The Laws of Cyberspace

Lawrence Lessig†

Draft 3

---

† Jack N. and Lillian R. Berkman Professor for Entrepreneurial Legal Studies, Harvard Law School. Thanks to Tim Wu for extremely helpful comments on an earlier draft.

Before the revolution, the Tsar in Russia had a system of internal passports. The people hated this system. These passports marked the estate from which you came, and this marking determined the places you could go, with whom you could associate, what you could be. The passports were badges that granted access, or barred access. They controlled what in the Russian state Russians could come to know.

The Bolsheviks promised to change all this. They promised to abolish the internal passports. And soon upon their rise to power, they did just that. Russians were again free to travel where they wished. Where they could go was not determined by some document that they were required to carry with them. The abolition of the internal passport symbolized freedom for the Russian people — a democratization of citizenship in Russia.

This freedom, however, was not to last. A decade and a half later, faced with the prospect of starving peasants flooding the cities looking for food, Stalin brought back the system of internal passports. Peasants were again tied to their rural land (a restriction that remained throughout the 1970s). Russians were once again restricted by what their passport permitted. Once again, to gain access to Russia, Russians had to show something about who they were.

* * *

Behavior in the real world — this world, the world in which I am now speaking — is regulated by four sorts of constraints. Law is just one of those four constraints. Law regulates by sanctions imposed ex post — fail to pay your taxes, and you are likely to go to jail; steal my car, and you are also likely to go to jail. Law is the prominent of regulators. But it is just one of four.

Social norms are a second. They also regulate. 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 — direct and constrain my behavior in a far wider array of contexts than any law. Norms say what clothes I will wear — a suit, not a dress; they tell you to sit quietly, and politely, for at least 40 minutes while I speak; they or-

ganize how we will interact after this talk is over. Norms guide behavior; in this sense, they function as a second regulatory constraint.

The market is a third constraint. It regulates by price. The market limits the amount that I can spend on clothes; or the amount I can make from public speeches; it says I can command less for my writing than Madonna, or less from my singing than Pavarotti. Through the device of price, the market sets my opportunities, and through this range of opportunities, it regulates.

And finally, there is the constraint of what some might call nature, but which I want to call "architecture." This is the constraint of the world as I find it, even if this world as I find it is a world that others have made. That I cannot see through that wall is a constraint on my ability to know what is happening on the other side of the room. That there is no access-ramp to a library constrains the access of one bound to a wheelchair. These constraints, in the sense I mean here, regulate.

To understand a *regulation* then we must understand the sum of these four constraints operating together. Any one alone cannot represent the effect of the four together.

* * *

This is the age of the cyber-libertarian. It is a time when a certain hype about cyberspace has caught on. The hype goes like this: Cyberspace is unavoidable, and yet cyberspace is unregulable. No nation can live without it, yet no nation will be able to control behavior in it. Cyberspace is that place where individuals are, inherently, free from the control of real space sovereigns. It is, in the words of James Boyle, the great techno-"gotcha" — nations of the world, you can't live with out it, but nations of the world, when you've got it, you won't live long with it.

My aim today is a different view about cyberspace. My aim is to attack this hype. For in my view, the world we are entering is not a world of perpetual freedom; or more precisely, the world we are entering is not a world where freedom is assured. Cyberspace has the potential to be the most fully, and extensively, regulated space that we have ever known — anywhere, at any time in our history. It has the potential to be the antithesis of a space of freedom. And unless we understand this potential, unless we see how this might be, we are likely to sleep through this transition from freedom into

control. For that, in my view, is the transition we are seeing just now.

Now I want to make this argument by using the two introductions that I began with today — the story about Bolshevik Russia, and the idea about regulation. For they together will suggest where cyberspace is going, and more importantly, just how we can expect cyberspace to get there.

First the idea: Just as in real space, behavior in cyberspace is regulated by four sorts of constraints. Law is just one of those constraints. For the hype notwithstanding, there is law just now in cyberspace — copyright law, or defamation law, or sexual harassment law, all of which constrain behavior in cyberspace in the same way that 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 others. They too function in cyberspace as norms function in real space, threatening punishments ex post by a community.

