# The Zones of Cyberspace

Lawrence Lessig

Cyberspace is a place. People live there. They experience all the sorts of things that they experience in real space, there. For some, they experience more. They experience this not as isolated individuals, playing some high tech computer game; they experience it in groups, in communities, among strangers, among people they come to know, and sometimes like.[1]

While they are in that place, cyberspace, they are also here. They are at a terminal screen, eating chips, ignoring the phone. They are downstairs on the computer, late at night, while their husbands are asleep. They are at work, or at cyber cafes, or in a computer lab. They live this life there, while here. And then at some point in the day, they jack out, and are only here. They step up from the machine, in a bit of a daze; they turn around. They have returned.

David Johnson and David Post want us to take this life in cyberspace seriously. They want the law to understand it as elsewhere. So far elsewhere is it that it deserves, they argue, a special respect from real space law. Cyberspace will "create" new law and legal institutions of its own,[2] and this new law should free this space from at least some of the claims of real space law. A separateness will emerge. Not quite a sovereignty, but something close will develop.

This is a small and quirky field, cyberlaw; these are two of its most important thinkers, and this is a paper that will be at the center of much thought in cyberlaw to come. I have no doubt that in large measure, Johnson and Post will be right: A new law will emerge here, and a certain comity will follow it around. But Johnson and Post want to argue for a separation between real space law and cyberspace law that I don't believe can yet be sustained, nor do I believe that it should. The effects of that place will never be far removed from this. And our understanding of what that place will become is just beginning. We, here, in this world, will keep a control on the development there. As well we should.

## *The closeness that cyberspace is*

There is an interesting link between Dan Farber's paper and this. Farber offered three perspectives on legislative jurisdiction—a localist, a globalist, and

1. For descriptions, see HOWARD RHEINGOLD, THE VIRTUAL COMMUNITY 38-65 (1995); SHERRY TURKLE, LIFE ON THE SCREEN: IDENTITY IN THE AGE OF THE INTERNET (1995).

2. David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1387-91 (1996).

an evolutionary.[3] The link is to the first two. A localist looks for strong links with stuff that happens in local space before she claims an authority to regulate beyond her borders. A globalist is far less picky. Everything affects everything, the globalist insists, and our regulation should reach anything that affects us.

Johnson and Post mix these two perspectives. They present a picture of cyberspace that is both global and local. They first establish the separateness of cyberspace by arguing that since it is everywhere if anywhere, and hence no place in particular, it is therefore a space no where here—separate, removed. Its globalness establishes its separateness; no locale can make any special claim upon it.

But in the very next breath, they are insistent localists: Cyberspace, separate from real space, has little effect over real space; hence should real space have little control over cyberspace. When real space jurisdictions assert control over cyberspace life, this is an "illegitimate extra-territorial power grab"[4]—unjustified,[5] and unwise. As they write: "[Governments cannot] 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."[6]

This argument they support with positive as well as normative arguments, but I confess I don't find the positive points very persuasive. The first is a kind of is-ism— the real world is made of atoms, cyberspace of bits; the rules of the atoms don't work very well when applied to bits. Bits don't respect borders, they can't be cabined by borders. They go wherever the net goes, and the net goes everywhere without much limit. Hence rules that would contain atoms can't be applied well to bits.

This feels more like slogan than argument. I don't care really whether it is atoms, or bits; the legitimacy of regulation turns upon effects. If the net has an effect on that half of the cybercitizen that is in real space, if it has an effect on third parties who are only in real space, then the claim of a real space sovereign to regulate it will be as strong as any equivalent atom induced effect. If a state has the power to regulate the importation of obscenity, it can't make any differ-

3. Daniel A. Farber, *Stretching the Margins: The Geographic Nexus in Environmental Law*, 48 STAN. L. REV. 1247, 1248 (1996).

4. Johnson & Post, *supra* note 2, at 1380.

5. So, of a net-based Ponzi scheme from the Cayman Islands over which Minnesota has tried to assert jurisdiction, Johnson and Post would argue that "clearly" Minnesota would not have any jurisdiction over the scheme. *Id.* at 1383.

6. *Id.* at 1390.

ence whether that importation is via atoms or bits,[7] at least from the perspective of the justifiability of the regulation.[8] Its justification rests here in effects.

If this localism, in Farber's terms, is to be defended, something other than physics must be appealed to. Johnson and Post have a second argument, grounded in futility: The example here is the German threat against Compuserve. In January, 1996, Bavarian officials threatened Compuserve with prosecution if it continued to carry sexually explicitly newsgroups from USENET. In response, Compuserve removed these newsgroups from its service worldwide.

