinct place for purposes of legal analysis does more than resolve the conflicting claims of different jurisdictions: It also allows the development of new doctrines that take into account the special characteristics of the online "place."

The basic justification for copyright protection is that bestowing an exclusive property right to control the reproduction and distribution of works on authors will increase the supply of such works by offering authors a financial incentive to engage in the effort required for their creation [44]. But even in the "real world," much creative expression is entirely independent of this incentive structure, because the author's primary reward has more to do with acceptance in a community and the accumulation of reputational capital through wide dissemination than it does with the licensing and sale of individual copies of works [45]. And that may be more generally true of authorship in Cyberspace; because authors can now, for the first time in history, deliver copies of their creations instantaneously and at virtually no cost anywhere in the world, one might expect authors to devise new modes of operation that take advantage of, rather than work counter to, this fundamental characteristics of the new environment [46]. One such strategy has already begun to emerge: giving away information at no charge -- what might be called the "Netscape strategy [47]" -- as a means of building up reputational capital that can subsequently be converted into income (e.g., by means of the sale of services). As Esther Dyson has written:

Controlling copies (once created by the author or by a third party) becomes a complex challenge. You can either control something very tightly, limiting distribution to a small, trusted group, or you can rest assured that eventually your product will find its way to a large nonpaying audience - if anyone cares to have it in the first place. . . . Much chargeable value will be in certification of authenticity and reliability, not in the content. Brand name, identity, and other marks of value will be important; so will security of supply. Customers will pay for a stream of information and content from a trusted source. For example, the umbrella of The New York Times sanctifies the words of its reporters. The content churned out by Times reporters is valuable because the reporters undergo quality-control, and because others believe them. . . . The trick is to control not the copies of your work but instead a relationship with the customers - subscriptions or membership. And that's often what the customers want, because they see it as an assurance of a continuing supply of reliable, timely content [48].

A profound shift of this kind in regard to authorial incentives fundamentally alters the applicable balance between the costs and benefits of copyright protection in Cyberspace, calling for a reappraisal of long-standing principles [49]. So, too, do other unique characteristics of Cyberspace severely challenge traditional copyright concepts [50]. The very ubiquity of file "copying" -- the fact that one cannot access any information whatsoever in a computer-mediated environment without making a "copy" of that information [51] --implies that any simple-minded attempt to map traditional notions of "copying" onto Cyberspace transactions will have perverse results [52]. Application of the "first sale" doctrine (allowing the purchaser of a copyrighted work to freely resell the copy she purchased) is problematic when the transfer of a lawfully owned copy technically involves the making of a new copy before the old one is eliminated [53], as is defining "fair use" when a work's size is indeterminate, ranging from (1) an individual paragraph sold separately on demand in response to searches to (2) the entire database from which the paragraph originates, something never sold as a whole unit [54].

Treating Cyberspace as a distinct location allows for the development of new forms of intellectual property law, applicable only on the Net, that would properly focus attention on these unique characteristics of this new, distinct place while preserving doctrines that apply to works embodied in physical collections (like books) or displayed in legally significant physical places (like theaters). Current debates about applying copyright law to the Net often do, implicitly, treat it as a distinct space, at least insofar as commercial copyright owners somewhat inaccurately refer to it as a "lawless" place [55]. The civility of the debate might improve if everyone assumed the Net should have an appropriately different law, including a special law for unauthorized transfers of works from one realm to the other; we could, in other words, regulate the smuggling of works created in the physical world, by treating the unauthorized uploading of a copy of such works to the Net as infringement. This new approach would help promoters of electronic commerce focus on developing incentive-producing rules to encourage authorized transfers into Cyberspace of works not available now, while also reassuring owners of existing copyrights to valuable works that changes in the copyright law for the Net would not require changing laws applicable to distributing physical works. It would also permit the development of new doctrines of implied license and fair use that, as to works first created on the Net or imported with the author's permission, appropriately allow the transmission and copying necessary to facilitate their use within the electronic realm [56].

Will Responsible Self-Regulatory Structures Emerge on the Net?

Even if we agree that new rules should apply to online phenomena, questions remain about who sets the rules and how they are enforced. We believe the Net can develop its own effective legal institutions.

The Trademark Example.

In order for the domain name space to be administered by a legal authority that is not territorially based, new law-making institutions will have to develop. Many questions that arise in setting up this system will need answers--decisions about whether to create a new top level domain, whether online addresses belong to users or service providers [57], and whether one name impermissibly interferes with another, thus confusing the public and diluting the value of the pre-existing name [58]. The new system must also include procedures to give notice in conflicting claims, to resolve these claims, and to assess appropriate remedies (including, possibly, compensation) in cases of wrongful use. If the Cyberspace equivalent of eminent domain develops, questions may arise over how to compensate individuals when certain domain names are destroyed or redeployed for the public good of the Net community [59]. Someone must also decide threshold membership issues for Cyberspace citizens, including how much users must disclose (and to whom) about their real-world identities to use e-mail addresses and domain names for commercial purposes. Implied throughout this discussion is the recognition that these rules will only be meaningful and enforceable if Cyberspace citizens view whomever makes these decisions as a legitimate governing body.

Experience suggests that the community of online users and service providers is up to the task of developing a self-governance system [60]. The current domain name system evolved from decisions made by engineers and the practices of Internet service providers [61]. Now that trademark owners are threatening the company that administers the registration system, the same engineers who established the original domain name standards are again deliberating whether to alter the domain name system to take these new policy issues into account [62]. Who has the ultimate right to control policy in this area remains unclear [63].

Every system operator who dispenses a password imposes at least some requirements as conditions of continuing access, including paying bills on time or remaining a member of a group entitled to access (e.g. students at a university) [64]. System operators (sysops) have an extremely powerful enforcement tool at their disposal to enforce such rules--banishment [65]. Moreover, communities of users have marshaled plenty of enforcement weapons to induce wrongdoers to comply with local conventions such as rules against flaming [66], shunning [67], mailbombs, and more [68]. And both sysops and users have begun explicitly to recognize that formulating and enforcing such rules should be a matter for principled discussion, not an act of will by whoever has control of the power switch [69].

While many of these new rules and customs apply only to specific, local areas of the global network, some standards apply through technical protocols on a nearly universal basis. And widespread agreement already exists about core principles of "netiquette" in mailing lists and discussion groups [70]--although, admittedly, new users have a slow learning curve and the Net offers little formal "public education" regarding applicable norms [71]. Dispute resolution mechanisms suited to this new environment also seem certain to prosper [72]. Cyberspace is anything but anarchic; its distinct rule sets are becoming more robust every day.

Perhaps the most apt analogy to the rise of a separate law of Cyberspace is the origin of the Law Merchant--a distinct set of rules that developed with the new, rapid boundary-crossing trade of the Middle Ages [73]. Merchants could not resolve their disputes by taking them to the local noble, whose established feudal law mainly concerned land claims. Nor could the local lord easily establish meaningful rules for a sphere of activity he barely understood, executed in locations beyond his control. The result of this jurisdictional confusion, arising from a then-novel form of boundary-crossing communications, was the development of a new legal system--Lex Mercatoria [74]. The people who cared most about and best understood their new creation formed and championed this new law, which did not destroy or replace existing law regarding more territorially-based transactions (e.g. transferring land ownership). Arguably, exactly the same type of phenomenon is developing in Cyberspace right now [75].

Governments cannot stop electronic communications coming across their borders, even if they want to do so. Nor can they credibly claim a right to regulate the Net based on supposed local harms caused by activities that originate outside their borders and that travel electronically to many different nations; one nation's legal institutions should not, therefore, monopolize rule-making for the entire Net. Even so, established authorities likely will continue to claim that they must analyze and regulate the new online phenomena in terms of some physical locations. After all, the people engaged in online communications still inhabit the material world. And, so the argument goes, local legal authorities must have authority to remedy the problems created in the physical world by those acting on the Net. The rise of responsible law-making institutions within Cyberspace, however, will weigh heavily against arguments that would claim that the Net is "lawless" and thus tie regulation of online trade to physical jurisdictions. As noted, sysops acting alone or collectively have the power of banishment to control wrongful actions online [76]. Thus, for online activities that minimally impact the vital interests of sovereigns, the self-regulating structures of Cyberspace seem better suited than local authorities to deal with the Net's legal issues [77].

Local Authorities, Foreign Rules: Reconciling Conflicts

What should happen when conflicts arise between the local territorial law (applicable to persons or entities by virtue of their location in a particular area of physical space) and the law applicable to particular activities on the Net? The doctrine of "comity," as well as principles applied when delegating authority to self-regulatory organizations, provide us with guidance for reconciling such disputes.

The doctrine of comity, in the Supreme Court's classic formulation, is "the recognition which one nation allows within its territory to the legislative, executive, or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or of other persons who are under the protections of its law [78]." It is incorporated into the principles set forth in the Restatement (Third) of Foreign Relations Law of the United States, in particular Section 403, which provides that "a state may not exercise jurisdiction to prescribe law with respect to a person or activity having connections with another state when the exercise of such jurisdiction is unreasonable [79]," and that when a conflict between the laws of two states arises, "each state has an obligation to evaluate its own as well as the other state's interest in exercising jurisdiction [and] should defer to the other state if that state's interest is clearly greater." [80]. It arose as an attempt to mitigate some of the harsher features of a world in which lawmaking is an attribute of control over physical space but in which persons, things, and actions may move across physical boundaries, and it functions as a constraint on the strict application of territorial principles that attempts to reconcile "the principle of absolute territorial sovereignty [with] the fact that intercourse between nations often demand[s] the recognition of one sovereign's lawmaking acts in the forum of another [81]." In general, comity reflects the view that those who care more deeply about and better understand the disputed activity should determine the outcome. Accordingly, it may be ideally suited to handle, by extension, the new conflicts between the a-territorial nature of cyberspace activities and the legitimate needs of territorial sovereigns and of those whose interests they protect on the other side of the cyberspace border. This doctrine does not disable territorial sovereigns from protecting the interests of those individuals located within their spheres of control, but it calls upon them to exercise a significant degree of restraint when doing so.

Local officials handling conflicts can also learn from the many examples of delegating authority to self-regulatory organizations. Churches are allowed to make religious law [82]. Clubs and social organizations can, within broad limits, define rules that govern activities within their spheres of interest [83]. Securities exchanges can establish commercial rules, so long as they protect the vital interests of the surrounding communities. In these cases, government has seen the wisdom of allocating rule-making functions to those who best understand a complex phenomenon and who have an interest in assuring the growth and health of their shared enterprise.

Cyberspace represents a new permutation of the underlying issue: How much should local authorities defer to a new, self-regulating activity arising independently of local control and reaching beyond the limited physical boundaries of the sovereign. This mixing of both tangible and intangible boundaries leads to a convergence of the intellectual categories of comity in international relations and the local delegation by a sovereign to self-regulatory groups. In applying both the doctrine of "comity" and the idea of "delegation" [84] to Cyberspace, a local sovereign is called upon to defer to the self-regulatory judgments of a population partly, but not wholly, composed of its own subjects [85].

