What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace

David G. Post*

Code and Other Laws of Cyberspace is Lawrence Lessig's ambitious attempt to make sense of the new kinds of legal and regulatory problems that cyberspace presents to us. It is built upon the foundational premise that code—the hardware and software elements that populate this new place, and the communication protocols that allow these elements to interact with one another—defines the architecture of this new space and is of paramount importance in determining how it will be regulated. As an anthropology of the various new regulatory and quasi-regulatory structures that may arise on the global network, Lessig's book is captivating and often dazzling; he demonstrates, compellingly, that cyberspace is a place in which code dominates, a world in which "code is law." As a normative call to arms, however, the book is somewhat less successful. Lessig argues that because we are the code writers—because cyberspace is a made, not a found, world—control over the code needs to be subject to political, collective decision-making. Post suggests several reasons why this conclusion might not follow as smoothly from the premise as Lessig might have us believe.

CODE AND OTHER LAWS OF CYBERSPACE. By Lawrence Lessig. Basic Books. 1999. 297 pp. $30.00.

The emergence of the vast informational ecosystem we call cyberspace is an event of incalculable importance in the history of human liberty. The diversity and vibrancy of this "never-ending worldwide conversation"[1] continues to astonish and amaze those who spend time there. But life, as Kierkegaard reminds us, has to be lived forward, even if it can only be understood backward. Having brought this thing into being, how do we keep it alive and growing so that it can realize its profound freedom-enhancing promise? What's the plan?

Some suggest that this is all too important to be "left to the market," that the choices cyberspace forces upon us involve fundamental, even "constitutional," values that commerce will ignore or even destroy. Lawrence Lessig's *Code and Other Laws of Cyberspace* is surely the most

* Associate Professor, Beasely School of Law at Temple University and Fellow, National Center of Technology and Law, George Mason University School of Law; DPost@vm.temple.edu. Many thanks to Dawn Nunziato, Eugene Volokh, and David Johnson for illuminating conversations about earlier drafts of this essay, to Bill Scheinler for his always-helpful research assistance, and to Larry Lessig, for sharing his thoughts on these matters (as well as a searchable electronic version of an early draft of his manuscript) with me.

1. American Civil Liberties Union v. Reno, 929 F. Supp. 824, 883 (E.D. Pa. 1996).

elegant articulation of this view: Politics and collective decisionmaking, not the invisible hand, will give us a cyberspace where these values are protected.[2] I want to try here to articulate a different vision of the space. Fundamental values are indeed at stake in the construction of cyberspace, but those values can best be protected by allowing the widest possible scope for uncoordinated and uncoerced individual choice among different values and among different embodiments of those values. We don't need "a plan" but a multitude of plans from among which individuals can choose, and "the market," and not action by the global collective, is most likely to bring that plenitude to us.

As I was preparing this essay, I was asked to speak at a panel discussion about the problem of unwanted and unsolicited email ("spam") at Prof. Lessig's home institution, Harvard Law School's Berkman Center for Internet and Society.[3] The discussion focused on one particular anti-spam institution, the Mail Abuse Prevention System ("MAPS"); Paul Vixie, the developer and leader of MAPS, was also a participant at the event. MAPS attacks the problem of spam by coordinating a kind of group boycott by Internet service providers ("ISPs"). It operates, roughly, as follows.[4] The managers of MAPS create a list—the Realtime Blackhole List ("RBL")—of ISPs who are, in their view, fostering the distribution of spam. MAPS defines "fostering the distribution of spam" as, inter alia, providing "spam support services" (e.g., hosting web pages that are listed as destination addresses in bulk emails, providing email forwarders or auto-responders that can be used by bulk emailers), or allowing "open-mail relay" (i.e., allowing mail handling servers to be used by nonsubscribers, which allows bulk emailers to "launder" email by launching it from a site to which they cannot be traced).[5] MAPS makes the RBL list available to other ISPs on a subscription basis.[6] ISPs who subscribe to the RBL can, if they choose, set their mail handlers to delete all email originating from, or going to, an address appearing on the list; blackholed addresses disappear, in a sense, from the Internet as far as the subscribing ISP (and its customers) are concerned.[7]

---

2. *See* text accompanying notes 87-94 *infra*.

3. My thanks go to Jonathan Zittrain, Executive Director of the Berkman Center, for inviting me to this event; those interested can view the "scribe's notes" of this discussion at *Internet and Society 1999: The Technologies and Politics of Control* <http://cyber.law.harvard.edu/is99/scribes10.html>, and the event itself in RealVideo at <http://cyber.law.harvard.edu/is99/class10>.

4. *See generally* MAPS Realtime Blackhole List <http://maps.vix.com/rbl/>; Mail Abuse Prevention System <http://mail-abuse.org/>.

5. *See* MAPS RBL Candidacy <http://maps.vix.com/rbl/candidacy.html>.

6. There is currently no charge to subscribe to the RBL. *See MAPS RBL Participants* <http://maps.vix.com/rbl/participants.html>.

7. For instance, suppose I use the facilities of Temple University to send and receive email over the Internet. Assume that Temple is a subscriber to the RBL, and that the ISP *XYZ.com* is placed on the RBL. If Temple chooses to implement the "boycott" of XYZ in its mail handling

The timing was propitious. Lessig, it happens, has made it very clear that he doesn't like the RBL at all. In one of the columns that he writes periodically for the *Industry Standard*, he castigates members of what he called the "self-righteous spam police," and he offered his opinion that "fundamental policy questions about how the Net will work" should not be in the hands of these "vigilantes."[8] Should network policy be subject to this kind of "policy-making by the 'invisible hand'"?[9]

> *The answer is obvious, even if the solution is not.* This is not how policy should be made. We know this, but we don't know what could replace it. We imagine policy decisions made in a context where dissent can be expressed without punishment, where collective decisions can be made. But no such context exists in cyberspace, nor in our imagination about what cyberspace might become.[10]

Now, my take on the RBL is quite different than Lessig's.[11] The MAPS "vigilantes" (bad) can just as easily be characterized as "activists" (good), and the kind of "bottom-up," uncoordinated, decentralized process of which the RBL is a part[12] strikes me as a perfectly reasonable way to make "network policy" and to "answer fundamental policy questions about how the Net will work."

What I found most puzzling is not that Lessig and I disagreed; we have engaged in a public and private conversation about law and governance in

---

software, any email that I send to *janedoe@xyz.com*, and any email that is addressed to me from *janedoe@xyz.com*, will be deleted before delivery.

8. Lawrence Lessig, *The Spam Wars*, THE INDUSTRY STANDARD (Dec. 31, 1998) <http://www.thestandard.com/article/display/0,1151,3006,00.html>.

