CORDELL HULL SPEAKERS FORUM*

CONSTITUTION AND CODE

LAWRENCE LESSIG**

I begin with a story, an observation, and an idea, as an introduction to an argument about cyberspace and the Constitution.

The story is this: Before the revolution, the Czar in Russia had a system of internal passports. These passports marked the estate from which you came, and your estate determined where you could go, and with whom you could associate. They were badges that granted access, or barred access. They determined what in the Russian state Russians could come to know.

The people hated these passports, and the Bolsheviks promised to abolish them. Soon after their rise to power, they did. Russians were then free to travel where they wished. Where they could travel was not determined by some document. The abolition of the internal passport was a mark of freedom for the Russian people.

A decade-and-a-half later, however, faced with the prospect of starving peasants flooding the cities looking for food, Stalin brought back the internal passport system. Peasants were then again tied to their rural land (a restriction that remained throughout the 1970s). And once again, Russian citizens were restricted to where their passport allowed.

That's the story. The observation is much shorter: We have specialized statutes about auto theft, and airplane theft, and theft of boats. We don't have specialized statutes about the theft of skyscrapers. Skyscrapers pretty much take care of themselves. Though valuable, and though value usually attracts crime, wonderfully (for owners of skyscrapers at least), the theft of skyscrapers isn't much a problem.

Finally the idea: Behavior in the real world is regulated by three sorts of constraints. The first is the constraint of law—laws order me to behave in certain ways; if I disobey the

---

* This essay was delivered at the Cordell Hull Speakers Forum at the Cumberland School of Law, November 21, 1996.

** Professor, University of Chicago Law School. B.A., B.S. 1983, University of Pennsylvania; M.A. Phil. 1986, Cambridge University; J.D. 1989, Yale Law School.

law, I'm likely to be punished. The second is the constraint of social norms—understandings or expectations about how I ought to behave, enforced not through some centralized norm enforcer, but rather through the understandings and expectations of just about everyone within a particular community. The third is the constraint of nature—of the world as I find it, which requires that I do certain things whether I want to or not; the constraints that demand, for example, that when I, unlike the Road Runner, step off a cliff, I will fall.

These three constraints combine, in the real world, to regulate behavior. Think, for example, about the protections for privacy. At the core is the protection of law, primarily in the Fourth Amendment. It, plus a host of other law, regulates the police, for example, in their decision to search my house. Social norms as well might protect privacy: ideas of politeness, for example, or appropriateness, may make the police search less invasive, or less likely. And finally, nature helps protect my privacy—police, unlike Superman, don't have x-ray vision, so they can't simply look through my walls to see what sorts of stuff I have on the other side. Thus laws, and norms, and constraints of the real word—what I've called nature—all combine to define the scope of my freedom. Changing any one will change the scope of my freedom.

Of course, *how* law and norms constrain behavior in the real world differs from how nature constrains behavior in the real world. One chooses whether to obey laws or norms; it's possible, that is, to imagine disobeying them. One doesn't choose to obey the constraints of nature. One doesn't stand before a wall and say, "Nature, I understand your laws mean that I can't see what's going on inside, but I choose to defy your laws, and see inside anyway." The laws of nature are in this sense non-optional, while the laws of man, and the norms of man, are.

Thus the idea. Now I want to use this story, and this observation, and this idea, to say something about cyberspace. You've heard lots of hype about the amazing place that cyberspace is, about all the things that cyberspace can do, about the virtual lives that cyberspace permits, and about the real lives that cyberspace has destroyed. But there's another view of cyberspace that my story, and observation, and idea, might focus.

Think first about the idea—about the three constraints on behavior. For just like the real world, behavior in cyberspace too is regulated by three sorts of constraints. There is law in

cyberspace—copyright law, or defamation law, or sexual harassment law, all of which constrain behavior in cyberspace as they constrain behavior in real space. There are also, perhaps quite surprisingly, norms in cyberspace—rules that govern behavior, and expose individuals to sanction from other people in cyberspace.