Despite the seeming contradiction of a sovereign deferring to the authority of those who are not its own subjects, such a policy makes sense, especially in light of the underlying purposes of both doctrines. Comity and delegation represent the wise conservation of governmental resources and allocate decisions to those who most fully understand the special needs and characteristics of a particular "sphere" of being. Although Cyberspace represents a new sphere that cuts across national boundaries, the fundamental principle remains. If the sysops and users who collectively inhabit and control a particular area of the Net want to establish special rules to govern conduct there, and if that rule set does not fundamentally impinge upon the vital interests of others who never visit this new space, then the law of sovereigns in the physical world should defer to this new form of self-government.

Consider, once again, the trademark example. A U.S. government representative has stated that, since the government paid for the initial development and administration of the domain name system, it "owns" the right to control policy decisions regarding the creation and use of such names [86]. Obviously, government funds, in addition to individual efforts on a global scale, created this valuable and finite new asset. But the government's claim based on its investment is not particularly convincing. In fact, the United States may be asserting its right to control the policies governing the domain name space primarily because it fears that any other authority over the Net might force it to pay again for the ".gov" and ".mil" domain names used by governmental entities [87]. To assuage these concerns, a Net-based authority should concede to the governments on this point. For example, it should accommodate the military's strong interest in remaining free to regulate and use its ".mil" addresses [88]. A new Net-based standards-making authority should also accommodate the government's interests in retaining its own untaxed domain names and prohibiting counterfeiting. Given responsible restraint by the Net-based authority and the development of an effective self-regulatory scheme, the government might well then decide that it should not spend its finite resources trying to wrest effective control of non-governmental domain names away from those who care most about facilitating the growth of online trade.

Because controlling the flow of electrons across physical boundaries is so difficult, a local jurisdiction that seeks to prevent its citizens from accessing specific materials must either outlaw all access to the Net--thereby cutting itself off from the new global trade--or seek to impose its will on the Net as a whole. This would be the modern equivalent of a local lord in medieval times either trying to prevent the silk trade from passing through his boundaries (to the dismay of local customers and merchants) or purporting to assert jurisdiction over the known world. It may be most difficult to envision local territorial sovereigns deferring to the law of the Net when the perceived threat to local interests arises from the very free flow of information that is the Net's most fundamental characteristic--when, for example, local sovereigns assert an interest in seeing that their citizens are not adversely affected by information that the local jurisdiction deems harmful but that is freely (and lawfully) available elsewhere. Examples include the German government's attempts to prevent its citizens access to prohibited materials [89], or the



prosecution of a California bulletin board operator for making material offensive to local "community standards" available for downloading in Tennessee [90]. Local sovereigns may insist that their interest (in protecting their citizens from harm) is paramount, and easily outweighs any purported interest in making this kind of material freely available. But the opposing interest is not simply the interest in seeing that individuals have access to ostensibly obscene material, it is the "meta-interest" of Net citizens in preserving the global free flow of information. If there is one central principle on which all local authorities within the Net should agree, it must be that territorially local claims to restrict online transactions (in ways unrelated to vital and localized interests of a territorial government) should be resisted. This is the Net equivalent of the First Amendment, a principle already recognized in the form of the international human rights doctrine protecting the right to communicate [91]. Participants in the new online trade must oppose external regulation designed to obstruct this flow. This naturally central principle of online law bears importantly on the "comity" analysis, because it makes clear that the need to preserve a free flow of information across the Net is just as vital to the interests of the Net as the need to protect local citizens against the impacts of unwelcome information may appear from the perspective of a local territorial sovereign [92]. For the Net to realize its full promise, online rule-making authorities must not respect the claims of territorial sovereigns to restrict online communications when unrelated to vital and localized governmental interests.

Internal Diversity

One of a border's key characteristics is that it slows the interchange of people, things, and information across its divide. Arguably, distinct sets of legal rules can only develop and persist where effective boundaries exist. The development of a true "law of Cyberspace," therefore, depends upon a dividing line between this new online territory and the nonvirtual world. Our argument so far has been that the new sphere online is cut off, at least to some extent, from rule-making institutions in the material world and requires the creation of a distinct law applicable just to the online sphere.

But we hasten to add that Cyberspace is not, behind that border, a homogeneous or uniform territory behind that border, where information flows without further impediment. Although it is meaningless to speak of a French or Armenian portion of Cyberspace, because the physical borders dividing French or Armenian territory from their neighbors cannot generally be mapped onto the flow of information in Cyberspace, the Net has other kinds of internal borders delineating many distinct internal locations that slow or block the flow of information. Distinct names and (virtual) addresses, special passwords, entry fees, and visual cues --software boundaries--can distinguish subsidiary areas from one another. The Usenet newsgroup "alt.religion.scientology" is distinct from "alt.misc.legal," each of which is distinct from a chat room on CompuServe or America Online which, in turn, are distinct from the Cyberspace Law Institute listserver or Counsel Connect. Users can only access these different forums through distinct addresses or phone numbers, often navigating through login screens, the use of passwords, or the payment of fees. Indeed, the ease with which internal borders, consisting entirely of software protocols, can be constructed is one of Cyberspace's most remarkable and salient characteristics; setting up a new Usenet newsgroup, or a "listserver" discussion group, requires little more than a few lines of code [93].

The separation of subsidiary "territories" or spheres of activity within Cyberspace and the barriers to exchanging information across these internal borders allow for the development of distinct rule sets and for the divergence of those rule sets over time [94]. The processes underlying biological evolution provide a useful analogy [95]. Speciation--the emergence over time of multiple, distinct constellations of genetic information from a single, original group--cannot occur when the original population freely exchanges information (in the form of genetic material) among its members. In other words, a single, freely-interbreeding population of organisms cannot divide into genetically distinct populations; while the genetic material in the population changes over time, it does so more or less uniformly--e.g. the population of the species *Homo erectus* becomes a population of *Homo sapiens*--and cannot give rise to more than one contemporaneous, distinct genetic set. Speciation requires, at a minimum, some barrier to the interchange of genetic material between subsets of the original homogeneous population. Ordinarily, a physical barrier suffices to prevent one subgroup from exchanging genetic data with another. Once this "border" is in place, divergence within the "gene pool"--the aggregate of the underlying genetic information--in each of the two subpopulations can occur [96]. Over time, this divergence may be substantial enough that even when the physical barrier disappears, the two subgroups can no longer exchange genetic material--i.e., they have become separate species.

Rules, like genetic material, are self-replicating information [97]. The internal borders within Cyberspace will thus allow for differentiation among distinct constellations of such information--in this case rule-sets rather than species. Content or conduct acceptable in one "area" of the Net may be banned in another. Institutions that resolve disputes in one "area" of Cyberspace may not gain support or legitimacy in others. Local sysops can, by contract, impose differing default rules regarding who has the right, under certain conditions, to replicate and redistribute materials that originate with others. While Cyberspace's reliance on bits instead of atoms may make physical boundaries more permeable, the boundaries delineating digital online "spheres of being" may become less permeable. Securing online systems from unauthorized intruders may prove an easier task than sealing physical borders from unwanted immigration [98]. Groups can establish online corporate entities or membership clubs that tightly control participation in, or even public knowledge of, their own affairs. Such groups can reach agreement on or modify these rules more rapidly via online communications. Accordingly, the rule sets applicable to the online world may quickly evolve away from those applicable to more traditional spheres and develop greater variation among the sets.

How this process of differentiation and evolution will proceed is one of the more complex and fascinating questions about law in Cyberspace--and a subject beyond the scope of this Article. We should point out, however, an important normative dimension to the proliferation of these internal boundaries between distinct communities and distinct rule-sets and the

process by which law will evolve in Cyberspace. Cyberspace may be an important forum for the development of new connections between individuals and mechanisms of self-governance by which individuals attain an increasingly elusive sense of community; commenting on the erosion of national sovereignty in the modern world and the failure of the existing system of nation-states to cultivate a "civic voice," a moral connection between the individual and the community (or communities) in which she is embedded, Sandel has written:

The hope for self-government today lies not in relocating sovereignty but in dispersing it. The most promising alternative to the sovereign state is not a cosmopolitan community based on the solidarity of humankind but a multiplicity of communities and political bodies--some more extensive than nations and some less--among which sovereignty is diffused. Only a politics that disperses sovereignty both upward [to transnational institutions] and downward can combine the power required to rival global market forces with the differentiation required of a public life that hopes to inspire the allegiance of its citizens. . . . If the nation cannot summon more than a minimal commonality, it is unlikely that the global community can do better, at least on its own. A more promising basis for a democratic politics that reaches beyond nations is a revitalized civic life nourished in the more particular communities we inhabit. In the age of NAFTA the politics of neighborhood matters more, not less [99].

Furthermore, the ease with which individuals can move between different rule sets in Cyberspace has important implications for any contractarian political philosophy deriving a justification of the State's exercise of coercive power over its citizens from their consent to the exercise of that power. In the nonvirtual world, this consent has a strong fictional element:

State reliance on consent inferred from someone merely remaining in the state is particularly unrealistic. An individual's unwillingness to incur the extraordinary costs of leaving his or her birthplace should not be treated as a consensual undertaking to obey state authority [100].

To be sure, citizens of France, dissatisfied with French law and preferring, say, Armenian rules, can try to persuade their compatriots and local decision-makers of the superiority of the Armenian rule-set [101]. However, their "exit" option, in Albert Hirschman's terms, is limited by the need to physically relocate to Armenia to take advantage of that rule set [102]. In contrast, in Cyberspace, any given user has a more accessible exit option, in terms of moving from one virtual environment's rule set to another's, thus providing a more legitimate "selection mechanism" by which differing rule sets will evolve over time [103].

The ability of inhabitants of Cyberspace to cross borders at will between legally significant territories, many times in a single day, is unsettling. This power seems to undercut the validity of developing distinct laws for online culture and commerce: How can these rules be "law" if participants can literally turn them on and off with a switch? Frequent online travel might subject relatively mobile human beings to a far larger number of rule sets than they would encounter traveling through the physical world over the same period. Established authorities, contemplating the rise of a new law applicable to online activities, might object that we cannot easily live in a world with too many different sources and types of law, particularly those made by private (non-governmental) parties, without breeding confusion and allowing anti-social actors to escape effective regulation.

But the speed with which we can cross legally meaningful borders or adopt and then shed legally significant roles should not reduce our willingness to recognize multiple rule sets. Rapid travel between spheres of being does not detract from the distinctiveness of the boundaries, as long as participants realize the rules are changing. Nor does it detract from the appropriateness of rules applying within any given place, any more than changing commercial or organizational roles in the physical world detracts from a person's ability to obey and distinguish rules as a member of many different institutional affiliations and to know which rules are appropriate for which roles [104]. Nor does it lower the enforceability of any given rule set within its appropriate boundaries, as long as groups can control unauthorized boundary crossing of groups or messages. Alternating between different legal identities many times during a day may confuse those for whom cyberspace remains an alien territory, but for those for whom cyberspace is a more natural habitat in which they spend increasing amounts of time it may become second nature. Legal systems must learn to accommodate a more mobile kind of legal person [105].

V1. Conclusion

Global electronic communications have created new spaces in which distinct rule sets will evolve. We can reconcile the new law created in this space with current territorially-based legal systems by treating it as a distinct doctrine, applicable to a clearly demarcated sphere, created primarily by legitimate, self-regulatory processes, and entitled to appropriate deference--but also subject to limitations when it oversteps its appropriate sphere.