9. *Id.*

10. *Id.* (emphasis added).

11. *See* David G. Post, *Of Horses, Black Holes, and Decentralized Law-Making in Cyberspace* (last modified March 1, 1999) <http://www.temple.edu/lawschool/dpost/blackhole.html>.

12. Many other organizations compete with MAPS's efforts to reduce or eliminate what they regard as "spam." The Open Relay Behavior Modification System (ORBS) focuses its efforts on identifying and providing a list of mail servers which permit third-party relay. *See Orbs* <http://www.orbs.org/>. The Network Abuse Clearinghouse forwards complaints about spam and other network related issues to the appropriate network administrator. *See Abuse.Net: Home Page* <http://www.abuse.net>. The site www.spam.abuse.net provides a wealth of information on current efforts to curb spam, as well as practical methods and practices to reduce spam on a given network or spam being passed through a given server. *See Fight Spam on the Internet!* <http://www.spam.abuse.net>. The Forum for Responsible & Ethical E-Mail educates system administrators in ways to reduce spam, educates end-users about how to reduce spam, and lobbies governmental bodies to pass legislation to reduce spam. *See Forum for Responsible and Ethical E-Mail* <http://www.spamfree.org/>. The Coalition Against Unsolicited Commercial E-Mail ("CAUCE") primarily concerns itself with lobbying governments to pass legislation restricting spam. *See Coalition Against Unsolicited E-Mail* <http://www.cauce.org/>. Finally, The Blacklist of Internet Advertisers keeps a regularly updated list of advertisers it deems to have violated netiquette by engaging in such practices as sending unsolicited bulk email. *See Blacklist of Internet Advertisers* <http://www-math.uni-paderborn.de/~axel/BL/blacklist.html>.

cyberspace over the past several years,[13] and we have disagreed before. It is that Lessig considered my view not merely incorrect, but *obviously* and *self-evidently* incorrect. Lessig had placed a "Do Not Enter" sign at the entrance to one path through the jungle of cyberspace policy—a path that I think looks pretty interesting—without any real explanation of why he had done so.[14]

Code, and Other Laws of Cyberspace is that explanation. The theme of *Code*—or at least one major theme of a book filled with complex, interlocking argument—is precisely the one that Lessig articulated in his column: that "[p]olicy-making by the invisible hand"[15] will create a cyberspace in which we will not want to live. There is "no reason," he states at the very beginning of the book,

> . . . to believe that the grounding for liberty in cyberspace will simply emerge. In fact, as I will argue, quite the opposite is the case. . . . *[W]e have every reason to believe that cyberspace, left to itself, will not fulfill the promise of freedom.* Left to itself, cyberspace will become a perfect tool of control. . . . [T]he argument of this book is that *the invisible hand of cyberspace is building an architecture for cyberspace that is quite the opposite of what it was at cyberspace's birth.* The invisible hand, through commerce, is constructing an architecture that perfects control. . . .[16]

Code is, in short, a dense and multi-layered indictment of the invisible hand. Good lawyer that he is, Lessig's argument has the feel of inevitability that the best arguments always have, marching logically and even inexorably from its premises to its conclusion: The accused is guilty as charged. Why then, he asks with frustration and even despair, don't the Net libertarians—those "for whom this point should be most important"—"get it"?[17] How can they "believe liberty will take care of itself"?[18] Why do they seem almost "proud" to "leave things to the invisible hand"?[19] Why don't they see that if

---

13. *See, e.g.*, David G. Post & David R. Johnson, *'Chaos Prevailing on Every Continent': A New Theory of Decentralized Decision-making in Complex Systems*, 73 CHI.-KENT L. REV. 1055 (1998) (available online at <http://www.temple.edu/lawschool/dpost/chaos/chaos.htm>) (responding to Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403 (1996), responding to David R. Johnson & David G. Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996)).

14. This is not meant as criticism; having myself written a fair number of short "popularized" columns about complex issues of cyberspace law over the past several years, I am well aware of the difficulties of sustaining a complete and fully specified argument within the draconian word-length constraints under which Lessig was undoubtedly operating.

15. Lessig, *supra* note 8.

16. Pp. 5-6 (emphasis added).

17. P. 58. The final chapter of *Code* is entitled "What Declan Doesn't Get." Declan refers to Declan McCullagh, a "smart, if young, libertarian" who writes for *Wired News* and runs a popular listserve, and "whose first reaction to any suggestion that involves government is scorn." P. 231. *See also Code and Other Laws of Cyberspace* <http://www.what-declan-doesnt-get.com>.

18. P. 58.

19. P. 234.

we just "do nothing" the invisible hand is poised to bring us a cyberspace that is "less free" than it is today?[20] How can they be so obtuse?

Although I have not been appointed the designated spokesman for the libertarian position—something of an oxymoron, that—I am someone who has, let us say, more sympathy than Lessig for the libertarian position, and I'm happy to take Lessig up on his challenge. I want to suggest here that some of us do *get* it—we even admire it and learn much from it. But we don't *buy* it. We do not fail to understand or appreciate the logic of Lessig's argument; we simply do not accept its premises—premises that are, I suggest below, not as self-evidently true as Lessig might have us believe. One can, in other words, start from a very different set of premises and march just as inexorably to a conclusion that at least casts reasonable doubt on the defendant's guilt.

I. THE IS OF IT

Let us, then, take a careful look at Lessig's argument. He first sets the context: What do we need to know about this new place in order to think clearly about law and governance there? Lessig does not subscribe to the "cyberspace is just like real-space" school of thought; he recognizes that one cannot understand law and governance in cyberspace unless one acknowledges that "something fundamental *has* changed,"[21] that "[c]yberspace presents something new for those who think about regulation and freedom. It demands a new understanding of how regulation works and of what regulates life there."[22]

That something new is the "code" of the book's title. The regulation of human behavior takes place through a complex interaction among four forces, four different "regulators." Three are familiar: law, markets, and social norms.[23] The fourth regulator is what Lessig calls "architecture," the combined constraints of physics, nature, and technology that in the aggregate define the contours of the place(s) where human behavior occurs and the

---

20. P. 109.

21. P. 126.

22. P. 6.

23. *See generally* Pp. 85-99. Lessig illustrates this point using the example of smoking: "If you want to smoke," he asks, "what constraints do you face? What factors *regulate* your decision to smoke or not?" P. 87. The law is one constraint, for there may be laws that prohibit sales to persons under 18, or laws that prohibit smoking in certain places. Norms also constrain, norms that say that one doesn't light a cigarette in a private car without first asking permission of the other passengers, or that one needn't ask permission to smoke at a picnic, or that others can ask you to stop smoking at a restaurant. And the market, too, is a constraint, inasmuch as the price/quality characteristics of the offerings in the market for cigarettes affects your ability and willingness to smoke. *See id*.