And so too with the market. The market constrains in cyberspace, just as in real space. Change the price of access, the constraints on access differ. Change the structure of pricing access, and the regulation of marginal access shifts dramatically as well.

But for our purposes, the most significant of these four constraints on behavior in cyberspace is the analog to what I called *architecture* in real space: This I will call *code*. By code, I simply mean the software and hardware that constitutes cyberspace as it is—the set of protocols, the set of rules, implemented, or codified, in the software of cyberspace itself, that determine how people interact, or exist, in this space. This code, like architecture in real space, sets the terms upon which I enter, or exist in cyberspace. It, like architecture, is not optional. I don't choose whether to obey the structures that it establishes — hackers might choose, but hackers are special. For the rest of us, life in cyberspace is subject to the code, just as life in real space is subject to the architectures of real space.

The substance of the constraints of code in cyberspace vary. But how they are experienced does not vary. In some places, one must enter a password before one gains access; in other places, one can enter whether identified or not. In some places, the transactions that one engages produce traces that link the transactions

back to the individual; in other places, this link is achieved only if the individual chooses. In some places, one can select to speak a language that only the recipient can hear (through encryption); in other places, encryption is not an option.

The differences are constituted by the code of these different places. The code or software or architecture or protocols of these spaces set these features; they are features selected by code writers; they constrain some behavior by making other behavior possible. And in this sense, they, like architecture in real space, regulate behavior in cyberspace.

Code and market and norms and law together *regulate* in cyberspace then as architecture and market and norms and law regulate in real space. And my claim is that as with real space regulation, we should consider how these four constraints operate together.

An example — a contrast between a regulation in real space, and the same regulation in cyberspace — will make the point more clearly. Think about the concern in my country (some might call it obsession) with the regulation of indecency on the net.

This concern took off in the United State early in 1995. Its source was an extraordinary rise in ordinary users of the net, and therefore a rise in use by kids, and an even more extraordinary rise in the availability of what many call "porn" on the net. An extremely controversial (and fundamentally flawed) study published in the Georgetown University Law Review reported the net awash in porn. Time and Newsweek both ran cover stories articles about its availability. And senators and congressmen were bombarded with demands to do something to regulate "cybersmut."

No doubt the fury at the time was great. But one might ask, why this fury was so great about porn in *cyberspace*. Certainly, more porn exists in real space than in cyberspace. So why the fury about access to porn in a place to which most kids don't have access?

To understand the why, think for a second about the same problem as it exists in real space. What regulates the distribution of porn in real space?

First: In America, laws in real space regulate the distribution of porn to kids— laws requiring sellers of porn to check the age of

buyers, or laws requiring that sellers locate in a section of the city likely to be far from kids. But laws are not the most significant of the constraints on the distribution of porn to kids.

More important than laws are norms. Norms constrain adults not to sell porn to kids. Even among porn distributors this restriction is relatively effective.

And not just social norms. The market too, for porn costs money, and as kids have no money.

But the most important real space constraint is what I've called *architecture*. For all of these other regulations in real space depend on this constraint of architecture. Laws and norms and market can discriminate against kinds in real space, since it is hard in real space to hide that you are a kid. Of course, a kid can don a mustache, and put on stilts, and try to enter a porn shop to buy porn. But for the most part, disguises will fail. For the most part, it will be too hard to hide that he is a kid. Thus, for the most part, constraints based on being a kid are constraints that can be effective.

Cyberspace is different. For even if we assume that the same laws apply to cyberspace as to real space, and even if we assume that the constraints of norms and the market carried over as well, even so, there remains a critical difference between the two spaces. For while in real space it is hard to hide that you are a kid, in cyberspace, hiding who you are, or more precisely, hiding features about who you are is the simplest thing in the world. The default in cyberspace is anonymity. And because it is so easy to hide who one is, it is practically impossible for the laws, and norms, to apply in cyberspace. For for these laws to apply, one has to know that it is a kid one is dealing with. But the architecture of the space simply doesn't provide this information.

Now the important point is to see the difference, and to identify its source. The difference is a difference in what I want to call the *regulability* of cyberspace — the ability of governments to regulate behavior there. As it is just now, cyberspace is a less *regulable* space than real space. There is less that government can do.