But most important for the purposes of what follows, there is something like nature in cyberspace—something that functions, at least, like nature, in cyberspace, in that like nature, for the most part, we simply live life in cyberspace subject to its terms.

This third constraint is *code*—the software that constitutes cyberspace as it is. This code, like nature, sets the terms upon which I enter, or exist in cyberspace. It, like nature, is not optional. I don't choose whether to obey the structures that it establishes—hackers might, but hackers are special. For the rest of us, life in cyberspace is subject to the code of cyberspace, just as life in real space is subject to the code of real space.

An example might better make this point. We might imagine three ways that America Online (AOL) could go about requiring that people, when they come into America Online, identify who they are. One way would be for customers to promise, in their contract with AOL to identify themselves when they enter, say, a chat room. The software then would simply ask, "Who are you?" and the user would be required to say, "I am X." If AOL discovered that users were not identifying themselves properly—if they were breaching their agreement to identify themselves like this—then AOL might, say, sue the users for breach of contract. This would be a constraint of law.

A second way that AOL might get users to identify themselves would be through a norm of self-identification. Netiquette for AOL might require that "users are expected to identify themselves as they enter a public space." Then if someone failed to self-identify, other users might complain to that person, or criticize that person, or "flame" that person. Whatever the remedy, it would be a remedy imposed by a decentralized community of norm-enforcers—what, in big cities we might call busybodies, in small towns, neighbors.

Now these two ways of enforcing this rule are both different from a third. These two ways (again through law or norms) are voluntary, in just the sense that it is relatively easy for an individual not to do as the rule requires. No doubt, not

to do as the rule requires would entail costs—the threat of suit, or the burden of being "flamed." But freedom doesn't mean the right to live without consequences. Freedom here just means the ability to do something other than what is required. And with law, and norms, there is that ability.

But with code, there is not. For again, there is a third way that AOL could require that people identify themselves as they enter AOL: through a sign-on screen that requires accurate self-identification. Through, that is, code. The software could ask for one's name and password, and check them against a verified list, and then allow one to enter only if one had given a proper name with a proper password. If one didn't obey, one wouldn't get in. This is a constraint like law and norms, for it is again a requirement. But unlike law and norms, it is a perfectly effective constraint. This is the nature of a constraint of code. One lives in AOL, or anywhere else in cyberspace, subject to the rules of its code, in a sense, much stronger than the sense in which one lives subject to the laws or norms.

Code, then, is a more efficient system of regulation than laws or norms are, in just the sense that it can assure compliance to a far greater degree than laws or norms do. And it is also more plastic: for the rules that are imposed by AOL through the code are rules that could be changed, simply by changing the code. It is a different kind of regulatory tool—as if the government were given the laws of nature to change through democratic politics. And it raises different kinds of questions for a constitutional regime. How, then, from the perspective of the Constitution, should we understand it? How do we read the Constitution in an era of code?

In one sense, this problem is not new. It is the problem of reading the Constitution in changed circumstances. How we do that should be fairly clear. One method is *translation*,[1] and one good example of this method is *Olmstead v. United States*.[2]

The question in *Olmstead*, presented in 1928, was whether wiretapping was within the scope of the Fourth Amendment.[3] Said the Court, it was not.[4] When the Constitution was

---

[1] Paul Brest, *The Misconceived Quest for the Original Understanding*, 60 B.U. L. REV. 204, 218 (1980). *See generally* Lawrence Lessig, *Fidelity in Translation*, 71 TEX. L. REV. 1165 (1993).

[2] 277 U.S. 438 (1928).

[3] *Id.* at 466.

