David R. Johnson and David G. Post, *Law and Borders —The Rise of Law in Cyberspace*
45 Stan. L. Rev. 1367 (1996)

Global computer-based communications cut across territorial borders, creating a new realm of human activity and undermining the feasibility—and legitimacy—of 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 its own law and legal institutions. Territorially based law-makers and law-enforcers 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 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 online participants' core values.

We take for granted a world in which geographical borders—lines separating physical spaces—are of primary importance in determining legal rights and responsibilities. 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 homogeneous applicable law and legal institutions fitting within existing physical borders. * * *

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 logical relationship to the development and enforcement of legal rules is 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. Law-making requires some mechanism for law enforcement, which in turn depends on the ability to exercise physical control over, and 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 business owners. Such an assertion of control would conflict with the Brazilian government's recognized monopoly on the use of force over its citizens.

Effects. The correspondence between physical boundaries and "law space" boundaries 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 within Brazil than anywhere else. For example, 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. 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, those people subject to a sovereign's laws, and most deeply affected by those laws, are the 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.

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 a local sovereign's efforts to regulate global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply. The Net thus radically subverts the 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 one 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. The Net enables transactions between people who do not know, and in many cases cannot know, each other's physical location. 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 the domain name initially assigned to a given machine may be associated with an Internet

Protocol address that corresponds to that machine's physical location (for example, a ".uk" domain name extension), the machine may be physically moved without affecting its domain name. Alternatively, the owner of the domain name might request that the name become associated with an entirely different machine, in a different physical location. Thus, a server with a ".uk" domain name need not 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.

The power to control activity in Cyberspace has only the most tenuous connections to physical location. Nonetheless, many governments' first response to electronic communications crossing their territorial borders is to try to stop or regulate that flow of information. Rather than permitting self-regulation by participants in online transactions, many governments establish trade barriers, attempt to tax border-crossing cargo, and respond especially sympathetically to claims that information coming into the jurisdiction might prove harmful to local residents. As online information becomes more important to local citizens, these efforts increase. 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," will impinge upon the privacy of local citizens, and will upset private property interests in information. Even local governments in the United States have expressed concern about their loss of control over information and transactions flowing across their borders.

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. Individual [electronic impulses] 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. United States 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. Banking and securities regulators seem likely to lose their battle to impose local regulations on a global financial marketplace. 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 easier to 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. Others have been quick to assert the right to regulate all online trade insofar as it might adversely affect local citizens. The Attorney General of Minnesota, for example, has asserted the right to regulate gambling that occurs on a foreign web page that a local resident accessed and "brought into" the state. The New Jersey securities regulatory agency has

similarly asserted the right to shut down any offending Web page accessible from within the state.

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 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.

Territorial regulation of online activities serves neither the legitimacy nor the notice justifications. There is no geographically localized set of constituents with a stronger and more legitimate claim to regulate it than any other local group. The strongest claim to control comes from the participants themselves, and they could be anywhere. And in Cyberspace, physical borders no longer function as signposts informing individuals of the obligations assumed by entering into a new, legally significant, place. Individuals are unaware of the existence of those borders as they move through virtual space.

The rise of an electronic medium that disregards geographical boundaries 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, although privacy on the Net may be a familiar concept, analogous to privacy doctrine for mail systems, telephone calls, and print publications, electronic communications create serious questions regarding the

nature and adequacy of geographically based privacy protections. Communications that create vast new transactional records may pass through or even simultaneously exist in many different territorial jurisdictions. What substantive law should we apply to protect this new, vulnerable body of transactional data? 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.

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. * * *

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.