The source of this difference in regulability is a difference in the architecture of the space — a difference in the code that constitutes cyberspace as it is. Its architecture, my claim is, renders it essentially unregulable.

Or so it did in 1995, and in 1996, when the U.S. Congress eventually got around to passing its attempt to deal with this problem—the Communications Decency Act. I'm going to talk a bit about what happened to that statute, but I first want to mark this period, and set it off from where we are today. It was the architecture of cyberspace in 1995, and 1996 that made it essentially unregulable.

Let's call that architecture Net 95 — as in 1995 — and here are its features: So long as one had access to Net95, one could roam without identifying who one was. Net95 was Bolshevik Russia. One's identity, or features, were invisible to the net then, so one could enter, and explore, without credentials—without an internal passport. Access was open and universal, not conditioned upon credentials. It was, in a narrow sense of the term, an extraordinary democratic moment. Users were fundamentally equal. Essentially free.

It was against this background — against the background of the net as it was — Net95 — that the Supreme Court then considered the Communications Decency Act. Two lower courts had struck the statute as a violation of the right to freedom of speech. And as millions watched as the court considered arguments on the case — watched in cyberspace, as the arguments were reported, and debated, and critiqued.

And in June, last year, the Court affirmed the decision of the lower courts, holding the statute unconstitutional. Just why it was unconstitutional isn't so important for our purposes here. What is important is the rhetoric that lead the court to its conclusion.

For the decision hung crucially on claims about the architecture of the net as it was — on the architecture, that is, of Net95. Given that architecture, the court concluded, any regulation that attempted to zone kids from porn would be a regulation that was too burdensome on speakers and listeners. As the net was, regulation would be too burdensome.

But what was significant was that the court spoke as if this architecture of the net as it was — Net 95 — was the only architecture that the net could have. It spoke as if it had discovered the nature of the net, and was therefore deciding the nature of any possible regulation of the net.

But the problem with all this, of course, is that the net has no nature. There is no single architecture that is essential to the net's design. Net95 is a set of features, or protocols, that constituted the net at one period of time. But nothing requires that these features, or protocols, always constitute the net as it always will be. And indeed, nothing in what we've seen in the last 2 years should lead us to think that it will.

An example may make the point more simply. Before I was a professor at Harvard, I taught at the University of Chicago. If one wanted to gain access to the net at the university of Chicago, one simply connected one's machine to jacks located throughout the university. Any machine could be connected to those jacks, and once connected, any machine would then have full access to the internet. Access was anonymous, and complete, and free.

The reason for this freedom was a decision by the administration. For the Provost of the University of Chicago is Geof Stone, a former dean of the University of Chicago Law School, and a prominent free speech scholar. When the University was designing its net, the technicians asked the provost whether anonymous communication should be permitted. The provost, citing a principle that the rules regulating speech at the university would be as protective of free speech as the first amendment, said yes: One would have the right to communicate at the university anonymously, because the first amendment to the constitution would guarantee the same right vis-à-vis the government. From that policy decision flowed the architectural design of the University of Chicago's net.

At Harvard, the rules are different. One cannot connect one's machine to the net at Harvard unless one's machine is registered — licensed, approved, verified. Only members of the university community can register their machine. Once registered, all interactions with the network are potentially monitored, and identified to a particular machine. Indeed, anonymous speech on this net is not permitted — against the rule. Access can be controlled based on who someone is; and interaction can be traced, based on what someone did.

The reason for this design is also due to the decision of an administrator — though this time an administrator less focused on the protections of the first amendment. Controlling access is the ideal at Harvard; facilitating access was the ideal at Chicago; tech-

nologies that make control possible were therefore chosen at Harvard; technologies that facilitate access chosen at Chicago.

Now this difference between the two networks is quite common today. The network at the University of Chicago is the architecture of the internet in 1995. It is, again, Net95. But the architecture at Harvard is not an internet architecture. It is rather an intranet architecture. The difference is simply this — that within an intranet, identity is sufficiently established such that access can be controlled, and usage monitored. The underlying protocols are still TCP/IP — meaning the fundamental or underlying protocols of the internet. But layered on top of this fundamental protocol is a set of protocols facilitating control. The Harvard network is the internet plus, where the plus mean the power to control.