thing(s) through which it is expressed. With regard to the smoking example Lessig uses to illustrate the way these regulators work,[24] he writes:

> [T]here are the constraints created, we might say, by the technology of cigarettes, or by the technologies affecting their supply. Unfiltered cigarettes present a greater constraint on smoking than filtered cigarettes if you are worried about your health. Nicotine-treated cigarettes are addictive and therefore create a greater constraint on smoking than untreated cigarettes. Smokeless cigarettes present less of a constraint because they can be smoked in more places. Cigarettes with a strong odor present more of a constraint because they can be smoked in fewer places. In all of these ways, how the cigarette *is* affects the constraints faced by a smoker. How it is, how it is designed, how it is built—in a word, its *architecture*.[25]

Each of these constraints is a "distinct modality of regulation."[26] The constraints are distinct, yet highly interdependent. Regulation of an individual's behavior is the "sum of these four constraints,"[27] and a complete picture of regulatory action must consider all four.

What makes cyberspace a new place is that *its* architecture is, uniquely, defined by its *code*—the design of the hardware and software elements that populate this new place, and of the communication protocols that allow these elements to interact with one another.

> [A]n analog for architecture regulates behavior in cyberspace—*code*. The software and hardware that make cyberspace what it is constitute a set of constraints on how you can behave. The substance of these constraints may vary, but they are experienced as conditions on your access to cyberspace. In some places (online services such as [America Online], for instance) you must enter a password before you gain access; in other places you can enter whether identified or not. In some places the transactions you engage in produce traces that link the transactions (the "mouse droppings") back to you; in other places this link is achieved only if you want it to be. In some places you can choose to speak a language that only the recipient can hear (through encryption); in other places encryption is not an option. The code or software or architecture or protocols set these features; they are features selected by code writers; they constrain some behavior by making other behavior possible, or impossible. . . .

---

24. *See* note 23 *supra*.

25. P. 87.

26. P. 88.

> Changes in any one [of these four regulators] will affect regulation of the whole. Some constraints will support others; some may undermine others.... The constraints are distinct, yet they are plainly interdependent.... Technologies can undermine norms and laws; they can also support them. Some constraints make others possible; others make some impossible. Constraints work together, though they function differently and the effect of each is distinct. Norms constrain through the stigma that a community imposes; markets constrain through the price that they exact; architectures constrain through the physical burdens they impose; and law constrains through the punishment it threatens. We can call each constraint a "regulator," and we can think of each as a distinct modality of regulation.

Pp. 87-88.

27. P. 87.

> In this sense, it too is regulation, just as the architectures of real-space codes are regulations.[28]

It is the *architecture* of these cyber-place(s) that, to a great extent, determines what they *are*, and the architecture of those places is constituted by their code. Lessig embarks on a lengthy anthropology of life in America Online ("AOL") to illustrate this point:

> What makes AOL is in large part the structure of the space. You enter AOL and you *find* it to be a certain universe. This space is constituted by its code. . . . As a member of AOL you can be any one of five people. This is just one amazing feature of the space. When you start an account on AOL, you have the right to establish up to five identities, through five different "screen names" that in effect establish five different accounts. . . . five different personae [one] can use in cyberspace.[29]

It is the code/architecture of this particular cyber-place that gives visitors this "fantastic power of pseudonymity," a power to construct their own identity that "the 'code writers' of real space simply do not give."[30] This is not an isolated example; other features of the code/architecture of AOL similarly determine other aspects of life there:

> There are places in AOL where people can gather; there are places where people can go and read messages posted by others. But there is no space where everyone gathers at one time, or even a space that everyone must sooner or later pass through. There is no public space where you could address all members of AOL. There is no town hall or town meeting where people can complain in public and have their complaints heard by others. There is no space large enough for citizens to create a riot. The owners of AOL, however, can speak to all. Steve Case, the "town mayor," writes "chatty" letters to the members. AOL advertises to all its members and can send everyone an e-mail. But only the owners and those they authorize can do so. The rest of the members of AOL can speak to crowds only where they notice a crowd. And never to a crowd greater than twenty-three. . . .
>
> A third feature of AOL's constitution also comes from its code. This is traceability. While members are within the exclusive AOL content area (in other words, when they're not using AOL as a gateway to the Internet), AOL can (and no doubt does) trace your activities and collect information about them. What files you download, what areas you frequent, who your "buddies" are—all this is available to AOL. These data are extremely valuable; they help AOL structure its space to fit customer demand. But gaining the ability to collect these data . . . . [is] part of the constitution that is AOL—again, a part constituted by its code . . . . [that] gives some but not others the power to watch.[31]

---

28. P. 89 (citations omitted).

29. Pp. 70, 67.

30. P. 68. You can, as Lessig points out, "try in real-space to live the same range of multiple lives . . . But unless you take extraordinary steps to hide your identity, in real space you are always tied back to you. You cannot simply define a different character; you must make it, and more important (and difficult), you must sustain its separation from your original identity." *Id.*

31. Pp. 68-69.

Lessig argues—most persuasively—that these features of AOL's code/architecture *matter* deeply for the kind of life that can be lived there and the experiences that one can have there.[32] Particular architectures allow certain values to flourish while making others difficult or impossible to achieve; they enable certain ways of living while disabling others; they can give expression to some human potentialities while silencing others. Architectures are always like this, he observes, but they are more powerful in cyberspace than elsewhere, for the codes of cyberspace have power that no real-space architectures—indeed, that no other regulator in real-space—can match. *Code can achieve a kind of perfection of control that will render it, in cyberspace, the most powerful regulator of all.*

This point, familiar enough to those who have read Lessig's other works on the law of cyberspace[33] but no less significant for that, is without question of the deepest importance for our thinking about governance and regulation in cyberspace. Lessig asks us to consider the "problems that perfection makes."[34] He illustrates with respect to the set of interests protected in real-space by copyright law:

> Today, when you buy a book, you may do any number of things with it. You can read it once or 100 times. You can lend it to a friend. You can [photocopy] pages in it or scan it into your computer. You can burn it, use it as a paper weight or you can sell it. You can store it on your shelf and never once open it.[35]

Some of these things you can do "because the copyright law explicitly gives you th[e] right," and some of these things you can do because the architecture of real-space makes it well-nigh impossible to stop you from doing them.[36] A book seller "might sell you the book at one price if you promise to read it once, and at a different price if you want to read it 100 times, but there is no way for the seller to know whether you have obeyed the contract."[37] The book seller could commission a police officer to follow you around to enforce this particular bargain, but only at prohibitive cost.[38]

---

32. *See* pp. 69-71; *see also* pp. 82-83 ("How Architectures Matter and Spaces Differ").