The law of any given place must take into account the special characteristics of the space it regulates and the types of persons, places, and things found there. Just as a country's jurisprudence reflects its unique historical experience and culture, the law of Cyberspace will reflect its special character, which differs markedly from anything found in the physical world. For example, the law of the Net must deal with persons who "exist" in Cyberspace only in the form of an email address and whose purported identity may or may not accurately correspond to physical characteristics in the real world. In fact, an e-mail address might not even belong to a single person. Accordingly, if Cyberspace law is to recognize the nature of its "subjects," it cannot rest on the same doctrines that give geographically based sovereigns jurisdiction


over "whole," locatable, physical persons. The law of the Net must be prepared to deal with persons who manifest themselves only by means of a particular ID, user account, or domain name.

Moreover, if rights and duties attach to an account itself, rather than an underlying real world person, traditional concepts such as "equality," "discrimination," or even "rights and duties" may not work as we normally understand them. New angles on these ideas may develop. For example, when AOL users joined the Net in large numbers, other Cyberspace users often ridiculed them based on the ".aol" tag on their email addresses--a form of "domainism" that might be discouraged by new forms of Netiquette. If a doctrine of Cyberspace law accords rights to users, we will need to decide whether those rights adhere only to particular types of online appearances, as distinct from attaching to particular individuals in the real world.

Similarly, the types of "properties" that can become the subject of legal discussion in Cyberspace will differ from real world real estate or tangible objects. For example, in the real world the physical covers of a book delineate the boundaries of a "work" for purposes of copyright law [106]; those limits may disappear entirely when the same materials are part of a large electronic database. Thus, we may have to change the "fair use" doctrine in copyright law that previously depended on calculating what portion of the physical work was copied [107]. Similarly, a web page's "location" in Cyberspace may take on a value unrelated to the physical place where the disk holding that Web page resides, and efforts to regulate web pages by attempting to control physical objects may only cause the relevant bits to move from one place to another. On the other hand, the boundaries set by "URLs" (Uniform Resource Locators, the location of a document on the World Wide Web) may need special protection against confiscation or confusingly similar addresses. And, because these online "places" may contain offensive material, we may need rules requiring (or allowing) groups to post certain signs or markings at these places' outer borders.

The boundaries that separate persons and things behave differently in the virtual world but are nonetheless legally significant. Messages posted under one e-mail name will not affect the reputation of another e-mail address, even if the same physical person authors both messages. Materials separated by a password will be accessible to different sets of users, even if those materials physically exist on the very same hard drive. A user's claim to a right to a particular online identity or to redress when that identity's reputation suffers harm, may be valid even if that identity does not correspond exactly to that of any single person in the real world [108].

Clear boundaries make law possible, encouraging rapid differentiation between rule sets and defining the subjects of legal discussion. New abilities to travel or exchange information rapidly across old borders may change the legal frame of reference and require fundamental changes in legal institutions. Fundamental activities of lawmaking--accommodating conflicting claims, defining property rights, establishing rules to guide conduct, enforcing those rules, and resolving disputes--remain very much alive within the newly defined, intangible territory of Cyberspace. At the same time, the newly emerging law challenges the core idea of a current law-making authority--the territorial nation state, with substantial but legally restrained powers.

If the rules of Cyberspace thus emerge from consensually based rule sets, and the subjects of such laws remain free to move among many differing online spaces, then considering the actions of Cyberspace's system administrators as the exercise of a power akin to "sovereignty" may be inappropriate. Under a legal framework where the top level imposes physical order on those below it and depends for its continued effectiveness on the inability of its citizens to fight back or leave the territory, the legal and political doctrines we have evolved over the centuries are essential to constrain such power. In that situation, where exit is impossible, costly, or painful, then a right to a voice for the people is essential. But when the "persons" in question are not whole people, when their "property" is intangible and portable, and when all concerned may readily escape a jurisdiction they do not find empowering, the relationship between the "citizen" and the "state" changes radically. Law, defined as a thoughtful group conversation about core values, will persist. But it will not, could not, and should not be the same law as that applicable to physical, geographically-defined territories. 

Authors

David R. Johnson: Chairman of Counsel Connect and Co-Director of the Cyberspace Law Institute.

David Post: Visiting Associate Professor of Law, Georgetown University Law Center and Co-Director of the Cyberspace Law Institute.

Acknowledgements

The authors wish to thank Becky Burr, Larry Downes, Henry J. Perritt, Jr., and Ron Plessner, as well as the other Fellows of the Cyberspace Law Institute (Jerry Berman, John Brown, Bill Burrington, Esther Dyson, David Farber, Ken Freeling, A. Michael Fromkin, Robert Gellman, I. Trotter Hardy, Ethan Katsch, Lawrence Lessig, Bill Marmon, Lance Rose, Marc Rotenberg, Pamela Samuelson, and Eugene Volokh), and Jim Campbell, for their assistance in the formulation of these ideas. The usual disclaimer, of course, applies: the authors alone are responsible for errors, omissions, misstatements, and misunderstandings set forth in the following.

Notes

1. American Banana Co. v. United Fruit Co. 213 US 347, 357 (1909) (holding that as a general rule of construction, any statute is presumed to be intended to operate within the territorial limits of the sovereign).

2. See 1a Jerome Gilson, *Trademark Protection and Practice* Sect. 9.01 (1991); Dan L. Burk, *Trademarks Along the Infobahn: A First Look at the Emerging Law of Cybermarks*, 1 U. Rich. J.L. & Tech. 1 (1995), available at <http://www.urich.edu/~jolt/v1i1/burk.html>; Jeffrey M. Samuels & Linda B. Samuels, *The Changing Landscape of International Trademark Law*, 27 G.W. J. Int'l L. & Econ. 433 (1993-94).

3. *Dawn Donut Co. v. Hart's Food Stores, Inc.*, 267 F.2d 358 (2d. Cir. 1959) (holding that the owner of a registered trademark may not enjoin another's use of that mark in a geographically separate market if the holder of the registered mark does not intend to expand into that market).

4. See e.g., *California Fruit Growers Exchange v. Sunkist Baking Co.*, 166 F.2d 971 (7th Cir. 1947) (permitting "Sunkist" fruits and "Sunkist" bakery products); *Restaurant Lutece Inc., v. Houbigant, Inc.*, 593 F.Supp. 588 (D.N.J. 1984) (denying the restaurant "Lutece's" preliminary injunction against "Lutece" cosmetics).

5. Clark W. Lackert, *International Efforts Against Trademark Counterfeiting* Colum. Bus. L. Rev. 161 (1988); Samuels & Samuels, *supra* note 4, at 433.

6. Restatement (Third) of Foreign Relations Law of the United States Sect. 201 (1987) ("Under international law, a state is an entity that has a defined territory and a permanent population, under the control of its own government . . ."); *id.* Sect. 402 (a state has "jurisdiction to prescribe law with respect to (1)(a) conduct that, wholly or in substantial part, takes place within its territory; (b) the status of persons, or interests in things, present within its territory; (c) conduct outside its territory that has or is intended to have substantial effect within its territory; . . ."); see also Lea Brilmayer, *Consent, Contract, and Territory*, 74 Minn. L. Rev. 1, 11-12 (noting the significance of state authority derived from sovereignty over physical territory in the context of social contract theory).

7. The ability of the sovereign to claim personal jurisdiction over a particular party, for instance, turns importantly on the party's relationship to the physical jurisdiction over which the sovereign has control, e.g., the presence of the party or assets belonging to the party, within the jurisdiction, or activities of the party that are directed to persons or things within the jurisdiction. Similarly, the law chosen to apply to a contract, tort, or criminal action has historically been influenced primarily by the physical location of the parties or the deed in question. See generally, Henry H. Perritt Jr., *Jurisdiction in Cyberspace* (October 28, 1995) (unpublished manuscript on file with the Stanford Law Review). Perritt, *LAW AND THE INFORMATION SUPERHIGHWAY*, ch. 12 (Wiley, 1996).

8. Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations, G.A. Res. 2625, 35th Sess. (1970); Declaration of the Inadmissibility of Intervention into the Domestic Affairs of States, G.A. Res. 2131, 30th Sess. (1965). See also Brilmayer, *supra* note 7, at 6 (discussing contractarian theories of state sovereignty and legitimacy).

9. The exception proves this rule--we feel outrage when a journalist who crosses a territorial boundary without any signs is imprisoned for any supposed offense against the local state. Some "signposts" are culturally understood conventions that accompany entry into specialized places, such as courtrooms, office buildings, and churches. But not all signposts and boundaries dividing different rule sets are geographically or physically based. Sets of different rules may apply when the affected parties play particular roles, such as members of self-regulatory organizations, agents of corporate entities, and so forth. Henry H. Perritt Jr., *Self-governing Electronic Communities* 36-49, 59-60 (Apr. 1995) (on file with the Stanford Law Review). But even these roles are most often clearly marked by cues of dress, or formal signatures that give warning of the applicable rules. See text at notes [93](#) and [105](#).

10. As Woody Allen once quipped: "Space is nature's way of keeping everything from happening to you." Although there is distance in online space, it behaves differently from distance in real space. See generally, M. Ethan Katsh, *The Electronic Media and the Transformation of Law* 92-94 (1989); M. Ethan Katsh, *Law in a Digital World* 57-59, 218 (1995).

11. See Burk, *supra* note 4, at 12-14, for a general description of the Domain Naming System; see also Bush, Carpenter, & Postel, *Delegation of International Top Level Domains*, Internet-Draft ymbk-itld-admin-00, available at <http://www.internic.net>; RFC 882, *Domain Names--Concepts and Facilities*, available at <ftp://ds.internic.net/rfc/rfc882.txt>; RFC 883, *Domain Names--Implementation and Specifications*, available online at <ftp://ds.internic.net/rfc/rfc883.txt>

12. See, Jon Auerbach, *Fences in Cyberspace; Governments Move to Limit Free Flow of the Internet*, Boston Globe, Feb. 1, 1996, at 1 (surveying "digital Balkanization" of the Internet through government censorship and filtration); Seth Faison, *Chinese Cruise Internet, Wary of Watchdogs*, N.Y. Times Feb. 5, 1995, at A1; see also *infra*, note 20 (describing German government's attempts to interrupt German citizens' access to certain Usenet discussion groups; see generally Anne Wells Branscomb, *Jurisdictional Quandaries for Global Networks*, in *Global Networks: Computers and International Communication* 83, 103 (exploring efforts to exercise jurisdictional control over electronic information services).

13. Anthony Paul Miller, *Teleinformatics, Transborder Data Flows and the Emerging Struggle for Information: An Introduction to the Arrival of the New Information Age*, 20 Colum. J. L. & Soc. Probs. 89, 107-08, 127-32 (1986) (exploring the willingness of some national governments to forego the benefits of unregulated TDF's so as to protect their political, social, and cultural interests).

14. *Id.* at 105-07, 111-18 (suggesting that the data storage capabilities and anonymity of information technologies have prompted the Organization for Economic Cooperation and Development (OCED) and governments throughout Western Europe to restrict the content of TDF's so as to protect individual and corporate privacy).

