Research Publication No. 1999-05
12/1999

The Law of the Horse: What Cyberlaw Might Teach

Lawrence Lessig

COMMENTARIES

THE LAW OF THE HORSE: WHAT CYBERLAW MIGHT TEACH

Lawrence Lessig

INTRODUCTION

A few years ago, at a conference on the "Law of Cyberspace" held at the University of Chicago, Judge Frank Easterbrook told the assembled listeners, a room packed with "cyberlaw" devotees (and worse), that there was no more a "law of cyberspace" than there was a "Law of the Horse";[1] that the effort to speak as if there were such a law would just muddle rather than clarify; and that legal academics ("dilettantes") should just stand aside as judges and lawyers and technologists worked through the quotidian problems that this souped-up telephone would present. "Go home," in effect, was Judge Easterbrook's welcome.

As is often the case when my then-colleague speaks, the intervention, though brilliant, produced an awkward silence, some polite applause, and then quick passage to the next speaker. It was an interesting thought — that this conference was as significant as a conference on the law of the horse. (An anxious student sitting behind me whispered that he had never heard of the "law of the horse.") But it did not seem a very helpful thought, two hours into this day-long conference. So marked as unhelpful, it was quickly put away. Talk shifted in the balance of the day, and in the balance of the contributions, to the idea that either the law of the horse was significant after all, or the law of cyberspace was something more.

Jack N. and Lillian R. Berkman Professor for Entrepreneurial Legal Studies, Harvard Law School. An earlier draft of this article was posted at the Stanford Technology Law Review, <http://stlr.stanford.edu>. This draft is a substantial revision of that earlier version. Thanks to Edward Felten, Deepak Gupta, David Johnson, Larry Kramer, Tracey Meares, Andrew Shapiro, Steve Shapiro, Polk Wagner, and Jonathan Zittrain for helpful discussions on an earlier draft of this essay. Thanks also to the Stanford and Chicago Legal Theory Workshops. Research assistance, much of it extraordinary, was provided by Karen King and James Staihar, and on an earlier draft by Timothy Wu. I expand many of the arguments developed here in a book published this month, CODE AND OTHER LAWS OF CYBERSPACE (1999).

[1] *See* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207. The reference is to an argument by Gerhard Casper, who, when he was dean of the University of Chicago Law School, boasted that the law school did not offer a course in "The Law of the Horse." *Id.* at 207 (internal quotation marks omitted). The phrase originally comes from Karl Llewellyn, who contrasted the U.C.C. with the "rules for idiosyncratic transactions between amateurs." *Id.* at 214.

Some of us, however, could not leave the question behind. I am one of that some. I confess that I've spent too much time thinking about just what it is that a law of cyberspace could teach. This essay is an introduction to an answer.[2]

Easterbrook's concern is a fair one. Courses in law school, Easterbrook argued, "should be limited to subjects that could illuminate the entire law."[3] "[T]he best way to learn the law applicable to specialized endeavors," he argued, "is to study general rules."[4] This "the law of cyberspace," conceived of as torts in cyberspace, contracts in cyberspace, property in cyberspace, etc., was not.

My claim is to the contrary. I agree that our aim should be courses that "illuminate the entire law," but unlike Easterbrook, I believe that there is an important general point that comes from thinking in particular about how law and cyberspace connect.

This general point is about the limits on law as a regulator and about the techniques for escaping those limits. This escape, both in real space and in cyberspace,[5] comes from recognizing the collection of tools that a society has at hand for affecting constraints upon behavior. Law in its traditional sense — an order backed by a threat directed at primary behavior[6] — is just one of these tools. The general point is that law can affect these other tools — that they constrain behavior themselves, and can function as tools of the law. The choice among tools obviously depends upon their efficacy. But importantly, the choice will also raise a question about values. By working through these examples of law interacting with cyberspace, we will throw into relief a set of general questions about law's regulation outside of cyberspace.

