به نام پروردگار متعال

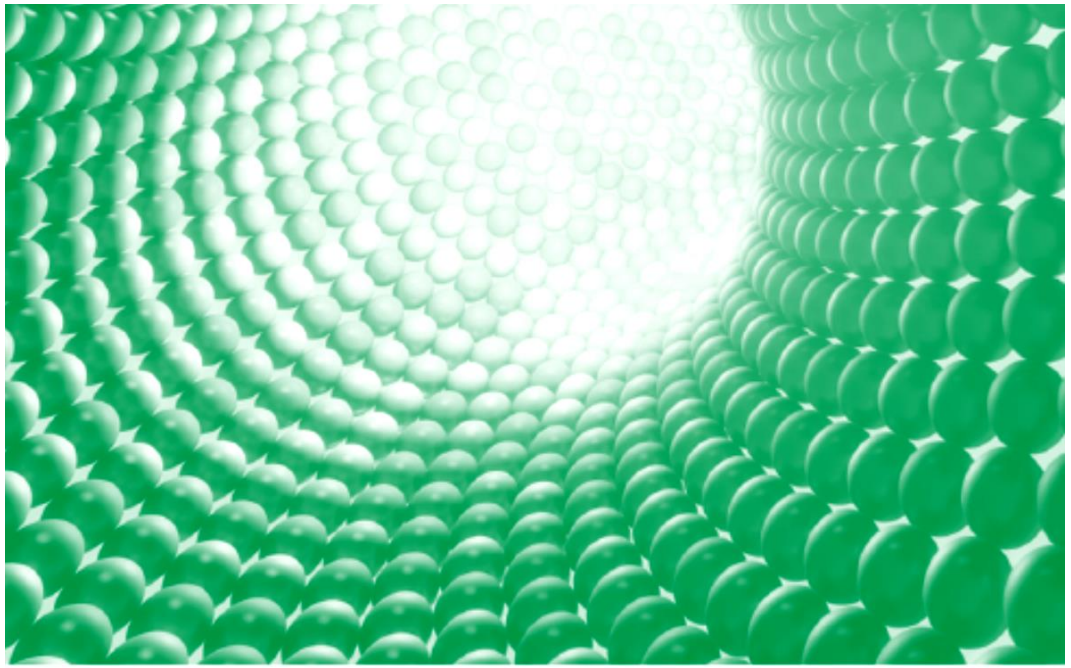
# فناوری و اجتماع

# Technology and Society

# مبحث چهارم: کدهای رایانه ای و معماری اجتماعی

| | |
|---|---|
| • Johnson-Wetmore: Ch.11 Code Is Law | کدهای رایانه‌ای<br>و معماری اجتماعی |

4. Johnson, D. G, Wetmore, J. M. (eds.) (2008). *Technology and Society, Building Our Sociotechnical Future (Inside Technology)*. MIT Press. England.