These two architectures reflect two philosophies about access. They reflect two sets of principles, or values, about how speech should be controlled. They parallel, I want to argue, the difference between political regimes of freedom, and political regimes of control. They track the difference in ideology between West and East Germany; between the United States and the former Soviet Republic; between the Republic of China, and Mainland China. They stand for a difference between control and freedom — and they manifest this difference through the architecture or design of code. These architectures enable political values. They are in this sense political.

Now I don't offer this example to criticize Harvard. Harvard is a private institution; it is free, in a free society, to allocate its resources however it wishes. My point instead is simply to get you to see how architectures are many, and therefore how the choice of one is political. And how, at the level of a nation, architecture is inherently political. In the world of cyberspace, the selection of an architecture is as important as the choice of a constitution. For in a fundamental sense, the code of cyberspace *is* its constitution. It sets the terms upon which people get access; it sets the rules; it controls their behavior. In this sense, it is its own sovereignty. An alternative sovereignty, competing with real space sovereigns, in the regulation of behavior by real space citizens.

But the United States Supreme Court treated the question of architecture as if the architecture of this space were given. It spoke as if there were only one design for cyberspace — the design it had.

In this, the Supreme Court is not alone. For in my view, the single greatest error of theorists of cyberspace — of pundits, and especially lawyers thinking about regulation in this space — is this error of the Supreme Court. It is the error of naturalism as applied to cyberspace. It is the error of thinking that the architecture as we have it is an architecture that we will always have; that the space will guarantee us liberty, or freedom; that it will of necessity disable governments that want control.

This view is profoundly mistaken. Profoundly mistaken because while we celebrate the "inherent" freedom of the net, the architecture of the net is changing from under us. The architecture is shifting from an architecture of freedom to an architecture of control. It is shifting already without government's intervention, though government is quickly coming to see just how it might intervene to speed it. And where government is now intervening, it is intervening in a way designed to change this very same architecture — to change it into an architecture of control, to make it, as I've said, more *regulable*. While pundits promise perpetual freedom built into the very architecture of the net itself, technicians and politicians are working together to change that architecture, to move it away from this architecture of freedom.

As theorists of this space, we must come to understand this change. We must recognize the political consequences of this change. And we must take responsibility for these consequences. For the trajectory of the change is unmistakable, and the fruit of this trajectory, poison.

As constitutionalists, we must then confront a fundamentally constitutional question: if there is a choice between architectures of control and architectures of freedom, then how do we decide these constitutional questions? If architectures are many, then does the constitution itself guide us in the selection of such architectures?

In my view, constitutional values do implicate the architecture of this space. In my view, constitutional values should guide us in our design of this space. And in my view, constitutional values should limit the types of regulability that this architecture permits.

But my view is absent in thinking about government's role in cyberspace. Indeed, my nation — for many years the symbol of freedom in world where such freedom was rare — has become a leader in pushing the architecture of the internet from an archi-

tecture of freedom to an architecture of control. From an architecture, that is, that embraced the traditions of freedom expressed in our constitutional past, to an architecture that is fundamentally anathema to those traditions.

But how? How can the government make these changes? How could the government effect this control? Many can't see how government could effect this control. So in the few minutes remaining in my talk today, I want show you how. I want to sketch for you a path from where we are to where I fear we are going. I want you to see how these changes are possible and how government can help make them permanent.

Return then with me to the idea that began this essay — the point about the different modalities of constraint — and notice something important about that idea that we have not so far remarked. I said at the start that we should think of law as just one of four modalities of constraint; that we should think of it as just one part of the structure of constraint that might be said to regulate.

One might take that to be an argument about law's insignificance. If so many forces other than law regulate, this might suggest that law itself can do relatively little.

But notice what should be obvious. In the model I have described law is regulating by direct regulation — regulating an individual through the threat of punishment. But law regulates in other ways as well. It regulates, that is, indirectly as well as directly. And it regulates indirectly when it regulates these other modalities of constraint, so that they regulate differently. It can, that is, regulate norms, so norms regulate differently; it can regulate the market, so that the market regulates differently; and it can regulate architecture, so that architecture regulates differently. In each case, the government can coopt the other structures, so that they constrain to the government's end.

