Code Is Law

On Liberty in Cyberspace

by LAWRENCE LESSIG

1.1.00

Every age has its potential regulator, its threat to liberty. Our founders feared a newly empowered federal government; the Constitution is written against that fear. John Stuart Mill worried about the regulation by social norms in nineteenth-century England; his book On Liberty is written against that regulation. Many of the progressives in the twentieth century worried about the injustices of the market. The reforms of the market, and the safety nets that surround it, were erected in response.

Ours is the age of cyberspace. It, too, has a regulator. This regulator, too, threatens liberty. But so obsessed are we with the idea that liberty means "freedom from government" that we don't even see the regulation in this new space. We therefore don't see the threat to liberty that this regulation presents.

This regulator is code--the software and hardware that make cyberspace as it is. This code, or architecture, sets the terms on which life in cyberspace is experienced. It determines how easy it is to protect privacy, or how easy it is to censor speech. It determines whether access to information is general or whether information is zoned. It affects who sees what, or what is monitored. In a host of ways that one cannot begin to see unless one begins to understand the nature of this code, the code of cyberspace regulates.

This regulation is changing. The code of cyberspace is changing. And as this code changes, the character of cyberspace will change as well. Cyberspace will change from a place that protects anonymity, free speech, and individual control, to a place that makes anonymity harder, speech less free, and individual control the province of individual experts only.

My aim in this short essay is to give a sense of this regulation, and a sense of how it is changing. For unless we understand how cyberspace can embed, or displace, values from our constitutional tradition, we will lose control over those values. The law in cyberspace--code--will displace them.

THE REGULATIONS OF CODE

The basic code of the Internet implements a set of protocols called TCP/IP. These protocols enable the exchange of data among interconnected networks. This exchange occurs without the networks knowing the content of the data, or without any true idea of who in real life the sender of a given bit of data is. This code is neutral about the data, and ignorant about the user.

These features of TCP/IP have consequences for the "regulability" of behavior on the Internet. They make regulating behavior difficult. To the extent that it is hard to identify who people are, it is harder to trace behavior back to a particular individual. And to the extent it is hard to identify what kind of data is being sent, it is harder to regulate the use of particular kinds of data. These architectural features of the Internet mean that governments are relatively disabled in their ability to regulate behavior on the Net.

In some contexts, for some, this unregulability is a virtue. This feature of the Net, for example, protects free speech. It codes a First Amendment into the architecture of cyberspace, because it makes it relatively hard for governments, or powerful institutions, to control who says what when. Information from Bosnia or East Timor can flow freely to the world because the Net makes it hard for governments in those countries to control how information flows. The Net makes it hard because its architecture makes it hard.

But in other contexts, in the view of others, this unregulability is not a virtue--take the German government confronted by Nazi speech, for example, or the U.S. government faced with child pornography. In these contexts, the architecture disables regulation as well. But in these contexts, unregulability is viewed as a vice.

And not just with Nazi speech and child porn. The most important contexts of regulation in the future will affect Internet commerce: where the architecture does not enable secure transactions; where it makes it very easy to hide the source of interference; where it facilitates the distribution of illegal copies of software and music. In these contexts, commerce at least will not view unregulability as a virtue; unregulability here will interfere with the ability of commerce to flourish.

So what can be done?

There are many who think that nothing can be done: that the unregulability of the Internet is fixed; that there is nothing we can do to change it; that it will, so long as it is the Internet, remain unregulable space. That its "nature" makes it so.

But no thought is more dangerous to the future of liberty in cyberspace than this faith in freedom guaranteed by the code. For the code is not fixed. The architecture of cyberspace is not given. Unregulability is a function of code, but the code can change. Other architectures can be layered onto the basic TCP/IP protocols, and these other architectures can make behavior on the Net fundamentally regulable. Commerce is building these other architectures; the government can help; the two together can transform the character of the Net. They can and they are.

OTHER ARCHITECTURES

What makes the net unregulable is that it is hard to tell who someone is, and hard to know the character of the content being delivered. Both of these features are now changing. Architectures for facilitating identification--or, more generally, for certifying facts about the user (that he is over 18; that he is a he; that he is an American; that he is a lawyer)--are emerging. Architectures for rating content (porn, hate speech, violent speech, political speech) have been described and are being implemented. Each is being developed without the mandate of government, and the two together could facilitate an extraordinary degree of control over behavior on the Net. The two together, that is, could flip the unregulability of the Net.

Could--depending upon how they are designed. Architectures are not binary. There is not simply a choice about implementing an identification architecture, or a rating architecture, or not. What the architecture enables, and how it limits its control, are choices. And depending upon these choices, much more than regulability will be at stake.