TECHNOLOGY AND SOCIETY

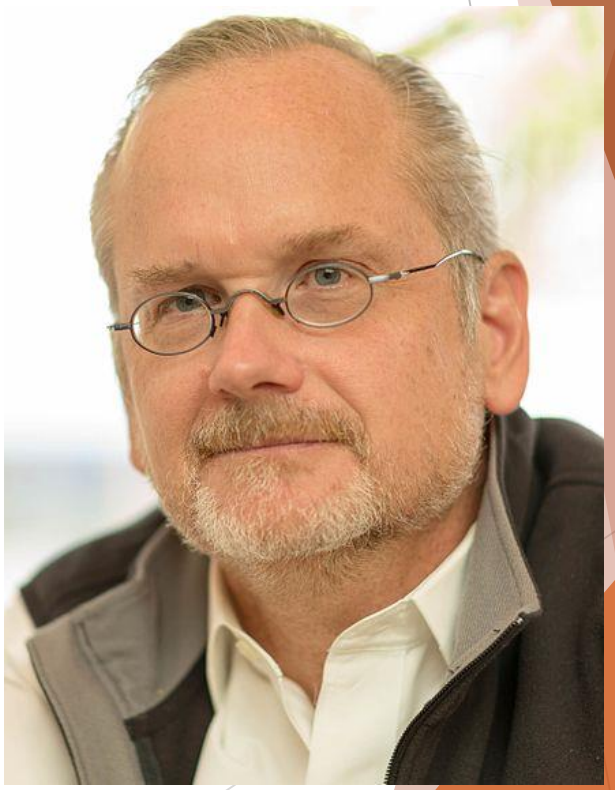
Building Our Sociotechnical Future

EDITED BY DEBORAH G. JOHNSON AND JAMESON M. WETMORE

# 11 "Code Is Law"

## Lawrence Lessig

From *Code: And Other Laws of Cyberspace*, 1999



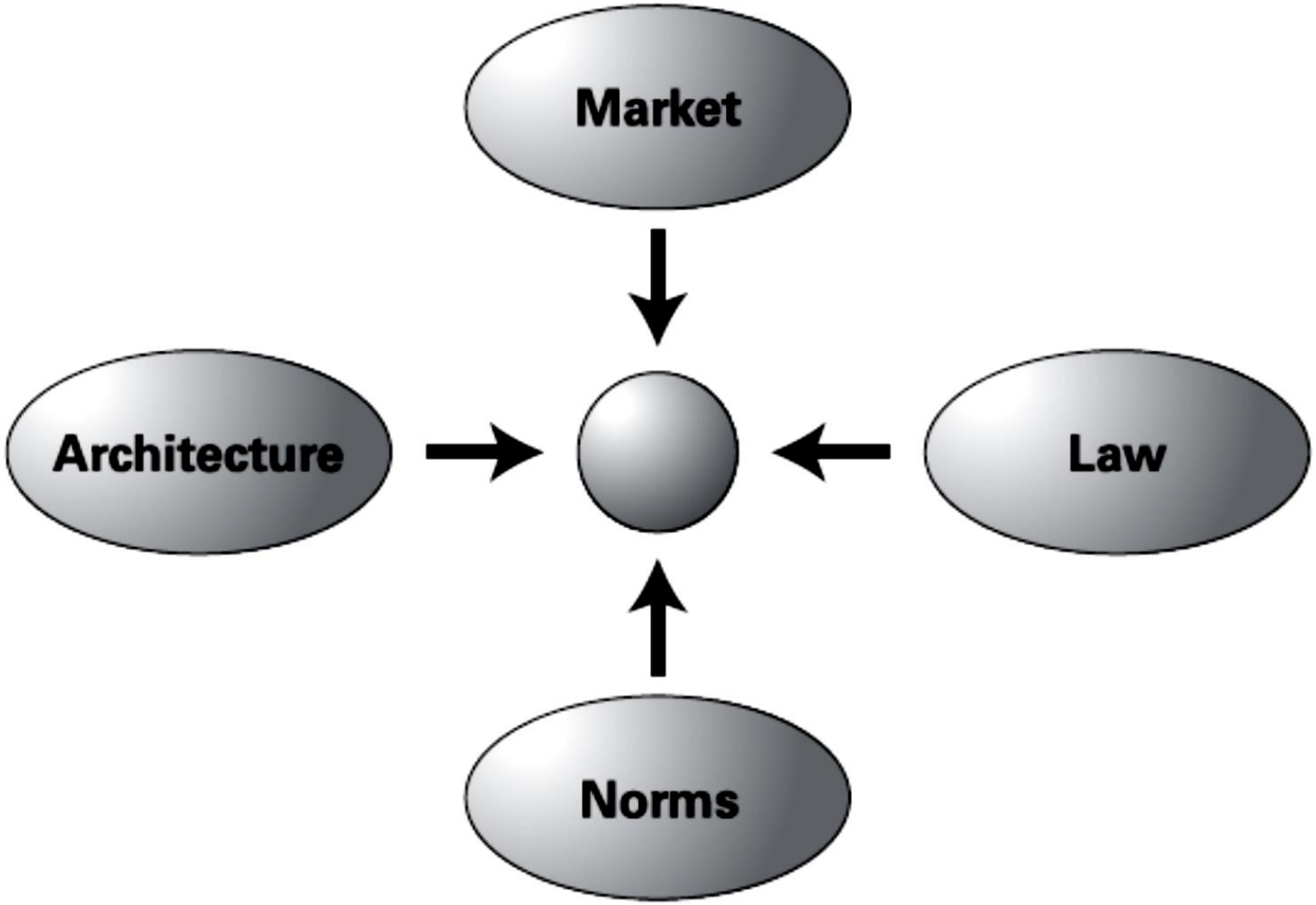
# کلیات دیدگاه های لارنس لسیگ در این مقاله:

- رفتار هر فرد متأثر از چهار گونه نظم دهی است: قانون، هنجارها، بازارها و معماری (آرشیتکچر)
- بنابراین، ما نمی توانیم فقط بر قوانین، هنجارها و بازارها تمرکز کنیم بلکه باید به معماری (طراحی (فناوری و ورود در جزئیات فنی) نیز توجه کنیم.
- عنوان مقاله حاکی از این ادعای لسیگ است که "کد کامپیوتری" با همان قدرت قانون، کنش های ما را توانمند یا محدود می کند.
- لسیگ معتقد است انسان ها این قدرت را دارند که فناوریی را که نهایتاً ما را شکل خواهد داد، کنترل کنند. ما باید هنگامی که فناوری هنوز در حال توسعه یافتن است دست به کنش بزنیم.

(Lessig, p. 189 )

# Real Life & Behavior Regulators

Thus, four constraints regulate this pathetic dot—the law, social norms, the market, and architecture—and the "regulation" of this dot is the sum of these four constraints.



(Lessig, p. 189 )

# How Do the Regulators Regulate?

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.

The constraints are distinct, yet they are plainly interdependent. Each can support or oppose the others. Technologies can undermine norms and laws; they can also support them. Some constraints make others possible; others make some impossible.

(Lessig, p. 190 )

# Cyberspace Regulators (Law, Norms)

Law regulates behavior in cyberspace. Copyright law, defamation law, and obscenity laws all continue to threaten *ex post* sanction for the violation of legal rights. How well law regulates, or how efficiently, is a different question: in some cases it does so more efficiently, in some cases less. But whether better or not, law continues to threaten a certain consequence if it is defied. Legislatures enact;[19] prosecutors threaten;[20] courts convict.[21]

Norms also regulate behavior in cyberspace. Talk about democratic politics in the alt.knitting newsgroup, and you open yourself to flaming; "spoof" someone's identity in a MUD, and you may find yourself "toaded";[22] talk too much in a discussion list, and you are likely to be placed on a common bozo filter. In each case, a set of understandings constrain behavior, again through the threat of *ex post* sanctions imposed by a community.

(Lessig, p. 190 )

# Cyberspace Regulators (Markets)

Markets regulate behavior in cyberspace. Pricing structures constrain access, and if they do not, busy signals do. (AOL learned this quite dramatically when it shifted from an hourly to a flat rate pricing plan.)[23] Areas of the Web are beginning to charge for access, as online services have for some time. Advertisers reward popular sites; on-line services drop low-population forums. These behaviors are all a function of market constraints and market opportunity. They are all, in this sense, regulations of the market.

(Lessig, p. 190 )

# Cyberspace Regulators (Architecture)

And finally, an 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 AOL, for instance) you must enter a password before you gain access; in other places you can enter whether identified or not.[24] 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.[25] In some places you can choose to speak a language that only the recipient can hear (through encryption);[26] in other places encryption is not an option.[27] 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.

(Lessig, p. 183 )

# Cyberspace: Is It Free "By Nature"?

The claim now was that government *could not* regulate cyberspace, that cyberspace was essentially, and unavoidably, free. Governments could threaten, but behavior could not be controlled; laws could be passed, but they would be meaningless. There was no choice about which government to install—none could reign. Cyberspace would be a society of a very different sort. There would be definition and direction, but built from the bottom up, and never through the direction of a state. The society of this space would be a fully self-ordering entity, cleansed of governors and free from political hacks.

Cyberspace, the story went, could *only* be free. Freedom was its nature.

# CODE

version 2.0

LAWRENCE LESSIG


A Member of the Perseus Books Group
New York



Published by Basic Books
A Member of the Perseus Books Group

Printed in the United States of America. For information, address Basic Books, 387 Park Avenue South, New York, NY 10016–8810.

Books published by Basic Books are available at special discounts for bulk purchases in the United States by corporations, institutions, and other organizations. For more information, please contact the Special Markets Department at the Perseus Books Group, 11 Cambridge Center, Cambridge MA 02142, or call (617) 252-5298, (800) 255-1514 or e-mail special.markets@perseusbooks.com.