The same indirection is possible in cyberspace. But here, I suggest, the indirection will be even more significant. For here the government can not only regulate indirectly to advance a particular substantive end of the government. More significantly, the government can regulate to change the very *regulability* of the space. The government, that is, can regulate the architectures of cyberspace, so that behavior in cyberspace becomes more regulable —

indeed, to an architecture potentially more regulable than anything we have known in the history of modern government.

Two examples will make the point — one an example of the government regulating to a particular substantive end, and the second, following from the first, an example of the government regulating to increase regulability.

The first is the regulation of encryption. The government's concern with encryption has been with the technology's use in protecting privacy — its ability to hide the content of communications from the eyes of an eavesdropping third party, whether that third party is the government, or a nosy neighbor. For much of the history of the technology, the American government has heavily regulated the technology; for a time it threatened to ban its use; it has consistently banned its export (as if only Americans understand higher order mathematics); and for a period it hoped to flood the market with a standard encryption technology that would leave a backdoor open for the government to enter.

The most recent proposals are the most significant. Last November, the FBI proposed a law that would require manufacturers to assure that any encryption system have built within it either a key recovery ability, or an equivalent back door, so that government agents could, if they need, get access to the content of such communications.

This is government's regulation of code, indirectly to regulate behavior. It is indirect regulation in the sense that I described before, and from a constitutional perspective — it is brilliant. Not brilliant because its ends are good; brilliant because the American constitution, at least, offers very little control over government regulation like this. The American constitution offers little protections against the government's regulation of business; and given the interests of business, such regulations are likely to be effective.

My second example follows from the first. For a second use of encryption is identification — as well as hiding what someone says, encryption, through digital certificates, can be used to authenticate who some it. With the ability to authenticate who someone is, the government could tell where someone comes from, or how old they are. And with this ability — through certifying IDs — passports on the information superhighway — governments could far more easily regulate behavior on this highway.

It would recreate the power to control behavior — recreate the power to regulate.

Note what both regulations would achieve. Since the US is the largest market for internet products, no product could hope to succeed unless it were successful in the United States. Thus standards successfully imposed in the US becomes standards for the world. And these standards in particular would first facilitate regulation, and second, assure that communications on the internet could be broken into by any government that followed the procedures outlined in the bill. But the standards that those government would have to meet are not the standards of the US constitution. They are whatever standard local government happen to have — whether that government be the government of Mainland China, or Switzerland.

The effect is that the United States government would be exporting an architecture that facilitates control, and control not just by other democratic governments, but by any government, however repressive. And by this, the US would move itself from a symbol of freedom, to a peddler of control. Having won the cold war, we would be pushing the techniques of our cold war enemies.

* * *

How should we respond? How should you — as sovereigns independent of the influence of any foreign government — and we, as liberal constitutionalists respond? How should we respond to moves by a dominant political and economic power to influence the architecture of the dominant architecture of regulation by code — the internet?

Sovereigns must come to see this: That the code of cyberspace is itself a kind of sovereign. It is a competing sovereign. The code is itself a force that imposes its own rules on people who are there, but the people who are there are also the people who are here — citizens of the Republic of China, citizens of France, citizens of every nation in the world. The code regulates them, yet they are by right subject to the regulation of local sovereigns. The code thus competes with the regulatory power of local sovereigns. It competes with the political choices made by local sovereigns. And in this competition, as the net becomes a dominant place for business and social life, it will displace the regulations of local sovereigns. You as sovereigns were afraid of the competing influence of na-

tions. Yet a new nation is now wired into your telephones, and its influence over your citizens is growing.

You, as sovereigns, will come to recognize this competition. And you should come to recognize and question the special role that the United States is playing in this competition. By virtue of the distribution of resources controlling the architecture of the net, the United States has a unique power over influencing the development of that architecture. It is as the law of nature were being written, with the United States at the authors side. This power creates an important responsibility for the United States — and you must assure that it exercises its power responsibly.

The problem for constitutionalists — those concerned to preserve social and political liberties in this new space — is more difficult.