I do not argue that any specialized area of law would produce the same insight. I am not defending the law of the horse. My claim is specific to cyberspace. We see something when we think about the regulation of cyberspace that other areas would not show us.

My essay moves in three parts. I begin with two examples that are paradigms of the problem of regulation in cyberspace. They will then suggest a particular approach to the question of regulation generally. In the balance of Part I, I sketch a model of this general approach.

In Part II, I apply this general approach to a wider range of examples. It is in the details of these examples that general lessons will be found.

---

[2] I have developed elsewhere a complete account of this answer, or as complete as my account can be. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

[3] Easterbrook, *supra* note 1, at 207.

[4] *Id.*

[5] I have discussed in considerable detail the idea that one is always in real space while in cyberspace or, alternatively, that cyberspace is not a separate place. *See* Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1403 (1996).

[6] *See, e.g.*, H.L.A. HART, THE CONCEPT OF LAW 6–7, 18–25 (2d ed. 1994).

These lessons reach beyond the domain of cyberspace. They are lessons for law generally, though the non-plasticity of real-space regulation tends to obscure them.

The final Part describes three of these lessons — the first about the limits on law's power over cyberspace, the second about transparency, and the third about narrow tailoring.

The first lesson is about constitutional constraints — not constitution in the sense of a legal text, but a constitution understood more generally. Just as the division of powers sets constraints on how far the federal government might reach, so, too, do the features of cyberspace that I will describe set limits on how far government may reach.

The lesson about transparency is more familiar, though I suspect its relationship to cyberspace is not. By making "non-transparency" easy and seemingly natural, cyberspace provides a special opportunity to appreciate both the value and costs of transparency. The final lesson, about narrow tailoring, is less familiar still, though it is potentially the most significant feature of the interaction between cyberspace, and real-space law. In the examples of regulation in cyberspace, we will see the threat that a failure to "tailor" presents. The lessons about transparency and narrow tailoring both carry significance beyond the world of engineers. Or better, the regulations by engineers will have important implications for us.

I conclude with an answer to Easterbrook's challenge. If my argument sticks, then these three lessons raise regulatory questions as troubling in real-space law as they are in cyberspace. They are, that is, general concerns, not particular. They suggest a reason to study cyberspace law for reasons beyond the particulars of cyberspace.

I. REGULATORY SPACES, REAL AND "CYBER"

Consider two cyber-spaces, and the problems that each creates for two different social goals. Both spaces have different problems of "information" — in the first, there is not enough; in the second, too much. Both problems come from a fact about *code* — about the software and hardware that make each cyber-space the way it is. As I argue more fully in the sections below, the central regulatory challenge in the context of cyberspace is how to make sense of this effect of code.

A. Two Problems in Zoned Speech

1. Zoning Speech. — Porn in real space is zoned from kids. Whether because of laws (banning the sale of porn to minors), or norms (telling us to shun those who do sell porn to minors), or the market (porn costs money), it is hard in real space for kids to buy porn. In the main, not everywhere; hard, not impossible. But on balance the regulations of real space have an effect. That effect keeps kids from porn.

These real-space regulations depend upon certain features in the "design" of real space. It is hard in real space to hide that you are a kid. Age in real space is a self-authenticating fact. Sure — a kid may try to disguise that he is a kid; he may don a mustache or walk on stilts. But costumes are expensive, and not terribly effective. And it is hard to walk on stilts. Ordinarily a kid transmits that he is a kid; ordinarily, the seller of porn knows a kid is a kid,[7] and so the seller of porn, either because of laws or norms, can at least identify underage customers. Self-authentication makes zoning in real space easy.