33. *See, e.g.*, Lawrence Lessig, *Commons and Code*, 9 FORDHAM INTELL. PROP., MEDIA & ENT. L.J. 405 (1999); Lawrence Lessig, *Constitution and Code*, 27 CUMB. L. REV. 1 (1996/97); Lawrence Lessig, *Intellectual Property and Code*, 11 ST. JOHN'S J. LEGAL COMMENT. 635 (1996); Lawrence Lessig, *The Limits in Open Code: Regulatory Standards and the Future of the Net*, 14 BERKELEY TECH. L.J. 759 (1999); Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869 (1996); Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403 (1996).

34. P. 139.

35. P. 128.

36. *Id.*

37. *Id*.

38. *See Id.*

The code/architecture(s) of cyberspace are, however, not so limited. Although there is "very little in the code as it exists now that regulates the distribution of and access to material on the Net,"[39] the codes can be designed so as to give far greater protection to these works than real-space architectures allow. Various technologies—"trusted systems"—permit a far more "fine-grained control over access to and use of protected material than law permits, and [they] can do so without the aid of law."[40] The code of trusted systems can regulate

> whether you read [a work] once or one hundred times; whether you [can] cut and paste from it or simply read it without copying; whether you [can] send it as an attached document to a friend or simply keep it on your machine; whether you [can] delete it or not; whether you [can] use it in another work, for another purpose, or not. . . .[41]

As Lessig points out, "[t]he power to regulate access to and use of copyrighted material [thus] is "about to be perfected. . . . giv[ing] holders of copyrighted property the biggest gift of protection they have ever known."[42]

So where does that leave us? In a world dominated by code—a world whose contours, and whose values, are shaped by the code. A world in which code can do much of "the work that the law used to do. . . . far more effectively than the law did."[43] A world in which "[c]ode can, and increasingly will, displace law."[44] A world in which "effective regulatory power [shifts] from law to code, from sovereigns to software."[45] A world in which code "displaces law by codifying the rules, making them more efficient than they were just as rules."[46]

Lessig is undoubtedly correct: This is a large, and a most fundamental, change.

> [Cyberspace] demands a new understanding of how regulation works and of what regulates life there. It compels us to look beyond the traditional lawyer's scope—beyond laws, regulations, and norms. . . . In cyberspace we must understand how code regulates—how the software and hardware that make cyberspace what it is *regulate* cyberspace as it is. As William Mitchell puts it, this code is cyberspace's "law." *Code is law*.[47]

---

39. P. 127. *See also id.* ("Given the present code of the Internet, you can't control well who copies what. If you have a copy of a copyrighted photo, rendered in a graphics file, you can make unlimited copies of that file with no effect on the original. When you make the one-hundredth copy, nothing indicates that it is the one-hundredth copy rather than the first. There is very little in the code as it exists now that regulates the distribution of and access to material on the Net.").

40. P. 129.

41. P. 128.

42. P. 127.

43. P. 130.

44. P. 126.

45. P. 206.

46. P. 130.

47. P. 6 (emphasis in original).

That is, one might say, the anthropology, the *is*, of it. To call this portion of Lessig's argument a *tour de force* renders it insufficient praise; the exposition here is truly dazzling, and Lessig has without question made a deeply important contribution to our understanding of law in this strange new place.

II. THE OUGHT OF IT

What, though, of the "ought"? The question remains: If one agrees with Lessig—and I do agree with Lessig—that this is what law looks like in cyberspace, how should we make that law? What kind of "policy-making" is best in a world constituted like this? What does this tell us about MAPS and the RBL?

Lessig begins his normative inquiry just where the libertarians do: by asking what, in this particular time and place and in this new world, "is the threat to liberty, and how can we resist it?"[48] How, he asks, can we best ensure that this is a world where human liberty can flourish? Or, rather, he asks how we can best ensure that this *remains* a world where human liberty can flourish, for he recognizes that the Net as it has come down to us—what he calls "Net95"—has a truly remarkable "architecture of liberty"[49]:

> The architecture of cyberspace makes regulating behavior difficult, because those whose behavior you're trying to control could be located in any place (meaning outside of your place) on the Net. Who someone is, where he is, and whether law can be exercised over him there—all these are questions that government must answer if it is to impose its will. But these questions are made impossibly difficult by the architecture of the space—at least as it was.[50]

These features of the code/architecture of Net95

> do not disable something important from the Net as it was; they enable something important about the Net as it was—liberty. They are virtues of a space where control is limited, and they help constitute that space. The constitution of Net95 is unregulability; these features of its code make it so.[51]

For example, it is the code/architecture of cyberspace, and not the First Amendment, that has been "the real protector of speech there,"[52] for it is the code/architecture that "protects against prior restraint just as the Constitution did—by ensuring that strong controls on information can no longer be

---

48. P. 85.

49. P. 30.

50. Pp. 19-20.

51. P. 28.

52. Pp. 166-67. *See also* p. 166:

> [O]n top of this list of protectors of speech in cyberspace is architecture. Relative anonymity, decentralized distribution, multiple points of access, no necessary tie to geography, no simple system to identify content, tools of encryption—all these features and consequences of the Internet protocol make it difficult to control speech in cyberspace.

achieved."[53] Through the code/architecture of the Net we have managed to "export[] to the world . . . a First Amendment *in code* more extreme than our own First Amendment *in law*."[54]

But that is Net95. The code/architecture of cyberspace can change. What cyberspace *is* is not what cyberspace must be. The "possible architectures of something that we would call 'the Net' are many, and the character of life within those different architectures is diverse."[55] It is not cyberspace's "nature" to be the way it is, or to have the code/architecture it has; we built it that way, and we can build it in a different way. The unregulability of Net95 and the freedom-enhancing values that the Net embodies, are functions of the code/architecture of Net95. Values very different from the freedom-enhancing values in today's code/architecture can be embedded in tomorrow's.[56]

And, Lessig goes on, they will be. Cyberspace, now so largely free from control, will, if we "do nothing,"[57] become a place of *perfect* control, an Orwellian space devoid of the very values of liberty and free expression built into Net95 and that we hold sacred. Why? What will cause this to happen?