Schemes like this to regulate local access don't work, Johnson and Post argue, because "the determined seeker of prohibited communications can simply reconfigure his connection so as to appear to reside in a [different] location."[9] True enough—Germans determined enough can (even now) use Compuserve to gain access to the prohibited material.[10] But this forgets my colleague Coase. A regulation need not be absolutely effective to be sufficiently effective. It need not raise the cost of the prohibited activity to infinity in order to reduce the level of that activity quite substantially. If regulation increases the cost of access to this kind of information, it will reduce access to this information, even if it doesn't reduce it to zero. That is enough to justify the regulation. If government regulation had to show that it was perfect before it was justified, then indeed there would be little regulation of cyberspace, or of real space either. But regulation, whether for the good or the bad, has a lower burden to meet.

There is something to the futility argument. This is David Post's piece, *Anarchy, State and the Internet.*[11] Post's argument there, echoed in the piece in this review, is that the architecture of cyberspace compels a different kind of

7. Pointing to the recent *Amateur Action* case, United States v. Thomas, 74 F.3d 701 (6th Cir. 1996), Johnson and Post argue that the standard for obscenity should not be the local physical community where the material is consumed, but rather the online community within which the material is delivered. But in that case, where the postmaster downloaded some material online, and received other material through the mail, this rule would require that one community govern the online access, and another govern the mail access. This is a difference I don't understand. Whatever the mode of transmission, whether the Internet or UPS, the test should be the same. And in both cases, the relevant question would seem to be what effect this has on them in the jurisdiction where they live, when they step away from the video machine or computer terminal. Maybe the effect is so insignificant that it ought in neither case be regulated. But if it is regulated in the one, the fact that the medium in the other is bits shouldn't change the matter. Except according to a quite different argument, which I sketch below.

8. Or at least, if it did make a difference, the difference would turn on the greater, not lesser, ability of bits to be regulated than atoms. If the only interest that obscenity laws advanced were a zoning interest—assuring that only those who want to view the material viewed it—then one might argue that because bytes are so much better regulated than atoms, the justification for obscenity regulation is reduced. Because, that is, the technology can better assure that only the intended recipient receives the regulated material, the regulations of that material in cyberspace should be less absolute than in real space. But the Court has never precisely defined for us the real interests advanced by obscenity regulation. In Stanley v. Georgia, 394 U.S. 557 (1969), it sounded as if the interest were purely a zoning interest; but the Court rejected this notion in Paris Adult Theater I v. Slaton, 413 U.S. 49 (1973).

9. Johnson & Post, *supra* note 2, at 1374.

10. *See* Jon Auberbach, *Fences in Cyberspace: Governments Move to Limit Free Flow of the Internet*, BOSTON GLOBE, Feb. 1, 1996, at 1, 15.

11. David G. Post, *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace*, 1995 J. ONLINE L. art. 3, *available at* http://www.law.cornell.edu/jol/post.html.

regulation. The internet, he argues, is a network of networks; each network is its own law, each carries its own rule-set. Because these "rule-sets" are not tied to any particular geographical space, they can exit whenever the geographical space becomes hostile. It matters not at all, the argument goes, whether the server supporting one network is located in Germany, or France, or Russia.[12] So long as the networks are interconnected, if the laws of Germany become hostile, the network can simply move to Russia. From the standpoint of the users, this move is invisible. And so any effort by Germany to control what exists on German servers will be defeated by this structural plasticity.

But what follows from this is not that no regulation is possible; what follows is that successful regulation will be different. There is a competition among rule-sets; cyberspace creates a market among these rule-sets. But there are still ways to regulate a market, so long as the regulator has some market power. Germany's effort at silencing sex-speech on Compuserve may be thought pathetic, since so easily evaded; nonetheless, it did have the effect of pushing Compuserve to implement a technology that would allow the company to censor material based on the location of the reader. A pathetic, but successful, regulation by Germany. Or the same could be said about America's regulation of cryptography.[13] No doubt any effort directly to ban encryption technologies will, in the end, fail; but efforts to subsidize particular technologies will not so obviously fail. Regulation is possible, but through different means.

The insight that Post, and Johnson and Post, have is that because the transactions costs of exit are so low, the power of government to regulate this space is futile. But the conclusion doesn't follow from the premise. Transactions costs are low; but so long as they are not zero, there is space for regulation. The regulation will be of a different form; its techniques will have to become quite different. But if well designed, they will not be futile.