For return to the story that began this talk — the world of internal passports. One way to understand the story I've told today about cyberspace is in line with this story about the Tsar's Russia. The birth of the net was the revolution itself; life under Net95 was life in Bolshevik Russia (the good parts at least, where internal passports were eliminated); the Net as it is becoming is Stalin's Russia, where internal passports will again be required.

Now there's a cheat to that story — a rhetorical cheat that tends to obscure an important fact about real space life. For we all live in the world of internal passports. In the United States, in many places, one cannot live without a car; one can't drive a car without a license; a license is an internal passport: It says who you are, where you come from, how old you are, whether you've recently been convicted of a crime; it links your identity to a database that will reveal whether you've been arrested (whether convicted or not) or whether any warrants for your arrest in any jurisdiction in the nation are outstanding. The license is the internal passport of the modern American state. And no doubt its ability to control or identify is far better than the Tsar's Russia.

But in the United States — at least for those who don't appear to be immigrants, or a disfavored minority — the burden of these passports is slight. The will to regulate, to monitor, to track, is not strong enough in the United States to support any systematic effort to use these passports to control behavior. And the will is not strong enough because the cost of such control is so great. There are not checkpoints at each corner; one isn't required to register

when moving through a city; one can walk relatively anonymously around most of the time. Technologies of control are possible, but in the main far too costly. And this costliness is, in large part, the source of great freedom. It is inefficiency in real space technologies of control that yield real space liberty.

But what if the cost of control drops dramatically. What if an architecture emerges that permits constant monitoring; an architecture that facilitates the constant tracking of behavior and movement. What if an architecture emerged that would costlessly collect data about individuals, about their behavior, about who they wanted to become. And what if the architecture could do that invisibly, without interfering with an individuals daily life at all?

This architecture is the world that the net is becoming. This is the picture of control it is growing into. As in real space, we will have passports in cyberspace. As in real space, these passports can be used to track our behavior. But in cyberspace, unlike realspace, this monitoring, this tracking, this control of behavior, will all be much less expensive. This control will occur in the background, effectively and invisibly.

Now to describe this change is not to say whether it is for the good or bad. Indeed, I suggest that as constitutionalists, we must acknowledge a fundamental ambiguity in our present political judgments about liberty and control. I our peoples are divided in their reaction to this picture of a system of control at once perfect, and yet invisible. Many would say of this system — wonderful. All the better to trap the guilty, with little burden on the innocent. But there are many as well who would say of this system — awful. That while professing our ideals of liberty and freedom from government, we would have established a system of control far more effective than any in history before.

So the response to all this is not necessarily to give up the technologies of control. The response is not to insist that Net95 be the perpetual architecture of the net. The response instead is to find a way to *translate* what is salient and important about present day liberties and constitutional democracy into this architecture of the net. The point is to be critical of the power of this sovereign—this emerging sovereign—as we are properly critical of the power of any sovereign.

What are these limits: As government takes control or influences the architecture of the code of the net, at a minimum, we

must assure that government does not get a monopoly on these technologies of control. We must assure that the sorts of checks that we build into any constitutional democracy get built into regulation by this constitution — the code. We must assure that the constraints of any constitutional democracy — the limits on efficiency constituted by Bills of Rights, and systems of checks and balances — get built into regulation by code. These limits are the "bugs" in the code of a constitutional democracy — and as John Perry Barlow says, we must build these bugs into the code of cyberspace. We must build them in so that they, by their inefficiency, might recreate some of the protections we have long known.

***

Cyberspace is regulated ¾ by laws, but not just by law. The code of cyberspace is one of these laws. We must come to see how this code is an emerging sovereign — omnipresent, omnipotent, gentle, efficient, growing — and that we must develop against this sovereign the limits that we have developed against real space sovereigns. Sovereigns will always say — real space as well as cyberspace — that limits, and inefficiencies — bugs — are not necessary. But things move too quickly for such confidence. My fear is not just that against this sovereign, we have not yet developed a language of liberty. Nor that we haven't the time to develop such language. But my fear is that we sustain the will — the will of free societies for the past two centuries, to architect constitutions to protect freedom, efficiencies notwithstanding.