Lessig suggests that two forces are aligned to bring this unpleasant world into being. First, the governments of the world, caught off-guard by the explosive growth of the Net, will arise from their slumber.[58] They will come to realize (if they have not yet realized) that the code/architecture of cyberspace holds the key to reasserting the power of their laws in this seemingly unregulable place. Given the code/architecture of the Net as it is, it is difficult for government to regulate behavior on the Net; but given the code/architecture of the Net, it is "not hard for the government to take steps to alter, or supplement, the architecture of the Net [to] . . . make behavior on the Net more regulable."[59] Liberty "depends on regulation remaining expensive"[60]; the current architecture of cyberspace makes regulation expensive; governments will therefore force the architecture to be altered to make regulation less expensive; this will let them reassert control over activities in cyberspace. If the governments of the world can't regulate conduct directly because of the code/architecture of cyberspace, they will "regulate the regu-

---

53. P. 170 (citing Floyd Abrams, *First Amendment Postcards from the Edge of Cyberspace*, 11 ST. JOHN'S J. LEGAL COMMENT. 693, 699 (1996)).

54. P. 167 (emphasis in original).

55. P. 25.

56. P. 60 (noting that where the "basic assumptions" underlying the code of Net95 were "liberty and openness," today "[a]n invisible hand . . . threatens both").

57. P. 109.

58. Pp. 43-60 (Chapter Five: "Regulating Code").

59. Pp. 43-44.

60. P. 56 ("Cost for the government is liberty for us. The higher the cost of a regulation, the less likely it will be pursued as a regulation. Liberty depends on the regulation remaining expensive.").

lability" of cyberspace, forcing changes in that code that will make it a much more regulable place.[61]

This idea is surely *not* what the libertarians "don't get"; this portion of *Code* reads like a kind of libertarian manifesto. Nor does this argument explain Lessig's objections to the RBL; the code/architecture that the proprietors of MAPS have in mind—elimination of open mail relay systems—is not government-backed or government-endorsed in any way (precisely why the libertarians find it attractive).

There must be more to Lessig's argument. And there is. The second of the forces bringing about change in cyberspace brings us to the heart of the matter. Even if the governments of the world are for some reason unable or unwilling to build a code/architecture of perfect control, Lessig continues, the forces of commerce will do it for them.[62] To flourish in cyberspace, commerce requires "architectures of identity"[63]—architectures that "enable identification to enable commerce."[64] With or without government action, these architectures will be added to the Net to make it serve commerce more efficiently; with or without government action, regulability (and the concomitant loss of liberty) will be the by-product of these changes.[65]

Take, for instance, the current battle over the distribution of MP3 audio files.[66] In an earlier time—last year—MP3 was the rage; music enthusiasts by the thousands built websites where every imaginable form of music was available for free downloading. "'Free music' joined the list of free stuff that the Internet would serve."[67] But already the story has changed:

> The recording industry is pushing a standard that would make it easier to control the distribution of these files; Congress has passed a statute that makes it a felony to produce software that evades this control; and one company that produces Sony Walkman–like machines to play MP3 files has already announced plans to enable its machine to comply with these standards of control.[68]

---

61. P. 198 ("[R]eal-space sovereigns . . . will come to see that the power of another sovereign is wired into their telephones, and they will struggle . . . as the rules and norms of this other sovereign affect the behavior of their citizens in their space. They have the tools at their disposal to resist the architecture of the Net to protect their regulatory power.").

62. Pp. 30-42 (Chapter Four: "Architectures of Control"); *see also* p. 30 ("[t]he Net is being remade to fit the demands of commerce . . . [and] [r]egulability will be a by-product of these changes.").

63. Pp. 34.

64. P. 30.

65. P. 58 ("Market forces encourage architectures of identity to facilitate online commerce. Government needs to do very little—indeed, nothing at all—to induce just this sort of development. The market forces are too powerful; the potential here is too great. If anything is certain, it is that an architecture of identity will develop on the Net—and thereby fundamentally transform its regulability.").

66. Lessig discusses this example in his Preface. P. x.

67. *Id.*

68. *Id*.

Lessig's target here is the code/architecture itself; he is equally concerned about efforts by government—"Congress has passed a statute"—and by private parties—"[t]he recording industry is pushing a standard"—to build these control architectures and to use them to regulate our activities in cyberspace.[69]

Once again, this portion of *Code*, has much to teach the libertarians; efforts to impose control over conduct in cyberspace can and will come from many diverse directions, and eternal vigilance is, after all, the price of liberty.

But as it turns out, Lessig's view of "commerce" is an unusual, even a startling, one. There's a small, but I think telling, moment early on in the book where he writes, apropos of government's power to regulate the code of the Net:

> In a world where the code writers were the sort of people who governed the Internet Engineering Task Force of a few years ago, government's power to regulate code would be slight. The underpaid heroes who built the Net have ideological reasons to resist government's mandate. They are not likely to yield to its threats. And unlike some commercial interests, they do not have millions riding on a single architecture winning out in the end. Thus, they would provide an important check on the government's power over the architectures of cyberspace.
>
> *But as code writing becomes commercial—as it becomes the product of a smaller number of large companies*—the government's ability to regulate it increases.[70]

As code writing becomes commercial, it becomes the product of a "smaller number of large companies"? Why is that? Lessig writes of this concentration of economic power as if it were somehow foreordained, an inevitable consequence of commercialization. He has, for example, a propensity towards use of the singular when describing the noisome effects of commerce; the forces of commerce will deploy "an architecture of security,"[71] "a general architecture of trust . . . that makes possible secure and private transactions";[72] encryption will be at the "core of any such architecture";[73] there are "many plans for deploying this architecture,"[74] for such "[a]n architecture" would provide "security greater than the best security in

---

69. Lessig thinks very little of the distinction that the law on occasion draws between "public" and "private" action. Pp. 186-87, 213-21 (developing argument that constitutional limitations should be applied to private conduct as well as to "state action").

70. P. 52 (emphasis added) (footnote omitted).

71. P. 40.

72. *Id.* (citation omitted).

73. P. 41.

74. *Id*.

real space";[75] unless and until "such an architecture is established," online commerce will not fully develop.[76]

Commerce drives towards uniformity. While the nations of the world "argue about what regulation there should be," commerce is moving cyberspace towards

> . . . a *fairly unified regulation* through code while law remains in flux. . . . Just as there was a push toward convergence on a simple set of network protocols, there will be a push toward convergence on a *uniform set of rules* to govern network transactions. This set of rules will include not the law of trademark that many nations have, but a *unified* system of trademark, *enforced by a single committee;* not a diverse set of policies governing privacy, but a *single set of rules*, implicit in the architecture of Internet protocols; not a range of contract law policies, implemented in different ways according to the values of different states, but a *single, implicit set of rules* decided through click-wrap agreements and enforced where the agreement says.[77]

That's a rather strong premise, it seems to me, and it appears to undergird much of Lessig's argument about what we have to fear. I say "appears," because as a proposition it is not always explicitly stated (or defended); but much of what Lessig writes makes little sense without it. For instance, he writes of the deployment of "trusted systems" for intellectual property:

> [W]hat happens when code protects the interests now protected by copyright law? What happens when . . . what the law protects as intellectual property can be protected through code? Should we expect that any of the limits [now provided by copyright law] will remain? Should we expect code to mirror the limits that the law imposes? Fair use? Limited term? Would private code build these "bugs" into its protections?
>
> *The point should be obvious*: when intellectual property is protected by code, *nothing requires that the same balance be struck.* Nothing requires the owner to grant the right of fair use. She might, just as a bookstore allows individuals to browse for free, but she might not. Whether she grants this right depends on whether it profits her. Fair use becomes subject to private gain.[78]

Why is that so—that word again!—"obvious"? True, if there are a "small[] number of large companies"[79] dominating the production and distribution of intellectual property, "nothing requires"[80] them to provide consumers with the ability to browse for free. And if there are a "small[] number of large companies" dominating the production and distribution of intellectual

---

75. *Id*.
76. *Id*.
77. P. 206 (emphasis added).
78. P. 135 (emphasis added).
79. P. 52.
80. P. 135.

property, when the "controls . . . are built into the systems," "no users (except hackers) have a choice about whether to obey these controls."[81]

But if there are many different architectures, then there *is* choice about whether to obey these controls. If there are multiple architectures from which to choose, it is no longer correct to say that "nothing requires" booksellers to provide users the ability to browse for free; the market for bookstores, the existence of competing bookstores, and consumers' desire to browse do so.[82] It is hardly nothing; these are the very same things that "require[]" the real-space booksellers that Lessig mentions to allow you to browse for free.[83] And if there are diverse architectures of privacy, of iden-

---

81. P. 130.

82. To return, for the moment, to Lessig's example of MP3 audio files, see text accompanying note 66 *supra*, there are any number of digital music formats available in addition to MP3. Schemes for the protection of digital music abound. Perhaps the most widely adopted non-MP3 format is Microsoft's Windows Media Audio (WMA). Microsoft has positioned the WMA format to be suitable for all sorts of audio applications, including distribution of music files and streaming applications, e.g., live broadcasts of "radio" shows over the Internet. *See* Starr Andersen, *About the Windows Media Audio Code* <http://www.msdn.microsoft.com/workshop/imedia/windowsmedia/Tools/MSAudio.asp>. Recently, Sony announced it would utilize the WMA format for the distribution of digital audio from its "bitmusic" website, coupling WMA with IBM's Electronic Music Management System ("EMMS") for the protection of copyrights. *See* Yoshiko Hara, *Sony Skips MP3 as It Spins Web Music Service*, EE TIMES, Issue 1092 (Dec. 20, 1999) <http://www.techweb.com/se/directlink.cgi?EET19991220S0009>. Sony has also created a digital rights management system consisting of "MagicGate" and "OpenMG" components, which limits where and how many times a given song may be copied. *See Sony and RealNetworks Announce Strategic Alliance for Secure Electronic Music Distribution* (Jan. 7, 2000) <http://www.realnetworks.com/company/pressroom/pr/00/sony.html>. IBM's EMMS system is based on an architecture that includes a "clearinghouse that authorizes and processes transactions. . . . [thereby providing] a highly secure rights management capability." *IBM and Major Record Companies to Test Internet Music Distribution* <http://www.ibm.com/news/ls/1999/02/mu_intro.phtml>. AT&T has developed what it calls its "a2b" technology, based on the MPEG Advanced Audio Coding specification. *See AT&T's a2b Music Delivers Highest Sound Quality for Digital Music Distribution* <http://www.att.com/campusalliance/a2bmusic.html>. The a2b format compresses music files using proprietary algorithms which can "compress music at ratios up to 20:1 without perceptual loss of quality" and uses the "CryptoLib Security Library," which utilizes various encryption algorithms including the RSA and DES algorithms for copy management. *a2b Music Technology* <http://www.a2bmusic.com/technology.asp>. RealNetworks has utilized still other strategies to protect and distribute music over the Internet, including the development of its own "G2" format. When RealNetworks introduced its "Real Jukebox" product, it included a tethering technology whereby digital copies of tracks from audio CDs were limited to single copies, unless the user turns off the protection system. *See* John Markoff, *New System for PC Music Stirs Concern Over Piracy*, N.Y. TIMES, May 3, 1999, at C1. RealNetworks recently announced that it would incorporate a digital rights management system from InterTrust Technologies into its secure digital format. *See* Lessley Anderson, *Secure Online Music: To Be or Not to Be?*, THE INDUSTRY STANDARD (May 5, 1999) <http://www.thestandard.com/article/display/0,1151,4473,00.html>. Other significant protection schemes include technologies from Bell Laboratories, Blue Spike Inc., Aris Technologies, Cognicity, and Solana Technology Development Corp. *See* Junko Yoshida and Margaret Quan, *Groups Debate Security Technology for Internet, DVD Audio—Watermark Wave Cresting*, EE TIMES, Issue 1052 (March 15, 1999) <http://www.techweb.com/se/directlink.cgi?EET19990315S0004>.

83. Similarly, Lessig writes that although you can "resist" the code imposed on you by America Online,

tity, and of content protection laid before the public, why is it so obvious that we will end up choosing the one(s) that deny us those things that Lessig (and I) think are so important?[84]

Lessig's notion that the invisible hand of commerce somehow drives towards uniformity may be correct,[85] but it is surely not *self-evidently* correct. The invisible hand may have many deficiencies, but the one thing that it does best—far better than any alternative of which I am aware—is to place before members of the public a diverse set of offerings in response to the diverse needs and preferences of that public. And it seems to be working rather well, thank you very much. When I gaze about the Net—even at those portions of the Net that have been invaded by the forces of "commerce"—I see something that looks more like the chaos of unchecked growth and diversity than it does uniformity and regularity. It is not just that new websites, and new architectures with them, seem to be sprouting like mushrooms after a spring rain; they actually *are* sprouting like mushrooms after a spring rain.[86]

Let me be clear on this point. Libertarians "get" the point that concentrations of power are dangerous and are to be resisted. Lessig is free to make the assumption that when left to themselves, the forces of commerce produce

---

> just as you can resist cold weather by putting on a sweater, . . . you are not going to change how [the code] is. You do not have the power to change AOL's code, and there is no place where you could rally AOL members to force AOL to change the code.

P. 70 (emphasis added). But unless AOL is in a highly unusual and non-functioning market, you *do* have the power to "change AOL's code"; the market gives you—consumers, in the aggregate—that power, even without a "rally."