Consider identification, or certification, architectures first. We have many certification architectures in real space. The driver's license is a simple example. When the police stop you and demand your license, they are asking for a certain certification that you are licensed to drive. That certification includes your name, your sex, your age, where you live. It must include all that because there is no other simple way to link the license to the person. You must give up all these facts about yourself to certify that in fact you are the proper holder of the license.

But certification in cyberspace could be much more narrowly tailored. If a site required that only adults enter, you could--using certification technologies--certify that you were an adult, without also revealing who you were or where you came from. The technology could make it possible to selectively certify facts about you, while withholding other facts about you. The technology could function under a "least-revealing-means" test in cyberspace even if it can't in real space.

Could--depending upon how it was designed. But there is no necessity that it will develop like this. There are other architectures developing--we could call them "one-card-shows all." In these architectures, there is no simple way to limit what gets revealed by a certificate. If a certificate holds your name, address, age, citizenship, and whether you are a lawyer, and if you need to certify that you are a lawyer, this architecture would certify not only that you are a lawyer--but also all the other facts about you that the certificate holds. Under this architecture, more is better. Nothing enables the individual to steer for less.

The difference between these designs is that one enables privacy in a way that the other does not. One codes privacy into an identification architecture by giving the user a simple choice about how much is revealed; the other is oblivious to that value.

Thus whether the certification architecture that emerges protects privacy depends upon the choices of those who code. Their choices depend upon the incentives they face. If protecting privacy is not an incentive--if the market has not sufficiently demanded it and if law has not, either--then this code will not provide it.

The example about identification is just one among many. Consider another, involving information privacy. RealJukebox is a technology for copying music from a CD to a computer, as well as for downloading music from the Net to store on a computer's hard drive. In October it was revealed that the system was a bit nosy--that it snooped the hard disk of the user and reported back to the company what it found. It did this secretly, of course; RealNetworks didn't tell anyone its product was collecting and reporting personal data. It just did. When this snooping was discovered, the company at first defended the practice (saying no data about individuals were actually stored). But it quickly came to its senses, and promised not to collect such data.

This "problem" is caused, again, by the architecture. You can't easily tell in cyberspace who's snooping what. And while the problem might be corrected by an architecture (a technology called P3P would help), here's a case where law would do well. If these data were deemed the property of the individual, then taking them without express permission would be theft.

In these contexts, and others, architectures will enable values from our tradition--or not. In each, there will be decisions about how best to build out the Internet's architecture consistent with those values, and how to integrate those architectures with law. The choice about code and law will be a choice about values.

MAKING CHOICES ABOUT VALUES

So should we have a role in choosing this code, if this code will choose our values? Should we care about how values emerge here?

In another time, this would have been an odd question. Self-government is all about tracking and modifying influences that affect fundamental values--or, as I described them at the start, regulations that affect liberty. In another time we would have said, "Obviously we should care. Obviously we should have a role."

But we live in an era fundamentally skeptical about self-government. Our age is obsessed with leaving things alone. Let the Internet develop as the coders would develop it, the common view has it. Keep government out.

This is an understandable view, given the character of our government's regulation. Given its flaws, it no doubt seems best simply to keep government away. But this is an indulgence that is dangerous at any time. It is particularly dangerous now.

Our choice is not between "regulation" and "no regulation." The code regulates. It implements values, or not. It enables freedoms, or disables them. It protects privacy, or promotes monitoring. People choose how the code does these things. People write the code. Thus the choice is not whether people will decide how cyberspace regulates. People--coders--will. The only choice is whether we collectively will have a role in their choice--and thus in determining how these values regulate--or whether collectively we will allow the coders to select our values for us.

For here's the obvious point: when government steps aside, it's not as if nothing takes its place. It's not as if private interests have no interests; as if private interests don't have ends that they will then pursue. To push the antigovernment button is not to teleport us to Eden. When the interests of government are gone, other interests take their place. Do we know what those interests are? And are we so certain they are anything better?

Our first response should be hesitation. It is proper to let the market develop first. But as the Constitution checks and limits what Congress does, so too should constitutional values check and limit what a market does. We should test both the laws of Congress and the product of a market against these values. We should interrogate the architecture of cyberspace as we interrogate the code of Congress.

Unless we do, or unless we learn how, the relevance of our constitutional tradition will fade. The importance of our commitment to fundamental values, through a self-consciously enacted constitution, will fade. We will miss the threat that this age presents to the liberties and values that we have inherited. The law of cyberspace will be how cyberspace codes it, but we will have lost our role in setting that law.

Lawrence Lessig is the Berkman professor for entrepreneurial legal studies at Harvard Law School. His most recent book, Code, and Other Laws of Cyberspace *(Basic Books), has just been published (see http://code-is-law.org). The website of the Berkman Center for Internet and Society at the law school (see page 50) is http://cyber.law.harvard.edu.*