In cyberspace, age is not similarly self-authenticating. Even if the same laws and norms did apply in cyberspace, and even if the constraints of the market were the same (as they are not), any effort to zone porn in cyberspace would face a very difficult problem. Age is extremely hard to certify. To a website accepting traffic, all requests are equal. There is no simple way for a website to distinguish adults from kids, and, likewise, no easy way for an adult to establish that he is an adult. This *feature* of the space makes zoning speech there costly — so costly, the Supreme Court concluded in *Reno v. ACLU*,[8] that the Constitution may prohibit it.[9]

2. Protected Privacy. — If you walked into a store, and the guard at the store recorded your name; if cameras tracked your every step, noting what items you looked at and what items you ignored; if an employee followed you around, calculating the time you spent in any given aisle; if before you could purchase an item you selected, the cashier demanded that you reveal who you were — if any or all of these things happened in real space, you would notice. You would notice and could then make a choice about whether you wanted to shop in such a store. Perhaps the vain enjoy the attention; perhaps the thrifty are attracted by the resulting lower prices. They might have no problem with this data collection regime. But at least you would know. Whatever the reason, whatever the consequent choice, you would know enough in real space to know to make a choice.

In cyberspace, you would not. You would not notice such monitoring because such tracking in cyberspace is not similarly visible. As Jerry Kang aptly describes,[10] when you enter a store in cyberspace, the store can record who you are; click monitors (watching what you choose with your mouse) will track where you browse, how long you view a particular page; an "em-

---

7 *Cf.* Crawford v. Lungren, 96 F.3d 380, 382 (9th Cir. 1996) (upholding as constitutional a California statute banning the sale of "harmful matter" in unsupervised sidewalk vending machines, because of a compelling state interest in shielding minors from adult-oriented literature).

8 521 U.S. 844 (1997).

9 *See id.* at 885; Lawrence Lessig, *What Things Regulate Speech: CDA 2.0 vs. Filtering*, 38 JURIMETRICS J. 630, 631 (1998).

10 *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1198–99 (1998); *cf. Developments in the Law — The Law of Cyberspace*, 112 HARV. L. REV. 1574, 1643 (1999) [hereinafter *Developments*] (suggesting that upstream filtering's invisibility is one potential problem of a proposed solution to children's access to pornography).

ployee" (if only a bot[11]) can follow you around, and when you make a purchase, it can record who you are and from where you came. All this happens in cyberspace — invisibly. Data is collected, but without your knowledge. Thus you cannot (at least not as easily) choose whether you will participate in or consent to this surveillance. In cyberspace, surveillance is not self-authenticating. Nothing reveals whether you are being watched,[12] so there is no real basis upon which to consent.

These examples mirror each other, and present a common pattern. In each, some bit of data is missing, which means that in each, some end cannot be pursued. In the first case, that end is collective (zoning porn); in the second, it is individual (choosing privacy). But in both, it is a feature of cyberspace that interferes with the particular end. And hence in both, law faces a choice — whether to regulate to change this architectural feature, or to leave cyberspace alone and disable this collective or individual goal. Should the law change in response to these differences? Or should the law try to change the features of cyberspace, to make them conform to the law? And if the latter, then what constraints should there be on the law's effort to change cyberspace's "nature"? What principles should govern the law's mucking about with this space? Or, again, how should law *regulate*?

* * *

To many this question will seem very odd. Many believe that cyberspace simply cannot be regulated. Behavior in cyberspace, this meme insists, is beyond government's reach. The anonymity and multi-jurisdictionality of cyberspace makes control by government in cyberspace impossible. The nature of the space makes behavior there *unregulable*.[13]

This belief about cyberspace is wrong, but wrong in an interesting way. It assumes either that the nature of cyberspace is fixed — that its architecture, and the control it enables, cannot be changed — or that government cannot take steps to change this architecture.

Neither assumption is correct. Cyberspace has no nature; it has no particular architecture that cannot be changed.[14] Its architecture is a function of its design — or, as I will describe it in the section that follows, its

---

[11] A "bot" is a computer program that acts as an agent for a user and performs a task, usually remotely, in response to a request.

[12] *See* FEDERAL TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 3 & n.9 (1998) [hereinafter PRIVACY ONLINE].