Lessig's colleague Andrew Shapiro, another member of this so-called "techno-realist" school of thought, seems to have a similar view of the uniformity towards which the forces of commerce inevitably lead. In *The Control Revolution*, a book that echoes many of the themes in *Code*, Shapiro writes that the Net's "potential for individual empowerment and unfettered citizen interaction" will not be fulfilled "unless it is characterized by a strong degree of diversity and fortuity"—as if that were not already the case. ANDREW SHAPIRO, THE CONTROL REVOLUTION: HOW THE INTERNET IS PUTTING INDIVIDUALS IN CHARGE AND CHANGING THE WORLD WE KNOW 203 (1999).

84. *See* Tom W. Bell, *Fair Use Vs. Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine*, 76 N.C. L. REV. 557 (1998) (making this argument with specific reference to fair use).

85. I am not unaware of the idea that the codes of cyberspace may be subject to powerful "network externalities" which can, in some circumstances, promote "winner-take-all" markets. *See generally* Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CAL. L. REV. 479 (1998).

86. *See* Réka Albert, Hawoong Jeong, and Albert-László Barabási, *Diameter of the World-Wide Web*, 401 NATURE 130 (1999); Bernardo A. Huberman and Lada A. Adamic, *Growth Dynamics of the World-Wide Web*, 401 NATURE 131 (1999) (demonstrating that the growth of websites, and of links among websites, follow quite precisely the mathematical distribution that characterizes growth in biological populations); *see generally* David G. Post & Michael B. Eisen, *How Long Is the Coastline of the Law? Thoughts on the Fractal Nature of Legal Systems*, 29 J. LEGAL STUD. 545 (2000) <http://www.temple.edu/lawschool/dpost/fractals.pdf> (discussing the general significance of these "power law" distributions for the study of social and biological systems).

such concentrations of power. But that hardly satisfies his burden of persuasion, and he should not be surprised that those who find his assumption unreasonable are also skeptical of his program.

To be fair to Lessig, this assumption is not the primary foundation of his indictment of the invisible hand. Even if, Lessig argues, the invisible hand were somehow able to provide a multiplicity of code/architectures for this new world, it is still guilty; even if the invisible hand were to provide us with choices among the different possible code/architectures of cyberspace, it is the wrong mechanism for us to make those choices. Lessig's argument proceeds as follows: (a) these code/architectures of cyberspace embed fundamental, sometimes even "constitutional," values; (b) to choose among them is, therefore, to make deeply important choices among different values; and (c) the choice among values is the stuff of politics, not markets.

> Ordinarily, when we describe competing collections of values, and the choices we make among them, we call these choices "political." They are choices about how the world will be ordered and about which values will be given precedence.
>
> Choices among values, choices about regulation, about control, choices about the definition of spaces of freedom—all this is the stuff of politics. Code codifies values, and yet, oddly, most people speak as if code were just a question of engineering. Or as if code is best left to the market. Or best left unaddressed by government.
>
> But these attitudes must be mistaken. *Politics is that process by which we collectively decide how we should live*. That is not to say a space where we collectivize—a collective can choose a libertarian form of government. The point is not the substance of the choice. The point about politics is process. Politics is the process by which we *reason* about how things ought to be.[87]

Lessig suggests that "we should not accept the idea that *any part* of what defines the world as it is, is removed from politics."[88] We need, Lessig says, "a plan";[89] the "architecture of cyberspace is up for grabs"—note again the use of the singular[90]—and, "depending upon who grabs it, there are several different ways it could turn out."[91] There are *choices* to be made; "[c]learly[,] some of these choices are collective—about how we collectively will live in this space."[92] We can stand by and "do nothing" as these choices are made "by others," or we can "try to imagine a world where [these choices] can again be made collectively, and responsibly."[93]

---

87. P. 59 (first emphasis added).

88. *Id.* (emphasis added).

89. P. 222.

90. *See* text accompanying notes 71-78 *supra* (noting Lessig's use of rhetoric of a single, uniform "architecture").

91. P. 219.

92. *Id.*

93. P. 220.

And this, he tells us, is just what governments are for; governments, properly constituted, are the means by which we make, fairly and equitably (one hopes), collective decisions of this kind. Contra the Net libertarians, we need more, not less, government in cyberspace if those collective values are to prevail:

> We stand on the edge of an era that demands we make fundamental choices about what life in this space . . . will be like. These choices will be made; there is no nature here to discover. And when they are made, the values we hold sacred will either influence our choices or be ignored. The values of free speech, privacy, due process, and equality define who we are. If there is no government to insist on these values, who will do it?[94]

Here, then, is the heart of the heart of the matter. This, finally, explains Lessig's aversion to MAPS, and to the RBL, and to the whole "policy making by the invisible hand" enterprise; it is not reasoned, it is not deliberative, it is not "political," it is not made by a collective process capable of expressing collective values.

The source of our disagreement here is now clear. I have no quarrel with the notion that the code/architectures of cyberspace embed fundamental values, and I have no quarrel with the notion that each of us, confronting the design of these new cyberplaces, faces a choice among different values. It does indeed matter, as Lessig says, whether the code of a cyber-place permits us to be anonymous or not, tracks our mouse droppings or not, allocates to us one screen name or ten, allows us to gather in groups of 20 or 50 or 500, or exposes us to many or to no random encounters.

But I do quarrel with the notion that the choices to be made among value-laden architectures are therefore "political" decisions that should necessarily be subject to "collective" decisionmaking. Consider, by way of counterexample, the original, and still probably the most powerful, value-laden code/architecture of them all: the English language.[95] The semantic and syntactic structures of English (and of all natural languages) are deep *architectural* constraints on our social life, as the crits (and, indeed, Lessig himself[96]) have been fond of pointing out (and, as it should in fairness be noted, the anthropologists have known for a while[97]). Language is not just "a

---

94. *Id.*

95. Any natural language would, of course, serve equally well in this example.

96. *See* Lawrence Lessig, *The Regulation of Social Meaning*, 62 U. CHI. L. REV. 943 (1995).

97. The classic statements of this view—that every language binds the thoughts of its speakers by the involuntary patterns of its grammar, and that we experience the world as we do because the structures of our language predisposes us towards certain interpretations of phenomena in the world—are in EDWARD SAPIR, LANGUAGE: AN INTRODUCTION TO THE STUDY OF SPEECH (1921); SELECTED WRITINGS OF EDWARD SAPIR IN LANGUAGE, CULTURE AND PERSONALITY (David G. Mandelbaum ed., 1949); and the works of Benjamin Whorf. *See* BENJAMIN LEE WHORF, LANGUAGE, THOUGHT, AND REALITY: SELECTED WRITINGS OF BENJAMIN LEE WHORF (John B. Carroll ed., 1956).

way of communicating propositions about the world," it is "a constitutive social activity," a means by and within which we "construct social reality."[98] Like the network protocols they so closely resemble,[99] these semantic and syntactic structures embed important and often fundamental values throughout.