CIP catalog record for this book is available from the Library of Congress.

ISBN-10: 0–465–03914–6
ISBN-13: 978–0–465–03914–2

06 07 08 09 / 10 9 8 7 6 5 4 3 2 1

(2006, p. 34 )

# TCP/IP

the information traveling across TCP/IP itself does not contain anything that would indicate what the content was. The protocol thus doesn't authenticate who sent the packet, where they sent it from, and what the packet is. All it purports to assert is an IP address to which the packet is to be sent, and an IP address from which the packet comes. From the perspective of the network, this other information is unnecessary surplus. Like a daydreaming postal worker, the network simply moves the data and leaves its interpretation to the applications at either end.

(2006, p. 44 )

# … as Simple as possible

This minimalism in the Internet's design was not an accident. It reflects a decision about how best to design a network to perform a wide range over very different functions. Rather than build into this network a complex set of functionality thought to be needed by every single application, this network philosophy pushes complexity to the edge of the network—to the applications that run on the network, rather than the network's core. The core is kept as simple as possible.

(2006, pp. 45-46

# … Anonymity

While in real space—and here is the important point—anonymity has to be created, in cyberspace anonymity is the given.

The state can say to websites, "don't let kids see porn." But the website operators can't know—from the data provided by the TCP/IP protocols at least—whether the entity accessing its web page is a kid or an adult.

(2006, p.16

# … Escape the Law (for Gambling)

The Boral attorney general thus now faces a difficult problem. She may have moved the server out of her state, but she hasn't succeeded in reducing Boralian gambling. Before the Net, she would have had a group of people she could punish—those running gambling sites, and those who give those places custom. Now, the Net has made them potentially free from punishment—at the least because it is more difficult to know who is running the server or who is gambling. The world for this attorney general has changed. By going online, the gamblers moved into a world where this behavior is no longer *regulable*.

(2006, p.26

# … Escape the Norms (and Law)

But regulation by whom? For the rules are different in one place versus another.

This was one important issue raised by Jake Baker. Jake lived in Ann Arbor, Michigan. His life there was subject to the norms of Ann Arbor, and he apparently adapted to these norms reasonably well. The authority of that space governed Jake, and, as far as anyone knew, it appeared to govern him exclusively.

But in cyberspace, Jake's behavior changed, in part because the norms of the space were different. That created the problem. For when Jake "went to" cyberspace, he didn't leave real space. In particular, he never left Ann Arbor. While sitting in a dorm at the University of Michigan, he was able to teleport himself—in the only normatively significant sense—to a different world where the norms of civility and decency that governed outside his dorm room did not reign. Cyberspace gave Jake the chance to escape Ann Arbor norms and to live according to the norms of another place.

(Lessig, p. 183 )

# Liberty: Build it upon a Constitution/Code

Liberty in cyberspace will not come from the absence of the state. Liberty there, as anywhere, will come from a state of a certain kind.[4] We build a world where freedom can flourish not by removing from society any self-conscious control; we build a world where freedom can flourish by setting it in a place where a particular kind of self-conscious control survives. We build liberty, that is, as our founders did, by setting society upon a certain *constitution*.

But by "constitution" I don't mean a legal text. Unlike my countrymen in Eastern Europe, I am not trying to sell a document that our framers wrote in 1787. Rather, as the British understand when they speak of their constitution, I mean an *architecture*—not just a legal text but a way of life—that structures and constrains social and legal power, to the end of protecting fundamental *values*—principles and ideals that reach beyond the compromises of ordinary politics.

(Lessig, p. 184 )

# Code: the greatest threat/ promise to liberal ideals

That regulator is the obscurity in the book's title—*Code*. In real space we recognize how laws regulate—through constitutions, statutes, and other legal codes. 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."[7] *Code is law*.

This code presents the greatest threat to liberal or libertarian ideals, as well as their greatest promise. We can build, or architect, or code cyberspace to protect values that we believe are fundamental, or we can build, or architect, or code cyberspace to allow those values to disappear. There is no middle ground. There is no choice that does not include some kind of *building*. Code is never found; it is only ever made, and only ever made by us. As Mark Stefik puts it, "Different versions of [cyberspace] support different kinds of dreams. We choose, wisely or not."[8]

(2006, p. 32

# No single Net

There is no single way that the Net has to be; no single architecture that defines the nature of the Net. The possible architectures of something that we would call “the Net” are many, and the character of life within those different architectures is diverse.