[4] *Id.*

enacted, said Chief Justice Taft for the majority, the Fourth Amendment was intended to limit trespass on property; that was the common law origin of the amendment;[5] wiretapping a public phone is not a trespass.[6] Therefore, concluded Taft, wiretapping did not invade the Fourth Amendment's interests.[7]

Justice Brandeis saw the case differently. Of course the Fourth Amendment originally protected against trespass, but this was because trespass was the only effective way that the state could invade privacy interests.[8] Sure, it could eavesdrop without trespassing, so it could, in some sense, intrude without constitutional violation; but eavesdropping was of minuscule significance at the founding since police were nonexistent. And in any case, it was not as significant as the invasion that would be permitted if the government could tap phones without limit. For even in 1928, much of life had moved onto the wires; and in these first steps into cyberspace, Brandeis argued, the Constitution should not leave citizens exposed. What had changed, Brandeis wrote, was a technology of surveillance and a technology of communication.[9] Life was now in cyberspace, and the Constitution should be read to protect the very same interests of privacy in cyberspace, changes in technology notwithstanding.[10]

If there is a justice who deserves C-world's praise, if there is an opinion of the Supreme Court that should be the model for cyberactivists in the future, if there is a first chapter in the fight to protect cyberspace, it is this justice, and this opinion, and this case. Here, in as clear an example as any, is a method that will be central to cyberspace's survival as a place where values of individual liberty are sustained. Brandeis worked first to identify values from the original Fourth Amendment, and then second, to *translate* these values into the context of cyberspace. He read beyond the specific applications the

---

[5] *Id.* at 463.

[6] *Id.* at 464-65.

[7] *Id.* at 466.

[8] As Brandeis wrote, "When the Fourth and Fifth Amendments were adopted, 'the form that evil had theretofore taken,' had been necessarily simple." 277 U.S. at 473.

[9] *Id.*

[10] Brandeis's fears were well stated: "Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home." *Olmstead*, 277 U.S. at 474.

framers had in mind, to find the meaning they intended to constitutionalize; and he found a way to read the Constitution in the context of 1928 to preserve that meaning. Brandeis taught us to translate the framers' values into our interpretive context, in a way that had an extremely strong claim to constitutional fidelity.

No doubt, this method of translation, as a method of constitutional interpretation, can do much to preserve founding values in changed circumstances. But it won't do it all. And what I want to argue today is that the change that cyberspace brings—in particular, this change of regulation through code—is not a change we understand well. My claim is that our ideas, or intuitions, about how to preserve the space of liberty that our framing document left, do not translate well when confronted by code. Code confuses us.

I want to make this point with three examples that will tie quite directly with the story, and the observation, and the idea, that I began with. The first links with the idea, the second with the observation, and the third with the story.

First the idea: There's a problem in cyberspace, not really different from the same problem in real space, of contraband on computers. Contraband here could mean illegal pornography (obscenity or child pornography); it could mean illegal trade secrets, stolen from another machine; or it could mean illegally copied software, stored and used on an individual's machine. Focus on the third. Let's say the FBI wanted to locate and prosecute, people who had, say, illegal copies of WordPerfect software stored on their machine. What could the FBI do?

In the real world, law and norms constrain the FBI in its objective. Congress would not be able to pass a law that said, for example, that the FBI could send an agent to every machine in America, and search the hard disk for illegal copies of WordPerfect. That would be a "general search" without particularized suspicion, plainly illegal under the Fourth Amendment.

Nor could the FBI hope to create a social norm to help it achieve its objectives—a norm, say, that people voluntarily open up their hard disks for the government's search. Perhaps there are places in the world where the government would be so trusted. My country is not such a place.

So law, and norms, would fail. But what about this:[11] Say the government wrote a "worm"—a tiny bit of code that was able to propagate itself across the network, and put itself on hard disks on the network. This worm would then scan the hard disk, and look for illegal copies of WordPerfect. If it found an illegal copy, it would send back to the FBI a message: on this disk, there is contraband. If it didn't find an illegal copy, it would destroy itself. The worm would have, let's assume, no effect on the functioning of the disks its scanned; and it would search only for contraband.

Would the worm be constitutional? When I've asked this question to lawyers and law professors who've indulged me my story, I get two very different responses—each given with equal vehemence. On the one hand, there's response best expressed by a colleague who was a former official at the Justice Department: of course, the worm is constitutional. The worm is nothing more than a dog sniff, but better, because one doesn't know one's being sniffed. It sniffs out contraband only; one hasn't the right to have contraband; so it interferes with no right of the individual at all.