There will be a law of cyberspace, but Johnson and Post have not shown enough to show just why it will be in any special way immune from real space regulations. It will be regulated by real space regulation to the extent that it affects real space life, and it will quite dramatically affect real space life. That is the amazing thing about this space—that this virtual place has such power over what we call the nonvirtual. This effect must be at the core of any argument about cyberspace's difference, not its absence.

12. Of course claims like this are always exaggeration. To an American user today, it matters quite a bit whether the server she is accessing is located in Ohio or Oslo, for access to Oslo, or any European location, can be quite slow. While in theory it doesn't matter where the server is, if the U.S. government succeeded in getting all material of a certain kind (say, obscenity) moved to nonAmerican servers, it would have a significantly reduce consumption of that material.

13. *See generally* A. Michael Froomkin, *The Metaphor is the Key: Cryptography, The Clipper Chip, and the Constitution*, 143 U. PENN. L. REV. 709 (1995) (examining the constitutional and policy questions that underlie governmental regulation of consumer cryptography).

*The question of what cyberspace will be*

To argue that real space law should leave cyberspace alone one needs a normative argument—an argument about why it is good or right to leave cyberspace alone. This depends upon consequences, and consequences depend upon what cyberspace will become. Johnson and Post push the first half of this quite well; but it is the second half that is the more important. And more troubling.

The argument focusing on consequences is simple pragmatism. Cyberlaw will evolve to the extent that it is easier to develop this separate law than to work out the endless conflicts that the cross-border existences here will generate.[14] Some fields will be easier to regulate with this cyber common law, and as this cyber common law of cyberspace develops, and earns the respect of other jurisdictions, it will be easier for these other jurisdictions simply to defer to this law.[15] The alternative is a revival of conflicts of law; but conflicts of law is dead—killed by a realism intended to save it. And without a usable body of law to deploy against it, a law of cyberspace will emerge as the simpler way to resolve the inevitable, and repeated, conflicts that cyberspace will raise.

But this pragmatism must say something about what cyberspace will become, and it is here that I think Johnson and Post are most ambitious, one might say romantic, while I am firmly skeptical. Their picture is of a democracy in cyberspace—of a world of cybercitizens deciding on the laws that will apply to them, and a claim that this more perfect democracy deserves respect.[16] The separation that they argue for comes then from the respect that we owe this autonomy.

This is a hope built on a picture of cyberspace as it is just now. As it is just now, cyberspace is such a place of relative freedom. The technologies of control are relatively crude. Not that there is no control. Cyberspace is not anarchy. But that control is exercised through the ordinary tools of human regulation—through social norms, and social stigma; through peer pressure, and reward. How this happens is an amazing question—how people who need never meet can establish and enforce a rich set of social norms is a question that will push theories of social norm development far. But no one who has lived any part of her life in this space as it is just now can doubt that this is a space filled with community, and with the freedom that the imperfections of community allows.

This is changing. Cyberspace is changing. And to understand what this change could be, we must think again about the very nature of cyberspace itself—more particularly, about the nature of how cyberspace regulates itself.

Think of how a community regulates itself in real space. In real space, when the state wants to regulate something—say littering—the state threatens, or cajoles, through prisons or fines or furry little animals on TV, to induce people to internalize this norm against littering. If the state succeeds, behavior changes. But its success depends upon individuals internalizing what the state

14. Johnson & Post, *supra* note 2, at 1391-95.

15. *Id.*

16. *See, e.g., id.* at 1389-91.

requires. Between the norm and the behavior sought is a human being, mediating whether to conform or not. Lots of times, for lots of laws, the choice is not to conform. Regardless of what the law says, it is an individual who decides whether to conform.

Regulation in cyberspace is, or can be, different. If the regulator wants to induce a certain behavior, she need not threaten, or cajole, to inspire the change. She need only change the code—the software that defines the terms upon which the individual gains access to the system, or uses assets on the system. If she wants to limit trespass on a system, she need not rely simply on a law against trespass; she can implement a system of passwords. If she wants to limit the illegal use of copyrighted material, she need not rely on the threat of copyright law; she can encrypt the copyrighted material so only those intended to have access will have access. Always in principle, and increasingly in practice, there is a code (as in software) to assure what the code (as in law) demands, which means always in principle and increasingly in practice, law is inscribed in the code.