15. *Id.* at 109-11 (noting the drive, particularly among computer software developers, to curb the threat that TDF's pose to intellectual property rights); see also Book Publishers Worry About Threat of Internet, *NY Times* (March 18, 1996) at A1 (describing appearance of *Le Grand Secret*, a book about former French President Francois Mitterrand, on the Internet despite its banning in France, and the general concern of book publishers about unauthorized Internet distributions).

16. For example, A. Jared Silverman, former chief of the New Jersey Bureau of Securities, expressed concern about the ability of the State to protect its residents against fraudulent schemes if it does not assert the right to regulate every online securities offering accessible, via the net, from within the State. Jared Silverman LEXIS Counsel Connect to [insert title], posted Law of the Electronic Road Seminar. See also Gregory Spears, *Cops and Robbers on the Net*, *Kiplinger's Pers. Fin. Mag.*, Feb. 1995, at 56 (surveying responses to online investment scams). Moreover, various state attorneys general have expressed concern about gambling and consumer fraud reaching their state's residents over the net. See note 21, *infra*.

17. The difficulty of policing an electronic border may have something to do with its relative length. See comment of Prof. Peter Martin, *NewJuris Electronic Conference* (Sept. 22, 1993) at p. 13 (discussing cyberspace's "near infinite boundary" with territorial jurisdictions). Physical roads and ports linking sovereign territories are few in number, and geographical boundaries can be fenced and policed. In contrast, the number of starting points for an electronic "trip" out of a given country is staggering, consisting of every telephone capable of connecting outside the territory. Even if electronic communications are concentrated into high volume connections, a customs house opened on an electronic border would cause a massive traffic jam, threatening the very electronic commerce such facilities were constructed to encourage.

18. Cf. Information Infrastructure Task Force, *Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights 221* (1995) ("White Paper") (discussing cross-border transmission of copies of copyrighted works):

Although we recognize that the U.S. Customs Service cannot, for all practical purposes, enforce a prohibition on importation by transmission, given the global dimensions of the information infrastructure of the future, it is important that copyright owners have the other remedies for infringements of this type available to them.

Id. Ironically, the Voice of America cannot prevent the information it places on the net from doubling back into the United States, even though this domestic dissemination violates the 1948 Smith-Mundt Act. John Schwartz, *Over the Net and Around the Law*, *Wash. Post*, Jan. 14, 1995, at C1.

19. See Walter B. Wriston, *The Twilight of Sovereignty* (1992) (examining the challenges to sovereignty posed by the information revolution):

Technology has made us a "global" community in the literal sense of the word Whether we are ready or not, mankind now has a completely integrated international financial and information marketplace capable of moving money and ideas to any place on this planet in minutes. Capital will go where it is wanted and stay where it is well treated. It will flee from manipulation or onerous regulation of its value or use, and no government power can restrain it for long.

Id. at 61-62. For example, the Securities and Exchange Commission has taken the position that securities offerings "that occur outside the United States" are not subject to the registration requirements of Section 5 of the Securities Act of 1933, even if United States residents are the purchasers in the overseas market. See SEC Rule 90; see also Rule 903 (in order for offers and sales to be deemed to "occur outside the United States," there must be, *inter alia*, "no directed selling efforts . . . made in the United States"); Rule 902(b)(1) (defining "directed selling efforts" as "any activity undertaken for the purpose of, or that could reasonably be expected to have the effect of, conditioning the market in the United States" for the securities in question). If, as many predict, trading on physical exchanges increasingly gives way to computerized trading over the Net, see, e.g., Therese H. Maynard, *What is an Exchange?: Proprietary Electronic Securities Trading Systems and the Statutory Definition of an Exchange*, 49 *WASH. & LEE L. REV.* 833, 362 (1992), Lewis D. Solomon and Louise Corso, *The Impact of Technology on the Trading of Securities*, 24 *JOHN MARSHALL L. REV.* 299, 318-319 (1991), this rule will inevitably become increasingly difficult to apply on a coherent basis; where, in such a market, does the offer "occur"? Can information about the offering placed on the World Wide Web "reasonably be expected to have the effect of conditioning the market in the United States" for the securities in question? See, generally, Solomon and Corso, *op. cit.*, at 330. [The authors wish to thank Prof. Merritt Fox, whose talk, entitled *The Political Economy of Statutory Reach: US Disclosure Rules for a Globalizing Market for Securities* (Georgetown University Law Center, March 6, 1996) drew our attention to these questions in this context].

20. For example, German authorities, seeking to prevent violations of that country's laws against distribution of pornographic material, ordered CompuServe to disable access by German residents to certain global Usenet newsgroups that would otherwise be accessible through that commercial service. See Karen Kaplan, *Germany Forces Online Service to Censor Internet*, *L.A. Times*, Dec. 29, 1995, at A1; *Why Free-Wheeling Internet Puts Teutonic Wall over Porn*, *Christian Sci. Monitor*, Jan 4, 1996, at 1; *Cyberporn Debate Goes International; Germany Pulls the Shade On*

CompuServe, Internet, Wash. Post, Jan. 1, 1996, at F13 (describing efforts by a local Bavarian police force had the effect of requiring CompuServe to temporarily cut off the availability of news groups to its entire audience (at least until a way to prevent delivery of specified groups to the German audience could be developed). Anyone inside Germany with an Internet connection could easily find a way to access the prohibited news groups during the ban. Auerbach, *supra* note 19, at 15. Although initially compliant, CompuServe subsequently rescinded the ban on most of the files by sending parents a new program to choose for themselves what items to restrict. CompuServe Ends Access Suspension: It reopens all but five adult-oriented newsgroups. Parents can now block offensive material, L.A. Times, Feb. 14, 1996, at D1.

Similarly, Tennessee may insist (indirectly, through enforcement of a federal law that defers to local community standards) that an electronic bulletin board in California install filters that prevent offensive screens from being displayed to users in Tennessee if it is to avoid liability under local obscenity standards in Tennessee. See *United States v. Thomas*, ___ F.3d ___, 1996 WL 30477 (6th Cir. 1996) (affirming the convictions of a California couple for violations of federal obscenity laws stemming from electronic bulletin board postings made by the couple in California but accessible from and offensive to the community standards of Tennessee). See generally Electronic Frontier Foundation, *A Virtual Amicus Brief in the Amateur Action Case*, (Aug. 11, 1995), available at http://www.eff.org/pub/Legal/Cases/AABBS_Thomas/Memphis/Old/aa_eff_vbrief.html. The bulletin board in this case had very clear warnings and password protection. This intangible boundary limited entrance to only those who voluntarily desired to see the materials and accepted the system operator's rules. It is our contention that posting offensive materials in areas where unwilling readers may come across them inadvertently raises different problems that are better dealt with by those who understand the technology involved rather than by extrapolating from the conflicting laws of multiple geographic jurisdictions. See text accompanying notes 64-67 *supra*.

21. The Minnesota Attorney General's Office distributed a "Warning to All Internet Users and Providers," (available at <http://www.state.mn.us/ebranch/ag/memo.txt>), stating that "[p]ersons outside of Minnesota who transmit information via the Internet knowing that information will be disseminated in Minnesota are subject to jurisdiction in Minnesota courts for violations of state criminal and civil laws". *Id.* (emphasis omitted). The conclusion rested on the Minnesota general criminal jurisdiction statute, which provides that "a person may be convicted and sentenced under the law of this State if the person... (3) Being without the state, intentionally causes a result within the state prohibited by the criminal laws of this State." Minn. Stat. Ann. Sect. 609.025 (West 1987). Minnesota also began civil proceedings against Wagernet, a Nevada gambling business which posted an Internet advertisement for online gambling services. See *Complaint, Minnesota v. Granite Gate Resorts, Inc.* (1995) (No. 9507227), available at <http://www.state.mn.us/ebranch/ag/gqcom.txt>. The Florida Attorney General, by contrast, contends that it is illegal to use the Web to gamble from within Florida but concedes that the Attorney General's office should not waste time trying to enforce the unenforceable. 95-70 Op. Fla. Att'y Gen. (1995), available at <http://legal.firn.edu/units/opinions/95-70.html>. For a general discussion of these pronouncements, see Mark Eckenwiler, *States Get Entangled in the Web*, *Legal Times*, Jan. 22, 1996, at S35.

22. See *State Regulators Crack Down on "Information Highway" Scams*, *Daily Rep. For Exec. (BNA)*, July 1, 1994, available in Westlaw, BNA-DER database, 1994 DER 125 at d16.

23. See David G. Post, *The State of Nature and the First Internet War*, *REASON* Apr. 1996, at 30-31 (describing the operation of the alt.religion.scientology Usenet group, noting that

"Usenet groups like alt.religion.scientology come into existence when someone . . . sends a proposal to establish the group to the specific newsgroup (named "alt.config") set up for receiving such proposals. The operators of each of the thousands of computer networks hooked up to the Internet are then free to carry, or to ignore, the proposed group. If a network chooses to carry the newsgroup, its computers will be instructed to make the alt.religion.scientology "feed," i.e., the stream of messages posted to alt.religion.scientology arriving from other participating networks, accessible to its users, who can read -- and, if they wish, add to -- this stream before it is passed along to the next network in the worldwide chain. It's a completely decentralized organism -- in technical terms, a distributed database' -- whose content is constantly changing as it moves silently around the globe from network to network and machine to machine, never settling down in any one legal jurisdiction, or on any one computer."). See, generally, *What is Usenet? and Answers to Frequently Asked Questions about Usenet*, available at <http://www.smartpages.com/bngfaqs/news/announce/newusers/top.html>.

24. European countries are trying to protect data regarding their citizens by banning the export of information for processing in countries that do not afford sufficient protections. See Peter Blume, *An EEC Policy for Data Protection*, 11 *Computer/Law Jour.* 399 (1992); Joseph I. Rosenbaum, *The European Commission's Draft Directive on Data Protection*, 33 *Jurimetrics* 1 (1992); Symposium, *Data Protection and the European Union's Directive*, 80 *Iowa L. Rev.* 431 (1995). But the data regarding their citizens' activities may not be subject to their control--it may originate as a result of actions recorded on servers outside their boundaries.

25. See Joel R. Reidenberg, *The Privacy Obstacle Course: Hurdling Barriers to Transnational Financial Services*, 60 *Fordham L. Rev.* S137 (1992); David Post, *Hansel & Gretel in Cyberspace*, *Am. Law. Oct.* 1995, at 110.

26. Privacy, at least, is a relatively familiar concept, susceptible of definition on the Net by reference to analogies with

mail systems, telephone calls and print publication of invasive materials. But many new issues posed by phenomena unique to the Net are not even so familiar. Because electronic communications are not necessarily tied to real world identities, new questions about the rights to continued existence, or to protection of the reputation, of a pseudonym arise. The potential to launch a computer virus or to "spam the net" by sending multiple offpoint messages to newsgroups, for example, creates a need to define rules governing online behavior. When large numbers of people collaborate across the net to create services or works of value, we will face the question whether they have formed a corporate entity or partnership--with rights and duties of its own that are distinct from those of the individual participants--in a context in which there may have been no "registration" with any particular geographic authority and the rights of any such authority to regulate that new "legal person" remain unsettled.