And then on the other hand, there's other reply—also given with vehemence. Of course, the worm is unconstitutional; it's just a general search performed by a computer. But the protection against general searches was not a protection limited to general searches by police; it was a protection against general searches. Translating the protections of the Fourth Amendment to the cyber age, these Brandeis-like jurists might argue, requires that we protect against computer searches just as we protect against searches of people.

Which answer is correct, I confess, I don't know. For this is a genuinely hard case. It is hard case because the search by code is in some ways like a general search, and in some way not. It is like a general search because it searches without suspicion; but it is unlike a general search because it's a search that has none of the collateral costs of a general search. Because we can define the code however we wish, we can assure that the code imposes none of the collateral costs of a generalized search. And we can assure this, again because code is more efficient and more plastic than laws or social norms.

---

[11] My example is drawn from Michael Adler, *Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search*, 105 YALE L.J. 1093 (1996).

And so are we pressed back to a fundamental question about what the Fourth Amendment was really about. Was it about protecting against the burdens of suspicionless searches? Or was it about limiting the scope of permissible searches, because it was about limiting what the government could regulate?[12] If the former, then the worm is constitutional; if the latter, then it is not. But the question is which, and more profoundly, what within our tradition will answer this question?

Consider now a second case, not a constitutional case, but a case raising a similar question, tied to my observation about skyscrapers. The law of copyright protects some forms of intellectual property. It gives to the author of this intellectual property the right to control the production, or better, reproduction, of that property. The copyright holder, for example, can forbid others to copy her work, except if they pay the copyright holder. But this right is subject to some important limitations: most important is the limitation of fair use. Regardless of the copyright holder's wishes, the public has the right to use the copyright protected property, for certain purposes, in certain limited ways. I can, for example, excerpt a bit of the copyrighted work and use that excerpt in an article criticizing that work.

Now we need a law like copyright law in the real world, because, like airplanes, and cars, and boats, intellectual property is so easy to steal. With the advent of Xerox machines of very high quality, it becomes very easy simply to copy, for example, a book rather than paying the publisher for another copy. Books, unlike skyscrapers, don't take care of themselves. Without the threat of prosecution, or without a social norm frowning on copying without paying, it would be very hard for producers of intellectual property to recover an adequate return from their investment.

But what if we could change the physics that govern airplanes, or cars, or boats, or books? What if we could make them as difficult to steal as skyscrapers are? Would we have anymore a need for *copyright* protected by law?

Well, again, in the model I've suggested, code is the analog for nature. And so when we ask, what if we could change the laws of nature to make it impossible to steal

---

[12] This is William Stuntz's understanding. *See* William Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393 (1995).

intellectual property, we are asking whether it is possible to make the code such that stealing intellectual property would be extremely difficult.

Think again about code. Initially, one might think that cyberspace is a place that needs more copyright protection, not less. For if it's easy to copy a book with a Xerox machine, it is much easier to copy a digital image on the network using a simply copy command. Indeed, the problem is much worse, since a Xerox copy, however good, is always inferior to an original, while a digital copy is identical to the original.

This fact about digital copying has panicked many holders of intellectual property, and their panic has been registered by the government. In particular, it has been registered in the government's WhitePaper on intellectual property.[13] The WhitePaper calls for changes in the copyright law, to adjust it to the changes that cyberspace brings. It also calls for increased education to convince people of the wrong of copying without permission. Thus a change in law and norms—but also, and here's the interesting point, a change in code.

In an elaborate and somewhat hopeful section on the ability of software to protect intellectual property, the WhitePaper makes plain just how, in the very near future, software will be able to control illegal copying. Or more generally, how in the very near future, software will be able to control, perfectly, the *use* and distribution of intellectual property. This, the WhitePaper encourages, and it even recommends that we punish people who interfere with such software. It thus recommends, that is, that we use law to protect code.