Each of us, therefore, has *choices* to make, choices about how our own personal architectures of social reality will be constituted. Notwithstanding powerful "network externalities" in any linguistic system, in which we each gain communicative power when we adopt more "interoperable" rules, the world persists in presenting us with an imposing array of diverse and distinctive linguistic variants. Linguistic communities, subcommunities, sub-subcommunities, and so on, each with its own shared architecture, form and dissolve around us all the time. We can (and should) argue about the ways in which particular linguistic architectures constrain our social worlds; we can (and should) subject the meanings of these code/architectures to discussion, debate, and deliberation; we can (and should) think carefully about the choices each of us has to make about which communities we want to join and which we want to avoid.

But now *I* get to assert the obvious. I take it as obvious that we do not, and that we should not, subject those semantic and syntactic structures *to the collective* for decision-making. English will evolve best not by subjecting it to a series of decisions by the collective empowered to impose its will on all, but by an aggregated series of individual and sub-group decisions. We do not have, and we do not want, the Ministry of Semantic Propriety, or our elected representatives, or a specially constituted board of experts, or even the law professors, to make a "plan" about the proper direction(s) that English may take or to make decisions for us in accordance with that plan. We do not, in fact, have or need a "plan" at all. We are, and should be, deeply suspicious of those who claim to have such a plan, and positively terrified of those who assert that they need to enlist the coercive powers of the State to implement that plan. If there is a serious alternative to the invisible hand that is suitable for this task, I am not aware of it.

Interestingly enough, Lessig disagrees—or so I read his earlier work, where he argues that the construction of language is indeed a "collective enterprise," that linguistic change "requires a collective effort" to solve the "collective action problem,"[100] and that the "collective must act together to effect [linguistic] reform."[101] This is not the place to continue that argument;

---

98. Lessig, *supra* note 96, at 976.

99. We should not lose sight of the fact that when we talk of the codes of cyberspace we are talking, when all is said and done, about truly *linguistic* constructs, built out of the new languages—Java, HTML, C++, and the like—of the digital age.

100. Lessig, *supra* note 96, at 1000.

101. *Id*. at 1007.

my goal here is merely to point out that it exists, and that it is, at bottom, the basis for our disagreements about cyberspace, and about MAPS.

For it is true: I am as dubious about the need for more politics to help devise the plan for the codes of cyberspace as I am dubious about the need for more politics to help devise the plan for the codes of English. This is not to advocate "doing nothing"; it is to defend the idea that decisions about the contours of the language we speak are best made by individuals and not by collectives. This is not to view English as "the product of something alien—something we cannot direct because we cannot direct anything[, s]omething . . . that we must simply accept, as it invades and transforms our lives"[102]; rather, it is to express the belief that the shape of the English language will best emerge not through politics and political processes, but as the aggregate outcome of uncoerced individual decisions. This is not "knee-jerk antigovernment rhetoric,"[103] the "pathology of modern politics" that is "so disgusted with self-government that [its] automatic response to government is criticism."[104] If there is a "patholog[ical]" position here it is, I suggest, the contrary one, for the history of "collective control" over the use and deployment of natural languages is an ugly one; ask the Armenians, or the Basques, or the Irish, or the Navajo.

Perhaps I am wrong, but I think I am not alone in this view. Lessig could do worse than starting here if he is interested in uncovering why so many people seem not to accept his argument.

III. COMMON GROUND

Lessig's argument is an elegant structure, with powerful timbers connecting its many parts together. It is, though, built on a patch of ground that is, and remains, rather far from the ground occupied by the Net libertarians. The gap separating the two encampments—let's call it "Liberty Gap"—is a substantial one. Lessig's calls for "collective action" are unlikely to entice those of us for whom liberty is a *paramount* value over to the Other Side. "Collective action," after all, is another way to denote the use of coercive force to bind some portion of the polity to act in ways that *others* think necessary for the common good; we might be forgiven for hearing not-entirely-liberty-enhancing overtones in those calls. Lessig himself points out that while sometimes the values of the collective action are "values of liberty," sometimes they are not; sometimes they must "deny or restrict liberty in the name of some other value that is weighed more strongly than liberty."[105] Those are not comforting words, at least to those of us on this side of Liberty Gap.

---

102. P. 233.

103. P. xi.

104. P. 209.

105. *Id.*

Before we move into Lessig's structure, we would like to know a bit more about how this collectivization process is going to work. It's just a thing we have; the first question we like to ask about structures of this kind is whether the "Constraints on the Exercise of Collective Power" wing has been completed. Lessig, though he acknowledges the need for such a wing,[106] does not give us any details about what it might look like, no sense of how the political power he seeks to impose on the Net is to be constrained. It is, I think, not enough to entice us to leave what we regard as safer ground.

I do not want to suggest that this gap between the two positions is unbridgeable, for that is clearly not the case. The truth, inevitably if somewhat anti-climactically, lies somewhere in between the rather more extreme positions to which rhetoric often confines us. Just as Lessig recognizes the need for constraints on collective power, the conscientious libertarian recognizes that there are times when collective action *is* required to promote the common welfare, that the government, while not always the answer, is not always the enemy, and that deliberation need not always be de-liberating.[107] Architectures of liberty *are* of fundamental importance. They arise only as the product of human action. They have always been, and will always be, under attack from many directions; if we, in the aggregate, "do nothing," we will get nothing (or worse) in return. On these points we agree, and Lessig has much to say that libertarians would be wise to heed about the ways in which these principles manifest themselves in cyberspace.

There is thus a building project at hand; cyberspace needs architectures where deliberation and reason and freedom can flourish, because—we both believe—people want to live in communities where deliberation and reason and freedom can flourish.[108] We can disagree about the extent to which the coercive power of the State needs to be invoked in order to get those communities built and to get people to live there. But we do not disagree about the need to build them. So let the building begin (or is it "continue"?).

---

106. P. 208 ("I am not a statist. I don't think the best of us is given to us from top-down. There is a proper space for collective life, and an important space for private life. A good constitution helps us navigate that balance.").

107. Talk about the architecture of English! As it turns out, the seeming opposition between "liberation" and "deliberation" is just an ironic semantic coincidence. The two words appear to have been derived independently from different roots, the former from the Latin *liber*, to set free (and related to the Roman god of growth, *Liber*), the latter from the Latin *librare*, to balance (hence *Libra*, the scales). *See* ERIC PARTRIDGE, ORIGINS: A SHORT ETYMOLOGICAL DICTIONARY OF MODERN ENGLISH 352 (1958).

108. See, for example, Lessig's eloquent defense of open source software in Chapter 8, which stakes out a position that many libertarians can (and should) heartily endorse.