[13] *See, e.g.*, David R. Johnson & David Post, *Law and Borders — The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1375 (1996); David Kushner, *The Communications Decency Act and the Indecent Indecency Spectacle*, 19 HASTINGS COMM. & ENT. L.J. 87, 131 (1996); David G. Post, *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace*, 1995 J. ONLINE L. art. 3, 12–17 (1995) <http://www.law.cornell.edu/jol/post.html>; Tom Steinert-Threlkeld, *Of Governance and Technology*, INTER@CTIVE WK. ONLINE (Oct. 2, 1998) <http://www1. zdnet.com/intweek/filters/tthrelkl.html>.

[14] *See Developments*, *supra* note 10, at 1635 ("The fundamental difference between [real space and cyberspace] is that the architecture of cyberspace is open and malleable. Anyone who understands how to read and write code is capable of rewriting the instructions that define the possible.").

code.[15] This code can change, either because it evolves in a different way, or because government or business pushes it to evolve in a particular way. And while particular versions of cyberspace do resist effective regulation, it does not follow that every version of cyberspace does so as well. Or alternatively, there are versions of cyberspace where behavior can be regulated, and the government can take steps to increase this regulability.

To see just how, we should think more broadly about the question of regulation. What does it mean to say that someone is "regulated"? How is that regulation achieved? What are its modalities?

B. Modalities of Regulation

1. Four Modalities of Regulation in Real Space and Cyberspace. — Behavior, we might say, is regulated by four kinds of constraints.[16] Law is just one of those constraints. Law (in at least one of its aspects) orders people to behave in certain ways; it threatens punishment if they do not

---

[15] As I define the term, *code* refers to the software and hardware that constitute cyberspace as it is — or, more accurately, the rules and instructions embedded in the software and hardware that together constitute cyberspace as it is. Obviously there is a lot of "code" that meets this description, and obviously the nature of this "code" varies dramatically depending upon the context. Some of this code is within the Internet Protocol (IP) layer, where protocols for exchanging data on the Internet (including TCP/IP) operate. Some of this code is above this IP layer, or in Jerome H. Saltzer's terms, at its "end":

> For the case of the data communication system, this range includes encryption, duplicate message detection, message sequencing, guaranteed message delivery, detecting host crashes, and delivery receipts. In a broader context, the argument seems to apply to many other functions of a computer operating system, including its file system.

Jerome H. Saltzer, David P. Reed & David D. Clark, *End-to-End Arguments in System Design*, *in* INNOVATIONS IN INTERNETWORKING 195, 196 (Craig Partridge ed., 1988). More generally, this second layer would include any applications that might interact with the network (browsers, e-mail programs, file-transfer clients) as well as operating system platforms upon which these applications might run.

In the analysis that follows, the most important "layer" for my purposes will be the layer above the IP layer. The most sophisticated regulations will occur at this level, given the Net's adoption of Saltzer's end-to-end design. *See also infra* note 24; *cf.* Timothy Wu, *Application-Centered Internet Analysis*, 85 VA. L. REV. 1163, 1164 (1999) (arguing that a legal analysis of the Internet that focuses on the user must necessarily focus on this layer) .

Finally, when I say that cyberspace "has no nature," I mean that any number of possible designs or architectures may affect the functionality we now associate with cyberspace. I do not mean that, given its present architecture, no features exist that together constitute its nature.

[16] I have adapted this analysis from my earlier work on regulation. *See generally* Lawrence Lessig, *The New Chicago School*, 27 J. LEGAL STUD. 661, 662–66 (1998) (discussing the way in which laws, norms, markets, and architecture operate as modalities of constraint). It is related to the "tools approach to government action," of John de Monchaux & J. Mark Schuster, but I count four tools while they count five. John de Monchaux & J. Mark Schuster, *Five Things to Do*, *in* PRESERVING THE BUILT HERITAGE: TOOLS FOR IMPLEMENTATION 3, 3 (J. Mark Schuster, with John de Monchaux & Charles A. Riley II eds., 1997). I don't think the ultimate number matters much, however. Most important is the understanding that there are functionally distinct ways of changing constraints on behavior. For example, the market may or may not simply be an aggregation of the other modalities; so long as the market functions and changes distinctly, however, it is better to consider the market distinct.

obey.[17] The law tells me not to buy certain drugs, not to sell cigarettes without a license, and not to trade across international borders without first filing a customs form. It promises strict punishments if these orders are not followed. In this way, we say that law regulates.