Code is an efficient means of regulation. But its perfection makes it something different. One obeys these laws as code not because one should; one obeys these laws as code because one can do nothing else. There is no choice about whether to yield to the demand for a password; one complies if one wants to enter the system.[17] In the well implemented system, there is no civil disobedience. Law as code is a start to the perfect technology of justice.

It is not this just now. Just now the architecture of cyberspace is quite imperfect. Indeed, what is central about its present architecture is the anarchy that it preserves. Some see this anarchy as inherent in the space, as unavoidable.[18] But this anarchy is just a consequence of the present design. In its present design, cyberspace is open, and uncontrolled; regulation is achieved through social forces much like the social forms that regulate real space. It is now unzoned: Borders are not boundaries; they divide one system from another just as Pennsylvania is divided from Ohio. The essence of cyberspace today is the search engine—tools with which one crosses an infinite space, to locate, and go to, the stuff one wants. The space today is open, but only because it is made that way. Or because we made it that way. (For whatever is true about society, at least cyberspace is socially constructed.)

It could be made to be different, and my sense is that it is. The present architecture of cyberspace is changing. If there is one animating idea behind the kinds of reforms pursued both in the social and economic spheres in cyberspace, it is the idea to increase the sophistication of the architecture in cyber-

17. Hackers don't. But what hackers do doesn't define what the effect of law as code is on the balance of the non-hacker public.

18. Hackers for example—the civil disobedients of cyberspace. Hackers define for themselves a certain anarchy, by devoting themselves to finding the holes in the existing code. Some believe that the complexity of the code means these holes will always exist, and hence this anarchy will always exist. But I don't think one need believe hacking impossible to believe it will become less and less significant. People escaped from concentration camps, but that hardly undermines the significance of the evil in concentration camps.

space, to facilitate boundaries rather than borders. It is the movement to bring to zoning to cyberspace. From this perspective, the Communications Decency Act of 1996, and the NII White Paper on Copyright are the very same thing: Neither aims at eliminating material in cyberspace; both aim instead at inducing a technology for zoning. The Communications Decency Act does this by granting wide defenses to individuals who take steps to block access by minors, while threatening huge penalties to those who don't.[19] The White paper does this by giving broad support to technologies that control access to copyrighted material, while narrowing the scope for fair use of material otherwise available on the net. The aim of both is to subsidize technologies of control—to increase the ability to select who gets access to what—and the medium cyberspace is perfectly designed for that control.

We are just at the beginning of this change. Zoning will replace the present wilderness of cyberspace, and this zoning will be achieved through code—a tool, as Johnson and Post suggest, more perfect than any equivalent tool of zoning in real space. The architecture of cyberspace will in principle allow for perfect zoning—a way perfectly to exclude those who would cross boundaries. It is the perfection of the architecture that Jerry Frug's contribution to this symposium speaks of; and the movement that I am describing from open to closed is just the movement that he, and Richard Ford, have described (and criticized) in real space law.[20] Indeed, if there is one clear return from the mixing of the perspectives that this symposium has done, it is the lessons that the first panel can offer the last: For in the rich descriptions offered there—of movements in real space from open to closed, and in the structures of incentives that might yield this move, even though individuals in the end might regret it,[21]—we can draw parallels to the movement that we might see here. Movements from what, speaking of free-speech terrains, Monroe Price calls an open terrain to a closed;[22] but more generally, from a world where boundaries are borders, to a world where boundaries are walls.

One might well say that this movement to more perfect zoning is just what "the people want." But want here is complex. They want control over what their kids get access to; they want control over who "takes" their intellectual

19. The Act has two defenses. The first gives a substantive defense to prosecution if a user "has taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors." § 501(2). The second directs that "no cause of action may be brought . . . against any person [where that person] has taken in good faith to implement a defense authorized under this section." § 501(2). These defenses together mark out an extraordinarily large scope for protection. Recently the Justice Department has outlined what it considers to be adequate steps to satisfy these defenses. These include simply registering an "indecent" site with one of the services that helps users screen "indecent" sites. The act is presently being challenged, and will most likely be held unconstitutional because of the overbreadth of the "indecency" provisions. But that is independent of the structure of its defenses. *See* American Civil Liberties Union v. Reno, 929 F. Supp. 824 (E.D. Pa. 1996).

20. Jerry Frug, *The Geography of Community*, 48 STAN. L. REV. 1047 (1996); Richard Thompsom Ford, *The Boundaries of Race: Political Geography in Legal Analysis*, 107 HARV. L. REV. 1841, 1860-78 (1994).