27. See note 11 supra.

28. Conflicts between domain names and registered trademarks have caused Network Solutions, Inc. (NSI), the agent for registration of domain names in the United States, to require that registrants "represent and warrant" that they have the right to a requested domain name and promise to "defend, indemnify and hold harmless" NSI for any claims stemming from use or registration of the requested name. See Network Solution Inc., NSI Domain Name Dispute Policy Statement (Revision 01, effective November 23, 1995), available at <ftp://rs.internic.net/policy/internic/internic-domain-4.txt>. For a useful overview of the domain name registration system and of the tensions between trademark rights and domain names, see Gary W. Hamilton, Trademarks on the Internet: Confusion, Collusion or Dilution?, 4 Tex. Intell. Prop. L.J. 1 (1995). See also Proceedings of the NSF/DNCEI & Harvard Information Infrastructure Project, Internet Names, Numbers, and Beyond: Issues in the Coordination, Privatization, and Internationalization of the Internet, Nov. 20, 1995, available at <http://ksgwww.harvard.edu/iip/nsfmin1.html> (discussing protection of the "trademark community" on the Net).

29. David R. Johnson, The Internet vs. the Local Character of the Law: The Electronic Web Ties Iowa and New York into One Big System, Legal Times, Dec. 5, 1994, at S32 (predicting the transformation of "local" regulation on the Net).

30. Cf. David R. Johnson, Traveling in Cyberspace, Legal Times, Apr. 3, 1995, at 26.

31. Indeed, the persistence and accessibility of electronic messages create such a sense of "placeness" that meetings in Cyberspace may become a viable alternative to meetings in physical space. See I. Trotter Hardy, Electronic Conferences: The Report of an Experiment, 6 Harv. J. Law & Tech. 213, 232-34 (1993) (discussing the advantages of e-mail conferences). In contrast, there is no "Telespace" because the conversations we conduct by telephone disappear when the parties hang up. Voicemail creates an aural version of electronic mail, but it is not part of an interconnected system that you can travel through, by hypertext links or otherwise, to a range of public and semi-public locations.

32. Some information products combine a local CD-ROM with online access to provide updated information. But even these products typically provide some on-screen indication when the user is going online. Failure to provide notice might well be deemed fraudulent, particularly if additional charges for use of the online system were imposed. In any event, a product that brings information to the screen, from an online location, without disclosing the online connection to the user, should not be characterized as having allowed the user to visit a legally significant user visit to online space. "Visiting" a space implies some knowledge that you are there.

33. See [Internal Diversity](#), differentiation among rule-sets in different online areas).

34. See infra note 98.

35. Having a noticeable border may be a prerequisite to the establishment of any legal regime that can claim to be separate from pre-existing regimes. If someone acting in any given space has no warning that the rules have changed, the legitimacy of any attempt to enforce a distinctive system of law is fatally weakened. No geographically based sovereign could plausibly claim to have jurisdiction over a territory with secret boundaries. And no self-regulatory organization could assert its prerogatives while making it hard for members and nonmembers to tell each other apart or disguising when they were (or were not) playing their membership-related roles.

36. For example, we will have to take into account the desire of participants in online communications for pseudonymity. This will affect the extent to which information about the applicant's identity must be disclosed in order to obtain a valid address registration. See David G. Post, Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace, UNIV. CHIC. LEGAL FORUM (forthcoming), available at <http://www-law.lib.uchicago.edu/forum/> (discussing the value of pseudonymous communications); A. Michael Froomkin, Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases (Dec. 4, 1995) (unpublished manuscript, on file with the Stanford Law Review) (exploring the use and possible regulation of computer-aided anonymity) available at <http://www.law.miami.edu/~froomkin>; A. Michael Froomkin, Anonymity and Its Enmities, 1995 J. of Online Law art. 4 available at <http://www.law.cornell.edu/jol/jol.table.html> (discussing the mechanics of anonymity and how it affects the creation of pseudonymous personalities and communication on the Net). And any registration and conflict-resolution scheme will have to take into account the particular ways in which Internet addresses and names are viewed in the marketplace. If shorter names are valued more highly (jones.com being more valuable than jones@isp.members.directory.com), this new form of "domain envy" will have to be considered in developing applicable policy.

37. See, e.g., Henry H. Perritt, Jr., Tort Liability, the First Amendment, and Equal Access to Electronic Networks, 5 Harv. J. Law & Tech., Spring 1992, at 65, 106-08 (assessing the applicability of the tort of libel to network users and operators); Michael Smyth and Nick Braithwaite, First U.K. Bulletin Board Defamation Suit Brought, National Law Journal, Sept. 19, 1994, at C10 (noting that English courts may be a more attractive forum for plaintiffs charging defamation in cyberspace).

38. Subsequent distribution of printed versions might be characterized as publication, without undermining the benefits of applying this new doctrine, because it is much easier to determine who has taken such action and where (in physical space) it occurred, and the party who engages in physical distribution of defamatory works has much clearer warning regarding the nature of the act and the applicability of the laws of a particular territorial state.

39. Edward A. Cavazos, Computer Bulletin Board Systems and the Right of Reply: Redefining Defamation Liability for a New Technology, 12 Rev. Lit. 231, 243-47 (1992). This "right of reply" doctrine might apply differently to different areas of the Net, depending on whether these areas do in fact offer a meaningful opportunity to respond to defamatory messages.

40. In the context of "telemedicine", early efforts to avoid this result seem to take the form of allowing doctors to interact with other doctors in consultations, requiring compliance with local regulations only when the doctor deals directly with a patient. See Howard J. Young and Robert J. Waters, Arent Fox Kitner Plotkin & Kahn, Licensure Barriers to the Interstate Use of Telemedicine, (1995) available at <http://www.arentfox.com/newslett/tele1b.htm>. The regulation of lawyers is muddled: Regulations are sometimes based on where the lawyer's office is (as in the case of Texas' regulation of advertising), sometimes based on the content of legal advice, and sometimes based on the nature and location of the client. See Katsh, Law in a Digital World, supra note 11, at 178-181.

41. Indeed, practicing the "law of the Net" itself presumably requires qualifications unrelated to those imposed by local bars.

42. In this, as in other matters, it is critical to distinguish the different layers of the "protocol stack." It may be possible to establish power with regard to physical connections. It is much harder to do so with respect to the logical connections that exist at the "applications" layer.

43. Jane C. Ginsburg, Global Use/Territorial Rights: Private International Law questions of the Global Information Infrastructure, J. COPY. SOC. 318, 319-320 (1995).

44. See, generally, Friedman, Standards as Intellectual Property, 19 U. DAYTON L.REV. 1109 (1994); William Landes & Richard Posner, An Economic Analysis of Copyright Law, 18 J. LEG. STUD 325 (1989).

45. For example, the creative output of lawyers and law professors -- law review articles, briefs and other pleadings, and the like -- may well be determined largely by factors completely unrelated to the availability or unavailability of copyright protection for those works, because that category of authors, generally speaking, obtains reputational benefits from wide dissemination that far outweigh the benefits that could be obtained from licensing individual copies. See Stephen Breyer, The Uneasy Case for Copyright: A Study of Copyright in Books, Photocopies, and Computer Programs, 84 HARV. L. REV. 281, 293-309 (1970) for an analysis of the incentive structure in the scholarly publishing market; see also Tuckman & Leahey, What is an Article Worth?, 83 J. POL. ECON. 951 (1975).

46. There is a large and diverse literature on the new kinds of authorship that are likely to emerge in cyberspace as a function of the interactive nature of the medium, the ease with which digital information can be manipulated, and new searching and linking capabilities. Among the more insightful pieces in this vein are Samuelson, Digital Media and the Changing Face of Intellectual Property Law, 16 RUTGERS COMP. AND TECH. L. J. 323 (1990); Katsh, Law in a Digital Age (1994), chaps. 4, 8, and 9; Volokh, Cheap Speech, 94 YALE. L. J. 1805 (1994); and Turkle, The Second Self: Computers and the Human Spirit (1984).

47. [Netscape Communications Corp.](http://www.netscape.com) gave away, at no charge, over 4 million copies of their Web browser; it is estimated that they now control over 70% of the Web browser market, which they have managed to leverage into dominance in the Web server software market, sufficient to enable them to launch one of the most successful Initial Public Offerings in the history of the United States. See Netscape IPO booted up; Debut of hot stock stuns Wall Street veterans, The Boston Globe, August 10, 1995, at 37; With Internet Cachet, Not Profit, A New Stock Is Wall St.'s Darling, NY Times, August 10, 1995, at 1. Other companies are following Netscape's lead; for example, Realaudio, Inc. is distributing software designed to allow Web browsers to play sound files in real time over the Internet, presumably in the hopes of similarly establishing a dominant market position in the server market. See <http://www.realaudio.com>

48. Esther Dyson, Intellectual Value, WIRED (August 1995).

49. David G. Post, Who Owns the Copy Right? Opportunities and Opportunism on the Global Network 2-3 (Oct. 29, 1995) (unpublished manuscript on file with the Stanford Law Review).

50. See Jane C. Ginsburg, Putting Cars on the Information Superhighway: Authors, Exploiters, and Copyright in cyberspace, 95 Colum. L. Rev. 1466, 1488 (1995) (concluding that authors enjoy rights whose effective enforcement in cyberspace is today rather uncertain); David G. Post, New Wine, Old Bottles: The Evanescent Copy, Am. Law., May

1995, at 103.

51. See David G. Post, *White Paper Blues: Copyright and the National Information Infrastructure*, LEGAL TIMES (Apr. 8, 1996) at [] ("For example, browsing' on the World Wide Web necessarily involves the creation of numerous copies' of information; first, a message is transmitted from Computer A to (remote) Computer B, requesting that Computer B send a copy of a particular file (e.g., the "home page" stored on Computer B) back to Computer A. When the request is received by Computer B, a copy of the requested file is made and transmitted back to Computer A (where it is copied again -- loaded' into memory -- and displayed). And the manner in which messages travel across the Internet to reach their intended recipient(s) -- via intermediary computers known as "routers," at each of which the message is read' by means of 'copying' the message into the computer's memory -- [involve] . . . innumerable separate acts of . . . reproduction'. File copying is not merely inexpensive in cyberspace, it is ubiquitous; and it is not merely ubiquitous, it is indispensable . . . Were you to equip your computer with a copy lock' -- an imaginary device that will prevent the reproduction of any and all information now stored in the computer in any form -- it will, essentially, stop functioning.")

52. See Jessica Litman, *The Exclusive Right to Read*, 13 CARDOZO ARTS & ENT. L.J. 29, 40-42 (noting that under a view that "one reproduces a work every time one reads it into a computer's random access memory . . . any act of reading or viewing [a digital] work would require the use of a computer and would, under this interpretation, involve an actionable reproduction"); Pamela Samuelson, *The Copyright Grab*, WIRED Jan. 1996 at 137 (same); Pamela Samuelson, *Legally Speaking: Intellectual Property Rights and the Global Information Economy*, 39 Commun. Assoc. Comp. Machinery 23, 24 (1996) (browsing of digital works potentially infringing if "temporary copying that must occur in a computer's memory to enable users to read documents" is considered "reproduction" within meaning of Copyright Act); Post, supra note 45, at 103-04 ("If the very act of getting a document to your screen is considered the making of a copy' within the meaning of the Copyright Act, then a high proportion of the millions of messages traveling over the Internet each day potentially infringes on the right of some file creator . . . to control the making of copies. And, if the very act reading such documents on line involves copying, then some form of a license . . . would, in this view, be required for virtually every one of those message transmissions").