But not only law regulates in this sense. Social norms do as well. Norms control where I can smoke; they affect how I behave with members of the opposite sex; they limit what I may wear; they influence whether I will pay my taxes. Like law, norms regulate by threatening punishment ex post. But unlike law, the punishments of norms are not centralized. Norms are enforced (if at all) by a community, not by a government. In this way, norms constrain, and therefore regulate.

Markets, too, regulate. They regulate by price. The price of gasoline limits the amount one drives — more so in Europe than in the United States. The price of subway tickets affects the use of public transportation — more so in Europe than in the United States. Of course the market is able to constrain in this manner only because of other constraints of law and social norms: property and contract law govern markets; markets operate within the domain permitted by social norms. But given these norms, and given this law, the market presents another set of constraints on individual and collective behavior.

And finally, there is a fourth feature of real space that regulates behavior — "architecture." By "architecture" I mean the physical world as we find it, even if "*as we find it*" is simply *how it has already been made*. That a highway divides two neighborhoods limits the extent to which the neighborhoods integrate. That a town has a square, easily accessible with a diversity of shops, increases the integration of residents in that town. That Paris has large boulevards limits the ability of revolutionaries to protest.[18] That the Constitutional Court in Germany is in Karlsruhe, while the capital is in Berlin, limits the influence of one branch of government over the other. These constraints function in a way that shapes behavior. In this way, they too regulate.

These four modalities regulate together. The "net regulation" of any particular policy is the sum of the regulatory effects of the four modalities together. A policy trades off among these four regulatory tools. It selects its tool depending upon what works best.

So understood, this model describes the regulation of cyberspace as well. There, too, we can describe four modalities of constraint.

---

[17] Obviously it does more than this, but put aside this argument with positivism. My point here is not to describe the essence of law; it is only to describe one part of law.

[18] In 1853, Louis Napoleon III changed the layout of Paris, broadening the streets in order to minimize the opportunity for revolt. *See* ALAIN PLESSIS, THE RISE AND FALL OF THE SECOND EMPIRE, 1852–1871, at 121 (Jonathan Mandelbaum trans., 1985) (1979); *Haussmann, George-Eugene Baron*, 5 ENCYCLOPAEDIA BRITANNICA 753 (15th ed. 1993).

Law regulates behavior in cyberspace — copyright, defamation, and obscenity law all continue to threaten ex post sanctions for violations. How efficiently law regulates behavior in cyberspace is a separate question — in some cases it does so more efficiently, in others not. Better or not, law continues to threaten an expected return. Legislatures enact,[19] prosecutors threaten,[20] courts convict.[21]

Norms regulate behavior in cyberspace as well: talk about democratic politics in the alt.knitting newsgroup, and you open yourself up to "flaming" (an angry, text-based response). "Spoof" another's identity in a "MUD" (a text-based virtual reality), and you may find yourself "toaded" (your character removed).[22] Talk too much on a discussion list, and you are likely to wind up on a common "bozo" filter (blocking messages from you). In each case norms constrain behavior, and, as in real space, the threat of ex post (but decentralized) sanctions enforce these norms.

Markets regulate behavior in cyberspace too. Prices structures often constrain access, and if they do not, then busy signals do. (America On-line (AOL) learned this lesson when it shifted from an hourly to a flat-rate pricing plan.[23]) Some sites on the web charge for access, as on-line services like AOL have for some time. Advertisers reward popular sites; on-line services drop unpopular forums. These behaviors are all a function of market constraints and market opportunity, and they all reflect the regulatory role of the market.