This last point may seem obvious, but in my view, we don't understand the potential here. For the question is not whether software can protect intellectual property—of course it can, and very quickly is. The more important question is whether this software will protect intellectual property too much.

The point is this: code could in principle make intellectual property unstealable—meaning unusable except in the ways the owner wants. But as it is understood just now, intellectual property is not supposed to be perfectly unstealable; it's not supposed to be perfectly protected. For the right that intellectual property grants is a compromised right: the holders of the right to intellectual property do so subject to a public use

[13] *See* INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE (1995) (hereinafter, the WhitePaper).

exception, called fair use. But when code develops to protect this property, there is nothing to assure that it will be protected with this public use exception intact. Code is a kind of private law, protecting the interests of the author; but unlike the public law protecting the interests of the author (copyright), nothing guarantees that code will preserve the public values implicit in that public law.

In a sense, this problem is just the reverse of the problem with the worm. With the worm, the code was undermining a private value—namely privacy—by making it possible for the government perfectly to enforce a search; and here, with code protecting intellectual property, the code is undermining a public value—namely, the public use exceptions to the property interest. In both cases, the efficiency of the code undermines an important real world value. And this again forces the question of how we should think about the value of code.

The most difficult case, however, is the third—the Communications Decency Act (CDA), recently struck down by two three-judge district courts, and now on appeal to the Supreme Court.[14] This example ties to my story about passports, but I need some more background before the connection will be clear.

When the net began, or when it was old enough to be called the "net," it was essentially unzoned—unzoned in the sense that there were very few rules restricting access, based on who someone was, or from where someone came. Zoning, in this sense, is what a local community does, when it decides that a movie theater can't open in a residential neighborhood; but it is also, in a broader sense, what law schools do when they make admission turn on LSAT scores, or what fancy restaurants do when they exclude men not wearing a tie. Zoning, in the sense I mean, is all the ways in which access or use is limited, or all the technologies for regulating access or use, based on criteria chosen by someone other than the consumer.

In this sense, the net was a place without zoning. Or in the sense of my story about Russia, it was a world without

---

[14] ACLU v. Reno, 929 F. Supp 824 (E.D. Pa. 1996) (restricting enforcement of Title V of the Telecommunications Act of 1996, Pub. L. No. 104-104, § 502, 110 Stat. 133, 133-36 (1996) (to be codified at 47 U.S.C. § 223(d))), *prob. juris. noted*, No. 96-511, 1996 WL 604702 (U.S. Dec. 6, 1996); Shea v. Reno, 930 F. Supp. 916 (S.D.N.Y. 1996), *petition for cert. filed*, 65 U.S.L.W. 3323 (U.S. Oct. 15, 1996) (No. 96-595).

internal passports. Once one entered the net, one defined who one was to be, and regardless of who one defined oneself to be, the net was open. Massive search engines expressed this freedom—tools for scanning the net, and then listing portholes into which you were free to step. Access was radically democratic—open, and free, regardless of who one was.

All this is changing. The net is changing. It is moving from an essentially unzoned space, to a place that is inherently zoned—to a place that allows for regulation and control of access in way that is far more efficient than the zonings that exist in real space. But the reasons, and the techniques here, are again the same as with the worm, or copyright: the reason is code. If there is one feature that defines the present development of the architecture of the net, it is just this: it is becoming a place where code facilitates zoning, a place where the technologies for discriminating in access are multiplied.

These discriminations are of many sorts. Some track the domain from which you come. Your domain name, for example, helps inform the web site you visit who you are. Some track the places you've been; this is the famous Cookies file, attached to your browser, which keeps a list of some of the places you've been. These are passive techniques of zoning; there are active techniques as well: screens that will not let you access information unless you've paid for that access (a kind of zoning, again), and screens that will not let you gain access to information unless you're the right sort of person.