53. Neel Chatterjee, *Imperishable Intellectual Creations: Use Limits of the First Sale Doctrine*, 5 Fordham Intell. Prop. Media & Ent. L.J. 383, 384, 415-18 (1995) (discussing Information Infrastructure Task Force proposal to exclude transmissions from the first sale doctrine).

54. See, e.g., *Telerate Systems, Inc. v. Cars*, 689 F.Supp. 221, 229 (S.D.N.Y. 1988) (finding that copying a "few pages" of a 20,000 page database was substantial enough to weigh against fair use).

55. Benjamin Wittes, *A (Nearly) Lawless Frontier: The Rapid Pace of Change in 1994 Left the Law Chasing Technology on the Information Superhighway*, Am. Law., Jan. 3, 1995, at 1.

56. For example, we could adopt rules that make the "caching" of web pages presumptively permissible, absent an explicit agreement, rather than adopting the standard copyright doctrine to the contrary (Caching involves copying Web pages to a hard drive so that future trips to the site take less time to complete). Because making "cached" copies in computer memory is essential to speed up the operation of the Web, and because respecting express limits or retractions on any implied license allowing caching would clog up the free flow of information, we should adopt a rule favoring browsing. See Cyberspace Law Institute, *Caching and Copyright Protections* (Sept. 1, 1995), available at <http://www.il.georgetown.edu:80/lc/cli.html>; Post, supra note 44b (proposing a new rule for caching Web pages); Samuelson, supra note 45b, at 26-27 (discussing copyright issues raised by file caching).

57. See text accompanying note 11 supra for an explanations of the domain name system.

58. This danger of confusion exists whether the name conflicts with "real world" trademark uses or only other online uses. To be sure, whoever decides these questions must consider the views of geographically based authorities when online names interfere with the existing trademarks of physical goods. But they must also decide ownership questions about online identities with addresses, names, and logos having no application offline. The views of territorially based authorities would appear to have less bearing in this context.

59. Domain name space may raise the question whether the Net should develop an online equivalent of eminent domain. Newly discovered public needs, such as to use a particular domain or to eliminate it to establish a new system, could interfere with "investment backed expectations." To keep geographically based trademark authorities at bay, Net authorities may need to "grandfather" in strong global trademarks and prevent those who acquired certain domain names on a "first-come, first-served" basis from engaging in holdups--a responsible "foreign policy" to ward off overregulation by local sovereigns. The impact on individuals of these efforts to pursue the greater good may be require mandatory compensation. Who will pay and how remains unclear.

60. See David G. Post, *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace*, 1995 J. Online L. art. 3, 10 available at <http://www.law.cornell.edu/jol/jol.table.html>.

61. A. M. Rutkowski, *Internet Names, Numbers and Beyond: Issues in the Coordination, Privatization, and Internationalization of the Internet*, (Nov. 20, 1995) (on file with the Stanford Law Review) (identifying issues associated

with the administration of Internet names and numbers).

62. David W. Maher, Trademarks on the Internet: Who's in Charge?, (Feb. 14, 1996) available at <http://www.aldea.com/cix/maher.html> (arguing that trademark owners have a stake in the Net that must be taken into account).

63. See text accompanying note 86 infra regarding recent claims by the U.S. Government.

64. Typical rules also require refraining from actions that threaten the value of the online space or increase the risk that the system operator will face legal trouble in the real world. Many coherent on line communities also have rules preserving the special character of their online spaces, rules governing posted messages, discouraging "flaming" (sending an insulting message) or "spamming" (sending the same message to multiple newsgroups), and even rules mandating certain professional qualifications for participants.

65. See Robert L. Dunne, Deterring Unauthorized Access to Computers: Controlling Behavior in Cyberspace Through a Contract Law Paradigm, 35 Jurimetrics J. 1, 12 (1994) (suggesting that system operator agreements to banish offenders would deter unauthorized computer access more effectively than current criminal sanctions).

66. See John Seabrook, My First Flame, New Yorker, June 6, 1994, at 70 (describing the online phenomenon of flaming, where a user loses "self control and write[s] a message that uses derogatory, obscene, or inappropriate language").

67. A computer user "shuns" another by refusing to receive messages from that person (or, more generally, by employing a software program known as a "kill file" to automatically deflect any e-mail messages from a specified address).

68. Computer users "mailbomb" a victim by sending a large number of junk electronic mail messages with the goal of overloading the receiving computer, or at least inconveniencing the receiver.

69. Jennifer Mnookin, Virtual(ly) Law: A Case Study of the Emergence of Law on LambdaMOO (May 15, 1995) (unpublished manuscript on file with the Stanford Law Review) (describing the emergence of a legal system in the LambdaMOO virtual community).

70. Joanne Goode and Maggie Johnson, Putting Out the Flames: The Etiquette and Law of E-Mail, ONLINE, Nov. 1991, at 61 (suggesting guidelines for using electronic mail and networking; S. Hambridge, Request For Comments: 1855, Netiquette Guidelines, (Oct. 1995) available at <ftp://ds.internic.net/rfc/rfc1855.txt>).

71. James Barron, It's Time to Mind your E-Manners, N.Y. Times, Jan. 11, 1995, at C1.

72. See Henry H. Perritt, Jr., Dispute Resolution in Electronic Network Communities, 38 VILL. L. REV. 349, 398-99 (1993) (proposing an alternative dispute resolution mechanism that could be implemented by a computer network service provider); Henry H. Perritt, Jr., President Clinton's National Information Infrastructure Initiative: Community Regained?, 69 Chi.-Kent L. Rev. 991, 995-1022 (1994) (advocating the use of new information technology to facilitate dispute resolution); I. Trotter Hardy, The Proper Legal Regime for "Cyberspace", 55 U. Pitt. L.Rev. 993, 1051-1053. One such dispute resolution service, the "Virtual Magistrate," has already arisen on the Net. ee <http://vmag.law.vill.edu:8080/>.

73. See Hardy, supra note 60, at 1020 (Law Merchant was "simply an enforceable set of customary practices that inured to the benefit of merchants, and that was reasonably uniform across all the jurisdictions involved in the [medieval] trade fairs"); Leon E. Trakman, the Law Merchant: The Evolution of Commercial Law 11-12 (1983) (Law Merchant was "a system of law that did . . . not rest exclusively on the institutions and local customs of any particular country, but consisted of certain principles of equity and usages of trade which general convenience and a common sense of justice have established to regulate the dealings of merchants and mariners in all the commercial countries of the civilized world"). Benson describes the development of the Law Merchant as follows:

"With the fall of the Roman Empire, commercial activities in Europe were almost nonexistent relative to what had occurred before and what would come after. Things began to change in the eleventh and twelfth centuries [with the] emergence of a class of professional merchants. There were significant barriers to overcome before substantial interregional and inter-national trade could develop, however. Merchants spoke different languages and had different cultural backgrounds. Beyond that, geographic distances frequently prevented direct communication, let alone the building of strong interpersonal bonds that would facilitate trust. Numerous middlemen were often required to bring about an exchange All of this, in the face of localized, often contradictory laws and business practices, produced hostility towards foreign commercial customs and led to mercantile confrontations. There was a clear need for Law as a language of interaction'."

Bruce L. Benson, The Spontaneous Evolution of Commercial Law, 55 Southern Econ. J. 644, 646-47 (1989). See also Perritt, supra note 10, at 46-49.

74. See Benson, supra note 62a, at 647 ("[D]uring this period, because of the need for uniform laws of commerce to facilitate international trade, . . . the basic concepts and institutions of modern Western mercantile law--lex

mercatoria--were formed, and, even more important, it was then that mercantile law in the West first came to be viewed as an integrated, developing system, a body of law'. Virtually every aspect of commercial transactions in all of Europe (and in cases even outside Europe) were governed' by this body of law after the eleventh century. . . . This body of law was voluntarily produced, voluntarily adjudicated and voluntarily enforced. In fact, it had to be. There was no other potential source of such law, including state coercion.").

75. See Perritt, *supra* note 10, at 49; Hardy, *supra* note 62a, at 1019 ("The parallels [between the development of the Law Merchant and] cyberspace are strong. Many people interact frequently over networks, but not always with the same people each time so that advance contractual relations are not always practical. Commercial transactions will more and more take place in cyberspace, and more and more those transactions will cross national boundaries and implicate different bodies of law. Speedy resolution of disputes will be as desirable as it was in the Middle Ages! The means of an informal court system are in place in the form of on-line discussion groups and electronic mail. A 'Law Cyberspace' co-existing with existing laws would be an eminently practical and efficient way of handling commerce in the networked world"); Post, *supra* note 50a, at par. 43 and n. 15.

76. This enforcement tool is not perfect -- any more than the tool of banishing merchants from the medieval trade fairs was perfect for the development of the Law Merchant. See Paul R. Milgrom, Douglass C. North, and Barry R. Weingast, *The Role of Institutions in the Revival of Trade: The Law Merchant, Private Judges, and the Champagne Fairs*, 2 *Econ. & Pol.* 1 (1990) (describing the use of banishment and other enforcement mechanisms prior to the rise of the state). Individuals intent on wrongdoing may be able to sneak back on the Net or into a particular online area with a new identity. But the enforcement tools used by legal authorities in the real world also have limits. We do not refrain from recognizing the sovereignty of our territorial governments just because they cannot fully control their physical borders or all of the actions of their citizens.

77. The social philosopher Michael Sandel has made a similar point in writing of the need for new transnational law-making institutions if the "loss of mastery and the erosion of community that lie at the heart of democracy's discontent" is to be alleviated:

"In a world where capital and goods, information and images, pollution and people, flow across national boundaries with unprecedented ease, politics must assume transnational, even global, forms, if only to keep up. Otherwise, economic power will go unchecked by democratically sanctioned political power. . . . We cannot hope to govern the global economy without transnational political institutions"

Michael Sandel, *America's Search for a New Public Philosophy*, *ATLANTIC MONTHLY* March 1996 at 72-73 (emphasis added). See also *infra*, text at note 75a, for additional parallels between our arguments and Sandel's.

78. *Hilton v. Guyot*, 115 U.S. 113, 163-64 (1995). See also *Lauritzen v. Larsen*, 345 U.S. 571, 582 (1953) ("International or maritime law . . . aims at stability and order through usages which considerations of comity, reciprocity and long-range interest have developed to define the domain which each nation will claim as its own."); *Mitsubishi Motors v. Soler Chrysler-Plymouth*, 473 U.S. 614 (1985); see also *The Bremen v. Zapata Off-Shore Co.*, 407 U.S. 1 (1972). Good general treatments of the comity doctrine can be found in Swanson, *Comity, International Dispute Resolution Agreements, and the Supreme Court*, 21 *LAW & POLICY IN INT'L BUS.* 333 (1990); Paul, *Comity in International Law*, 32 *HARV. INT. L.J.* 1 (1991); Yntema, *The Comity Doctrine*, 65 *MICH. L. REV.* 9 (1966); James S. Campbell, *NEW LAW FOR NEW INTERNATIONAL TRADE* 5 (Dec. 3, 1993) (on file with the Stanford Law Review); Janis, *AN INTRODUCTION TO INTERNATIONAL LAW* 250 ff. (1988); Brilmayer, *CONFLICT OF LAWS: FOUNDATIONS AND FUTURE DIRECTIONS* 145-90 (1991).