21. *See* Vicki Been, *Comment on Professor Jerry Frug's* The Geography of Community, 48 STAN. L. REV. 1109 (1996).

22. Monroe E. Price, *Free Expression and Digital Dreams: The Open and Closed Terrain of Speech*, 22 CRITICAL INQUIRY 64 (1995).

"property." They want to control what their citizens read. All these "theys" have lots to gain from the architecture that cyberspace is becoming, and we are a lot of these "theys." Commerce is built on property, and property depends upon boundaries. What possible reason could there be to question the value of clear borders?[23]

But we might nonetheless find reason to be skeptical, or at least reason to raise doubts. And it is upon two such doubts that I want to end this essay. First, a doubt about the design: As important as the nature of these newly zoned spaces is, more important is who is designing them. They are the construction, as Johnson and Post describe, of "engineers."[24] Engineers write the code; the code defines the architectures, and the architectures define what is possible within a certain social space. No process of democracy defines this social space, save if the market is a process of democracy.[25]

This might not be so bad, assuming that there are enough places to choose from, and given that it is cyberspace, the places to choose from could be many, and the costs of exit are quite low.[26] Even so, note the trend: the progression away from democratic control. We will stand in relation to these places of cyberspace as we stand in relation to the commodities of the market: one more place of unending choice; but one less place where we, collectively, have a role in constructing the choices that we have.

Which brings us back to the question that I began with above, and the second doubt that I want to raise in the end. This next generation of cyberspace will provide individuals with the perfect technology of choice; it will empower individuals to select into the world that they want to see, to select out of the world that they don't.[27] But the they who check out also live here; when not in cworld, they must participate in the making, and regulating, of the life that is here. And so the question: Just how will this life in cworld affect their ability to connect to this life in the real world? Will this power of exit enhance or undermine their ability to engage as citizens in the world from which they can't easily disengage? Will the many communities of that world make it more or less possible to function well in the communities of this world? These are questions, the answers to which turn on the architecture that cyberspace will become. But what the architecture of cyberspace will become is a choice we make here. So again we are back to the question how this space may regulate that space, if that space affects life here.

These questions point to a choice, about what cyberspace will become. One alternative is an open space; the other closed. I don't mean these are the only

23. *See* William Ian Miller, *Sanctuary, Red Light Districts, and Washington, D.C.: Some Observations on Neuman's Anomalous Zones*, 48 STAN. L. REV. 1235 (describing the costs of clear lines).

24. *See* Johnson & Post, *supra* note 2. at 1388.

25. *See* CASS SUNSTEIN, DEMOCRACY AND THE PROBLEM OF FREE SPEECH (1994); Cass R. Sunstein, *The First Amendment in Cyberspace*, 104 YALE L.J. 1757 (1995).

26. Not zero, mind you. Given the anonymity of this space, one must build a certain social capital to function well. Exit, or banishment, is the forfeiting of that social capital. As in real life, this is a real loss, and this loss is what makes communities somewhat sticky.

27. See the world Eugene Volokh describes in *Cheap Speech and What It Will Do*, 104 YALE L.J. 1805 (1995).

choices. Architectures don't come in natural kinds. My point instead is the choice—that there is a decision to be made about the architecture that cyberspace will become, and the question is how that decision will be made.

Or better, *where* will that decision be made. For this change has a very predictable progress. It is the same progress that explains the move to zoning in cities. It is the result of a collection of choices made at an individual level, but no collective choice made at a collective level. It is the product of a market. But individual choice might aggregate in a way that individuals collectively do not want. Individual choices are made within a particular architecture; but they may yield an architecture different from what the collective might want.

Might, not will. The point is not about pessimism, it is about possibility. But the possibility suggests a question about how quickly we liberate that space from regulation by the real space. For if there are choices to be made about how this space will evolve, it is not quite clear where in cyberspace these choices can be made. If cyberspace were to become this perfect technology of technology *and* democracy, then there would be little reason to worry. But a perfect technology of control does not entail a perfect technology of justice, and it is this that commends a continued check.

It is not clear where that leaves the law of cyberspace, or what strategy this recommends. But if the argument for deference that Johnson and Post here beg is a normative argument, we must say something more about the normative attractiveness of the world that cyberspace will be. If it is a world that facilitates our isolation, if it is an even better technology for constructing this isolation, if it is an even more efficient way to undermine the citizenship of this world, then one might question it. At a minimum, one might question whether we know what we must do to avoid these as outcomes. And we might want to preserve the possibility to avoid them.