It is this last kind of zoning that introduces the CDA, and that the CDA wants to introduce. What the CDA does is require that sites with "indecent material" screen out minors from access to that material. It does this with a common carrot-and-stick technique: If you make indecent material available, you will be punished. But if in good faith, you try to screen out minors, you will be immune from punishment. Thus the statute is better understood simply as a requirement to screen. And the constitutional question we should then ask is whether a requirement to screen, or more generally, whether a requirement to zone in a particular way, is unconstitutional.

Now I think the CDA is unconstitutional, but that's because of the sloppiness of its definitions of indecency, rather than any problem with its inherent structure. If we could eliminate the problems with definitions, then I don't think

there would be a problem with the structure. And that's the point I want to make here.

Here's a story that might make the point. Of all the cyber-rights activists who opposed the CDA, the ACLU was the first to succeed in challenging the statute after it was passed. It was their case—*ACLU v. Reno*[15]—that succeeded first in striking the statute down. The claims of the ACLU were in part clearly correct—their attack again on the definition of "indecency" was, in my view, an extremely strong attack—but in part just missed the point.

I saw this most clearly when I was asked to be on a panel sponsored by the ACLU, debating the merits of the CDA. The panel was in Chicago, and was hosted by Christy Heffner, president of *Playboy*, and a strong supporter of the ACLU. The local ACLU chapter had, on its web site, a page describing the event, and associated with each name was a link to a web page that might give more information about that participant. The link next to my name was the University of Chicago; next to Christy Heffner's, *Playboy*.

Just before this panel discussion was to begin, I accessed this web page to learn something more about the other panelists. In the process, I clicked on Christy Heffner's name. I was taken to a "cgi"—a log-in screen, that asked me for my "I-Code." I didn't know what an I-Code was, and so I clicked on the button that advertised itself for the I-Code ignorant. This took me to another screen, run by the company, I-Code, Inc.[16] On this screen was a form. The form asked a series of questions about who I was, how much money I made, what my sex and age were, and what I did for a living.[17] Once I had answered all these questions, I clicked a button and was given an I-Code. This in hand (or in my paste buffer at least), I was returned to the *Playboy* web page, with the key that I now needed to enter. I entered the key, and was immediately taken to a page where I could learn about Christy Heffner, or about one of the most popular "zines" on the web today, *Playboy*.

This whole process took about a minute, and with this minute's investment, I was then armed with a code that would

---

[15] 929 F. Supp. 824 (E.D. Pa. 1996).

[16] See the description of I-Code, Inc., at http://icode.ipro.com/icode_ description.html (site under revision at time of publication).

[17] *See* http://icode.ipro.com/register/icode_reg_form.html (site under revision at time of publication).

(I was promised) give me access to a wide range of web pages that similarly limit access to the I-Code savvy.

Why did *Playboy* want me to register with I-Code? What's plain is that this registration had nothing to do with the CDA; the I-Code form could not verify my age. Instead, I-Code is a system developed by I-Code, Inc., for providing web sites with demographic data about who has accessed their site. Knowledge may be power, but data is money. With this demographic data, *Playboy* can sell advertisements on its site, an extremely large source of revenue for a company like *Playboy*.

The I-Code system, in the sense that I have described, is a zoning device. It makes possible a kind of discrimination that before would not have been possible, by linking access to data about who the accessors are. With this information, the web sites can do any number of things: they could sell advertising (as *Playboy* no doubt does); they could in principle discriminate as to access (giving some I-Code users higher priority than others); they could in principle exclude some users. (For example, a web site set up for women only might use an I-Code-like system to screen men from the site.)

The market created the incentive for *Playboy* to exclude from its web site people who refused to give it information, and *Playboy* acted on that incentive and excluded those who wouldn't pay. Privacy nuts, for example, were banned from seeing the *Playboy* home page, because they were unwilling to give information about themselves. This is a kind of discrimination in access, just as the CDA demands a discrimination in access. The CDA's discrimination is based on age; *Playboy*'s, on privacy.