79. *Restatement (Third) of Foreign Relations Law of the United States* Sect. 403(1) (1987).

80. *Id.*, at Sect. 403(3).

81. Maier, *Remarks*, 84 *PROC. AM. SOC. INT'L LAW* 339, 339 (1990); *id.*, at 340 (principle of comity informs the "interest-balancing" choice of law principles in the Restatement); Paul, *supra* note 63a, at 12 (comity arose out of "[t]he need for a more sophisticated system of conflicts . . . in connection with the emergence of the nation state and the rise of commerce that brought different nationalities into more frequent contact and conflict with one another"); *id.*, at 45-48 (noting that although the relationship between the "classical doctrine of comity" and the Restatement's principle of "reasonableness" is uncertain, the former "retains a significant function in the Restatement"); *id.*, at 54 (comity principle "mitigates the inherent tension between principles of territorial exclusivity and sovereign equality"); Cf. Campbell, *supra* note 63A, at 6 (The Supreme Court's comity jurisprudence "inquires, in cases involving international trade, what values facilitate that trade. Trading nations have a common interest in supporting these values, and therefore national agencies--courts, legislators, administrators--should seek to respect, and thereby strengthen, these values as they engage in the processes of law formation").

67 Perritt, *supra* note 10, at 1-2, 36-49.

82. Cf. Gopnik, *The Virtual Bishop*, *NEW YORKER* March 18, 1996 at 63 ("Of course, the primitive Church was a kind of Internet itself, which was one of the reasons it was so difficult for the Roman Empire to combat it. The early Christians

understood that what was most important was not to claim physical power in a physical place but to establish a network of believers--to be on line," quoting French Bishop Jacques Gaillot).

83. Perritt, *supra* note 10, at 42. Cf. Michael Walzer, *Spheres of Justice: A Defense of Pluralism and Equality* 281-83 (1983) (discussing differences between different spheres of power and authority).

84. The idea of "delegation" is something of a fiction. But legal fictions have a way of becoming persuasive and, therefore, real. See, e.g., Lon L. Fuller, *Legal Fictions*, 55 (1967). Self-regulatory bodies evolve independently of the State and derive their authority from the sovereign only insofar as the sovereign, after the fact, claims and exercises a monopoly over the use of force.

85. See generally, Henry H. Perritt, Jr., *Computer Crimes and Torts in the Global Information Infrastructure: Intermediaries and Jurisdiction* (Oct. 12, 1995) (on file with the Stanford Law Review).

86. See Maher, *supra* note 62 (noting the "arrogance" of the Federal Networking Council's position on this issue).

87. Cf. *id.* (noting that while other groups faced fees for new domain names, "[s]pecial arrangements are made for users of '.gov' and '.edu.'")

88. See *id.* (noting "[t]he .mil domain is excluded" from the jurisdiction of the private corporation that administers the registration of domain names).

89. See *supra*, note 20.

90. See *id.*

91. See Jonathan Graubert, *What's News: A Progressive Framework for Evaluating the International Debate Over the News*, 77 Cal. L. Rev. 629, 633 (1989) ("The guiding principle in international communications since World War II has been the U.S.-inspired goal of a free flow of information.' According to this principle, [f]reedom of information implies the right to gather, transmit and publish news anywhere and everywhere without fetters.") (citing G.A. Res. 59 (I), 1(2), U.N. GAOR Resolutions at 95, U.N. Doc. A/64/Add. 1 (1947). The free-flow-of-information principle has been defined as a necessary part of freedom of opinion and expression. See Article 19 of the Universal Declaration of Human Rights, G.A. Res. 217(III)A, 3(1) U.N. GAOR Resolutions at 71, 74-75, U.N. Doc. A/810 (1948) (stating that freedom of expression includes "freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers").

92. Moreover, the right of individuals to participate in various online realms depends critically on their obtaining information about those realms. Insofar as any territorial government merely claims moral superiority of its laws and values, it is not well situated to oppose a free flow of information that might lead its citizens to disagree, for this would be the equivalent of defending ignorance as a necessary ingredient of preservation of the values espoused by the local state. This view is unlikely to persuade external rulemakers who do not share those values.

93. Listservers, for example, can be set up on any network (or Internet) server by means of simple instructions given to one of several widely-available software programs (listproc or majordomo). A Usenet discussion group in the "alt." hierarchy can be established by sending a simple request to the "alt.config" newsgroup. See sources cited *supra*, note 23.

Cyberspace not only permits the effective delineation of internal boundaries between different online spaces, but it also allows for effective delineation of distinct online roles within different spheres of activity and as to which different rules apply. In the nonvirtual world, we slip in and out of such roles frequently; the rules applicable to the behavior of a single individual, in a single territorial jurisdiction, may change as he moves between different legally-significant persona (acting as an employee, a member of a church, a parent, or the officer of a corporation, for example). Cyberspace may make the boundaries between these different roles easier to maintain, insofar as explicit "tags" -- distinct "signature files," or screen names-- can relatively easily be attached to messages originating from the author's different roles.

94. Post, *supra* note 50a, art. 3, at par. 7 (asserting that the individual network "organizations" will probably determine the substantive rule-making for Cyberspace); David R. Johnson and Kevin A. Marks, *Mapping Electronic Data Communications onto Existing Legal Metaphors: Should We Let Our Conscience (and Our Contracts) Be Our Guide?*, 38 Vill. L.Rev. 487, 489-89 (1993) (explaining that communication service providers, owners of disks carrying centralized databases, and people presiding over electronic discussion groups have the power to select applicable rules).

95. For illuminating discussions of the many parallels between biological evolution and social evolution in Cyberspace, see Kevin Kelly, *Out of Control: The Law of Neo-Biological Civilization* (1994); John Lienhard, *Reflections on Information, Biology, and Community*, 32 Hous. L. Rev. 303 (1995); Michael Schrage, *Revolutionary Evolutionist*, *Wired* (July 1995).

96. This geographic barrier merely permits divergence to occur; it does not guarantee it. Specification will only occur, for example, if the two divided subpopulations are subject to different selection pressures or at least one of them is small enough to accrue significant random changes in its gene pool ("genetic drift"). For good, non-technical descriptions of evolutionary theory, see Daniel C. Dennett, *Darwin's Dangerous Idea: Evolution and the Meanings of Life* (1995); John

Maynard-Smith, *Did Darwin Get it Right? Essays on Games, Sex, and Evolution* (1989); John Maynard-Smith, *On Evolution* (1972); George C. Williams, *Adaptation and Natural Selection: A Critique of Some Current Evolutionary Thought* (1966).

97. To survive, rules must be passed on somehow, whether in the form of "case reports" or other inter-individual or inter-generational methods. See Richard Dawkins, *The Selfish Gene* (1989). General parallels between biological evolution and the evolution of legal rules are discussed in FRIEDRICH HAYEK, 1 *LAW, LEGISLATION, AND LIBERTY* at 44-49 (1973); FRIEDRICH HAYEK, *THE CONSTITUTION OF LIBERTY*, 56-61 (1960); see generally Tom W. Bell, *Polycentric Law*, 7 *Humane Studies Rev.* [] (available at <http://osf1.gmu.edu/~ihs/w91issues.html>).

98. Cyberspace, as M. Ethan Katsh has written, is a "software world" where "code is the Law." M. Ethan Katsh, *Software Worlds and the First Amendment: Virtual Doorkeepers in Cyberspace*, UNIV. OF CHIC. LEGAL FORUM (forthcoming), quoting WILLIAM MITCHELL, *CITY OF BITS* (MIT Press, 1995).

"To a considerable extent, networks really are what software allows them to be. The Internet is not a network but a set of communications protocols. . . . [T]he Internet is software. Similarly, the World Wide Web is not anything tangible. It is client-server software that permits machines linked on a network to share and work with information on any of the connected machines."

Id., at [7]. See also Post, *supra* note 50a, at par. 16 ("[N]etworks are not merely governed by substantive rules of conduct, they have no existence apart from such rules"). And software specifications can be unforgiving (as anyone who has tried to send an e-mail message to an incorrectly spelled network recipient can attest):

Entry of messages into, and routing of messages across, digitally-based electronic networks . . . are controlled by more effective protocols [than generally govern non-electronic communications networks in the "real world"]: each network's technical specifications (typically embodied in software or switching mechanisms) constitute rules that precisely distinguish between compliant and non-compliant messages. This boundary [is not an] artificial construct because the rules are effectively self-enforcing. To put the matter simply, you can't 'almost' be on the Georgetown University LAN or America Online--you are either transmitting LAN or AOL-compliant messages or you are not."

Id., at par. 20 (emphasis added). Thus, individual network communities can be configured, by means of unique specifications of this kind, to bar all (or some specified portion of) inter-network traffic with relative ease.

99. Sandel, *supra* note 63, at 73-4 (emphasis added)

100. Brilmayer, *supra* note 7, at 5.

101. In Albert Hirschman's terms, they have a "voice" in the development of French law, at least to the extent that French law-making institutions represent and are affected by citizen participation. Albert O. Hirschman, *Exit, Voice and Loyalty* 106-19 (1970); cf. Richard A. Epstein, *Exit Rights under Federalism*, *Law & Contemp. Probs.*, Winter 1992, at 147, 151-165 (discussing the ability of exit rights to constrain governmental power and the limitations of such rights).

102. "There has always been a strong fictional element to using this notion of a social contract as a rationale for a sovereign's legitimacy. When exactly did you or I consent to be bound by the US Constitution? At best, that consent can only be inferred indirectly, from our continued presence within the US borders -- the love-it-or-leave-it, vote-with-your-feet theory of political legitimacy. But by that token, is Saddam Hussein's rule legitimate, as least as to those Iraqis who have 'consented' in this fashion? Have the Zairois consented to Mobutu's rule? In the world of atoms, we simply cannot ignore the fact that real movement of real people is not always so easy, and that most people can hardly be charged with having chosen the jurisdiction in which they live or the laws that they are made to obey. But in cyberspace, there is an infinite amount of space, and movement between online communities is entirely frictionless. Here, there really is the opportunity to obtain consent to a social contract; virtual communities can be established with their own particular rule-sets, power to maintain a degree of order and to banish wrongdoers can be lodged, or not, in particular individuals or groups, and those who find the rules oppressive or unfair may simply leave and join another community (or start their own)." Post, *supra* note 24, at 33.