(2006, pp. 33-34

# Chicago's Net (vs. Harvard's)

In the middle 1990s at the University of Chicago, if you wanted access to the Internet, you simply connected your machine to Ethernet jacks located throughout the university.[4] Any machine with an Ethernet connection could be plugged into these jacks. Once connected, your machine had full access to the Internet—access, that is, that was complete, anonymous, and free.

From that policy decision flowed the architecture of the University of Chicago's net.

(2006, pp. 33-34

# Harvard's Net (vs. Chicago's)

At Harvard, the rules are different. If you plug your machine into an Ethernet jack at the Harvard Law School, you will not gain access to the Net. You cannot connect your machine to the Net at Harvard unless the machine is registered—licensed, approved, verified. Only members of the university community can register their machines. Once registered, all interactions with the network are monitored and identified to a particular machine. To join the network, users have to "sign" a user agreement.

. Control was the ideal at Harvard; access was the ideal at Chicago. Harvard chose technologies that made control possible; Chicago chose technologies that made access easy.

(2006, pp. 45-46

# IP Tracing

. With that IP address, and the time you made your post, using "a reverse DNS look-up,"[4] it is simple to identify the Internet Service Provider that gave you access to the Internet. And increasingly, it is relatively simple for the Internet Service Provider to check its records to reveal which account was using that IP address at that specified time. Thus, the ISP could (if required) say that it was your account that was using the IP address that posted the nasty message about your boss.

(2006, pp. 47-48

# Cookies

But IP tracing isn't the only technology of identification that has been layered onto the Internet. A much more pervasive technology was developed early in the history of the Web to make the web more valuable to commerce and its customers. This is the technology referred to as "cookies."

This is a small step toward authenticated identity. It's far from that, but it is a step toward it. Your computer isn't you (yet). But cookies make it possible for the computer to authenticate that it is the same machine that was accessing a website a moment before. And it is upon this technology that the whole of web commerce initially was built. Servers could now "know" that this machine is the same machine that was here before. And from that knowledge, they could build a great deal of value.

(2006, p. 54

# IPv6

Indeed, as Shawn Helms describes, the next generation of the Internet Protocol—IPv6—"marks each packet with an encryption 'key' that cannot be altered or forged, thus securely identifying the packet's origin. This authentication function can identify every sender and receiver of information over the Internet, thus making it nearly impossible for people to remain anonymous on the Internet."[16]

And even if not impossible, sufficiently difficult for the vast majority of us. Our packets will be marked. We—or something about us—will be known.

(2006, p. xv

# Challenge

- How do we protect liberty when the architectures of control are managed as much by the government as by the private sector?
- How do we assure privacy when the ether perpetually spies?
- How do we guarantee free thought when the push is to propertize every idea?
- How do we guarantee self-determination when the architectures of control are perpetually determined elsewhere?

(Lessig, p. 186 )

# Code Revolutions

Change is possible. I don't doubt that revolutions remain in our future; the open code movement is just such a revolution. But I fear that it is too easy for the government to dislodge these revolutions, and that too much will be at stake for it to allow the revolutionaries to succeed. Our government has already criminalized the core ethic of this movement, transforming the meaning of *hacker* into something quite alien to its original sense. This, I argue, is only the start.

Things could be different. They are different elsewhere. But I don't see how they could be different for us just now. This no doubt is a simple confession of the limits of my own imagination. I would be grateful to be proven wrong. I would be grateful to watch as we relearn—as the citizens of the former Communist republics are learning—how to escape our disabling ideas about the possibilities for governance.

(Lessig, p. 191

# Netizens and Architects

Laws, norms, the market, and architectures interact to build the environment that "Netizens" know. The code writer, as Ethan Katsh puts it, is the "architect."[29]

But how can we "make and maintain" this balance between modalities? What tools do we have to achieve a different construction? How might the mix of real-space values be carried over to the world of cyberspace? How might the mix be changed if change is desired?