Now this discrimination *Playboy*, or for that matter, the ACLU, didn't seem to mind much. What troubled them was the government required discrimination on the basis of age—not, because *Playboy* really believes twelve-year-olds should be consuming pornography, but rather because somehow this zoning was a violation of speech rights.

But it is that step I don't think we can make. For what this zoning through code is doing is channeling access to the material on the net, in a way that is far more effective, or efficient, than the channeling or zoning of real space. Just as Playboy has decided who should have access and who should not, so too does the government try to influence who should have access and who should not. If there is no problem in real space with governments making just that sort of choice, why in cyberspace? No one thinks moving porn shops to a remote

area of a city violates the Constitution; so why does it violate the Constitution to require walls on pornshops in cyberspace?

The answer is that it doesn't—or at least, when the Court is presented with a decently crafted statute—it will say that it doesn't. And again, the reason ties to the power of code. Zoning in cyberspace is better than zoning in real space, or put more ambiguously, it does its terrible job more efficiently. The cost it imposes on someone who wants access, and who has a right to access, is slight. It perfects the power of control.

But then this just pushes us back to a more general question about the virtue of systems that control access, about the values of zoning. For here is the real question that cyberactivists should be asking: should zoned space itself raise constitutional concerns? My view is that it should, but that's a way to say that I would like it if it did, or better, that this is the policy I would prefer. But a policy argument is not a constitutional argument. And my sense here again is that the Constitution doesn't give us the policy arguments we would prefer. That again we are left with an ambiguous conclusion about the effect of code.

I've offered here three cases that present something of the ambiguity that code presents, three cases where code seems to give us something that law in real space couldn't. But it can give us this only as cyberspace becomes zoned. Unzoned, cyberspace is unregulable, or unregulable at least by code. But zoned, or perfectly zoned, then the possibilities of regulation are unlimited.

The question then might be whether this is a good thing. And the problem, I suggest, is that we don't have a good way to think about the answer to this. We have a libertarian tradition in our constitutional past, but we also have a tradition of activist regulation. What we are learning about the libertarianism is that in large part, it was a consequence of the frictions, or imperfections, of regulation. What when these imperfections disappear? What tradition do we have to appeal to so as to argue that inefficiency should be preserved?

I don't have an answer to this large question, but I do have a clue about some smaller points. First, what is unavoidable in the story I've just told is that code is political, that the architectures that are established in cyberspace have normative significance, and that choices can be made about the values that this architecture will embed. The question of what the architecture of cyberspace should be is not a neutral question. We need to think about it in political terms.

Second, we need to think about who is making the code. If code is political, then it is not the task of engineers alone. If there are fundamental questions about how cyberspace is to be structured, these are questions that should be addressed by the citizens of cyberspace. If code constitutes cyberspace, then citizens must choose the code. But as it is, the architecture is the product of private interests—whether the relatively open Internet Engineering Task Force or the absolutely closed Microsoft Corporation.

Finally, a point about how we read the Constitution, as it is, in cyberspace. For our tradition has been to leave these questions to the judges, to let them engage this practice of translation, to carry the values of the framers into our own era.

But if translation here gives out—if the choices that need to be made have not in any meaningful sense already been made—then we have a problem. For by leaving this practice of Constitution making to judges, we may well have lost the ability meaningfully to address, and resolve, these questions of value. We are used to these questions being resolved by courts; we have forgotten how to do this ourselves.

Code presses on us, urgently and impatiently, choices about what kind of place we want cyberspace to be, and more importantly, what kind of power over real space we will let cyberspace have. It presses this, but it is as if we have forgotten how to speak. It is here that constitutional theory should have something to say, but here that constitutional theory just gives out.

There was a time when constitutional theory was just this—when it was about what structures preserved what values, and about what values should be preserved. But in our legacy of interpreting an ancient constitution, we have somehow lost this past. In our obsession with figuring out just how to read an ancient document, we have lost a way to speak about the values such a document should embrace. We have become so concerned with pretending that the choices of value that we champion are choices already made, that we have lost the practice of making choices of value ourselves. At least constitutional value; at least so far.