103. The ease with which individuals may move between communities (or inhabit multiple communities simultaneously through a fractionation of their own individual identities) also implies that Cyberspace may provide conditions necessary and sufficient for something more closely resembling the optimal collective production of a particular set of goods -- namely, "laws" -- than can be achieved in the real world. Cyberspace may closely approximate the idealized model for the allocation of local goods and services set forth by Charles Tiebout, see Charles Tiebout, *A Pure Theory of Local Expenditures*, 64 *J. POL. ECON.* 416 (1956), in which optimal allocation of locally-produced public goods is provided by small jurisdictions competing for mobile residents. The Tiebout model of intergovernmental competition has four components: (1) a perfectly elastic supply of jurisdictions, (2) costless mobility of individuals among jurisdictions, (3) full information about the attributes of all jurisdictions, and (4) no interjurisdictional externalities. See Robert P. Inman and Daniel L. Rubinfeld, *The Political Economy of Federalism*, Working Paper No. 94-15, Boalt Hall Program in Law and Economics (1994), at 11-16, (reprinted in D. Mueller (ed.), *Developments in Public Choice*, Cambridge Univ. Press 1995). (As Inman and Rubinfeld demonstrate, a fifth assumption of the Tiebout model--the provision of public goods with a "congestible technology" such that the per capita cost of providing each level of a public good first decreases and then

increases as more individuals move into the jurisdiction--is not necessary for the model. Id., at 13.) In a Tieboutian world,

. . . each locality provides a package of local public goods consistent with the preferences of its residents (consumer-voters). Residents whose preferences remain unsatisfied by a particular locality's package of goods and services would (costlessly) move. . . . Escape from undesirable packages of goods and services is feasible as a result of two explicit characteristics of the Tiebout model: absence of externalities and mobility of residents.

Gillette, In Partial Praise of Dillon's Rule, or, Can Public Choice Theory Justify Local Government Law, 67 CHI-KENT L. REV. 959, 969 (1991). We suggest that cyberspace may be a closer approximation to ideal Tieboutian competition between rule-sets than exists in the nonvirtual world, a consequence of (1) the low cost of establishing an online "jurisdiction," see text at note 93, (2) the ease of exit from online communities, (3) the relative ease of acquiring information about the practices of online communities, and (4) the greater impermeability of the internal, software-mediated boundaries between online communities in cyberspace, see supra note 98, which may mitigate (at least to some extent) the problem of inter-community externalities.

104. The Net may need new meta-rules for transporting information across these borders. For example, the members of the LambdaMOO multi-user domain debated at length whether to permit the use of information obtained from the virtual discussion group out in the "real world." See Mnookin, supra note 57, at 20-21. Various online systems have rules about copying or reposting materials from one online area to another. For example, the terms of service for Counsel Connect contains the following rules for acceptable copying:

[M]embers who submit material shall be deemed to (I) grant to . . . subscribers to the system a paid up, perpetual, world-wide irrevocable license to use, copy, and redistribute such materials and any portions thereof and any derivative works therefrom . . . Each member agrees, as a condition of such license, (I) not to remove identifying source information from verbatim copies of member-supplied materials . . . and (ii) not to reproduce portions thereof in any way that identifies the source but fails to describe accurately the nature and source of any modification, alteration thereto or selection therefrom B. Notwithstanding the licenses granted by members and information suppliers, subscribers . . . shall not engage in systematic, substantial and regular replication of materials supplied to the system by a commercial publisher . . . where the effect of such actions is to provide another person who is not an authorized subscriber to such materials with a substantial substitute for such a subscription.

Terms and Conditions for Use of Counsel Connect (on file with the Stanford Law Review) America Online's Terms of Service Agreement contain a somewhat similar clause:

4. Rights and Responsibilities (a) Content . . . [Members] Acknowledge that (I) AOL contains information, software, photos, video, graphics, music, sounds and other material and services (collectively, "Content") . . . AOL permits access to Content that is protected by copyrights, trademarks, and other proprietary (including intellectual property) rights. . . . [members'] use of Content shall be governed by applicable copyright and other intellectual property laws. . . . By submitting Content to and "Public Area" . . . [members] automatically grant . . . AOL Inc. the royalty free, perpetual, irrevocable, non-exclusive right and license to use, reproduce, modify, adapt, publish, translate, create derivative works from, distribute, perform and display such Content (in whole or part) worldwide . . .

. For more details, here is a fuller extract from the text of AOL's Term of Service:

"2.6 Content

(a) Proprietary Rights.

Member acknowledges that the AOL Service contains information, software, photos, video, graphics, music, sounds or other material (collectively, "Content") that are protected by copyrights, trademarks, trade secrets or other proprietary rights, and that these rights are valid and protected in all forms, media and technologies existing now or hereinafter developed. All Content is copyrighted as a collective work under the U.S. Copyright laws, and AOL Inc. owns a copyright in the selection, coordination, arrangement and enhancement of such Content. Member may not modify, publish, transmit, participate in the transfer or sale, create derivative works, or in any way exploit, any of the Content, in whole or in part. If no specific restrictions are displayed, Member may make copies of portions of the Content, including copyrighted material, trademarks, or other proprietary materials, provided that the copies are made only for Member's personal use and that Member maintains any notices contained in the Content such as all copyright notices, trademark legends or other proprietary rights notices. Except as provided in the preceding sentence or as permitted by the fair use privilege under the U.S. copyright laws (see e.g. 17 U.S.C. Section 107), You may not upload, post, reproduce, or distribute Content protected by copyright, or other proprietary right, without obtaining permission of the copyright owner. Use of any software Content shall be governed by the software license agreement accompanying such software or, if none exists, then such use shall be proscribed by the terms governing licensing and use of the AOL Software as provided in Section 6 herein.

(b) Distribution/Uploading of Third Party Content.

Member may upload to the software files or otherwise distribute on the AOL Service only Content that is not subject to any copyright or other proprietary rights protection (collectively, "Public Domain Content"), or Content in which the

author has given express authorization for on-line distribution. Any copyrighted Content submitted with the consent of a copyright owner should contain a phrase such as "Copyright owned by [name of the owner]; Used by Permission." The unauthorized submission of copyrighted or other proprietary Content constitutes a breach of the TOS and could subject You to criminal prosecution as well as personal liability for damages in a civil suit. Remember You, not AOL Inc. or its independent contractors, are liable for any damage resulting from any infringement of copyrights, proprietary rights, or any other harm arising from such submission. By submitting Content to any "Public Area" (Public Area(s) are those areas of the AOL Service that are generally accessible to other Members, such as chat rooms, message boards, and file uploads) You automatically grant, or warrant that the owner of such Content has expressly granted, AOL Inc. the royalty-free, perpetual, irrevocable, non-exclusive right and license to use, reproduce, modify, adapt, publish, translate and distribute the Content (in whole or part) worldwide and/or to incorporate it in other works in any form, media, or technology now known or hereafter developed for the full term of any copyright that may exist in such Content. You also permit any Member to access, view, store or reproduce the Content for that Member's personal use. Subject to this grant, the owner of Content placed on the AOL Service retains any and all rights which may exist in such Content.

© Export.

The U.S. export control laws regulate the export and re-export of technology originating in the United States. This includes the electronic transmission of information and software to foreign countries and to certain foreign nationals. Member agrees to abide by these laws -- including but not limited to the Export Administration Act, the Arms Export Control Act and their implementing regulations -- and not to transfer, by electronic transmission or otherwise, any Content derived from the AOL Service to either a foreign national or a foreign destination without first obtaining any required government authorization. Member further agrees not to upload to the AOL Service any data or software that cannot be exported without prior written government authorization, including, but not limited to, certain types of encryption software. This assurance and commitment shall survive termination of the Agreement. In addition, because the U.S. export control laws currently prohibit nationals of Cuba, Iran, Libya, North Korea and Syria from gaining access to certain Content on the AOL Service, nationals of these countries currently may not legally access the AOL Service at this time.

(d) Benefit of Provisions.

The foregoing provisions of this section 2.6 are for the benefit of AOL Inc. and its independent third-party information providers ("Information Providers"), merchants ("Merchants") and licensors ("Licensors"), and each shall have the right to assert and enforce such provisions directly on their own behalf.

2.7 Third Party Content.

AOL Inc. is a distributor (and not a publisher) of Content supplied by third parties and Members. Accordingly, AOL Inc. has no more editorial control over such Content than does a public library, bookstore, or newsstand. Any opinions, advice, statements, services, offers, or other information or Content expressed or made available by third parties, including Information Providers, Merchants (as defined herein), Members, or any other user of the AOL Service, are those of the respective author(s) or distributor(s) and not of AOL Inc. NEITHER AOL INC. NOR ANY THIRD-PARTY PROVIDER OF INFORMATION GUARANTEES THE ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY CONTENT, NOR ITS MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE. ...

In many instances, the Content available through the AOL Service represents the opinions and judgments of the respective Information Provider, Member, or other user not under contract with AOL Inc. AOL Inc. neither endorses nor is responsible for the accuracy or reliability of any opinion, advice or statement made on the AOL Service by anyone other than authorized AOL Inc. employee spokespersons while acting in their official capacities. (Forum leaders and Member Guides are not authorized spokespersons.) Under no circumstances will AOL Inc. be liable for any loss or damage caused by a Member's reliance on information obtained through the AOL Service. It is the responsibility of Member to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other Content available through the AOL Service. Please seek the advice of professionals, as appropriate, regarding the evaluation of any specific information, opinion, advice, or other Content.

2.8 Retention of Files.

Member is responsible for retention of all files, information data and other materials as may be necessary for reconstruction of any files, information material or messages lost or misprocessed by AOL Inc."

¹⁰⁵ See Sandel, *supra* note 63, at 74 ("Self-government today . . . requires a politics that plays itself out in a multiplicity of settings, from neighborhoods to nations to the world as a whole. Such a politics requires citizens who can abide the ambiguity associated with divided sovereignty, who can think and act as multiply situated selves."); see also, Sherry Turkle, *Life on the Screen: Identity in the Age of the Internet* (1995); Sherry Turkle, *The Second Self: Computers and the Human Spirit* 95 (1984). To be sure, sophisticated analysis even of traditional legal doctrines suggests that we appear before the law only in certain partial, conditional roles. Joseph Vining, *Legal Identity: The Coming of Age of Public Law* 139-69 (1978). But this partial and conditional nature of "persons" who hold rights and duties is more pronounced in Cyberspace.

106. See Chatterjee, *supra* note 45c, at 425 n.142 (noting that "[o]riginal copyright paradigms were created to protect only physical books").

107. Electronic information can be dispensed in any sized serving, ranging from a few words to an entire database. If we use the database as a whole as our measure, then any user's selection will be an insignificant portion. In contrast, if we tried to use the traditional boundaries of the books cover, the user cannot observe this standard; in some cases it is an entirely theoretical boundary, with respect to material only dispensed from the database. This case demonstrates again that the absence of physical borders setting off distinct "works" in Cyberspace undermines the utility of doctrines like copyright law that are based on the existence of such boundaries in the real world.

108. Whether the law should consider that interest to be a "property" right or a right on behalf of the "persona" in question remains in doubt.

Copyright © 1996, *First Monday*

Law and Borders - The Rise of Law in Cyberspace by David R. Johnson and David Post.

First Monday, volume 1, number 1 (May 1996),

URL: [http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php?journal=fm&page=article&op=view&path\[\]=468&path\[\]=389](http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php?journal=fm&page=article&op=view&path[]=468&path[]=389)