And finally the architecture of cyberspace, or its *code*, regulates behavior in cyberspace. The code, or the software and hardware that make cyberspace the way it is, constitutes a set of constraints on how one can behave.[24] The substance of these constraints varies — cyberspace is not one

---

19 The ACLU lists eleven states that passed Internet regulations between 1995 and 1997. *See* ACLU, *Online Censorship in the States* (visited Nov. 2, 1999) <http://www.aclu.org/issues/cyber/ censor/stbills.html>.

20 *See, e.g.*, *Warning to All Internet Users and Providers* (visited Nov. 2, 1999) <http://www.ag.state.mn.us/home/consumer/consumernews/OnlineScams/memo.html> (posting warning of Minnesota Attorney General with respect to illicit Internet activities).

21 *See, e.g.*, United States v. Thomas, 74 F.3d 701, 716 (6th Cir. 1996); Playboy Enters. v. Chuckleberry Publ'g, Inc., 939 F. Supp. 1032, 1034 (S.D.N.Y. 1996).

22 *See* Julian Dibbell, *A Rape in Cyberspace or How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database Into a Society*, 2 ANN. SURV. AM. L. 471, 477–78 (1995).

23 *See, e.g.*, *America Online Plans Better Information About Price Changes*, WALL ST. J., May 29, 1998, at B2; *AOL Still Suffering But Stock Price Rises*, NETWORK WK., Jan. 31, 1997, *available in* 1997 WL 8524039; David S. Hilzenrath, *"Free" Enterprise, Online Style: AOL, CompuServe and Prodigy Settle FTC Complaints*, WASH. POST, May 2, 1997, at G1.

24 *Cf. Developments*, *supra* note 10, at 1635 (suggesting that alterations in code can be used to solve the problems of cyberspace). By "code" in this essay, I do not mean the basic protocols of the Internet — for example, TCP/IP. *See generally* CRAIG HUNT, TCP/IP NETWORK ADMINISTRATION 1–22 (2d ed. 1998) (explaining how TCP/IP works); ED KROL, THE WHOLE INTERNET: USER'S GUIDE & CATALOG 23–25 (2d ed. 1992) (same); PETE LOSHIN, TCP/IP CLEARLY EXPLAINED 3–83 (2d ed. 1997) (same); Ben Segal, *A Short History of Internet Protocols at CERN* (visited Aug. 14, 1999)

place. But what distinguishes the architectural constraints from other constraints is how they are experienced. As with the constraints of architecture in real space — railroad tracks that divide neighborhoods, bridges that block the access of buses, constitutional courts located miles from the seat of the government — they are experienced as conditions on one's access to areas of cyberspace. The conditions, however, are different. In some places, one must enter a password before one gains access;[25] in other places, one can enter whether identified or not.[26] In some places, the transactions that one engages in produce traces, or "mouse droppings," that link the transactions back to the individual;[27] in other places, this link is achieved only if the individual consents.[28] In some places, one can elect to speak a language that only the recipient can understand (through encryption);[29] in other places, encryption is not an option.[30] Code sets these features; they are features selected by code writers; they constrain some behavior (for example, electronic eavesdropping) by making other behavior possible (encryption). They embed certain values, or they make the realization of certain values impossible. In this sense, these features of cyberspace also regulate, just as architecture in real space regulates.[31]

These four constraints — both in real space and in cyberspace — operate together. For any given policy, their interaction may be cooperative, or

---

<http://wwwinfo.cern.ch/pdp/ns/ben/TCPHIST.html> (describing the history of Internet protocols generally, including the TCP/IP protocol). Rather, I mean "application space" code — that is, the code of applications that operates on top of the basic protocols of the Internet. As Tim Wu describes, TCP/IP can be usefully thought of as the electric grid of the Internet; applications "plug into" the Internet. *See* Wu, *supra* note 15, at 1191–92 (1999). As I use the term "code" here, I am describing the applications that plug into the Internet.

25 An example of such a place is an online service like America Online (AOL).

26 For example, USENET postings can be anonymous. *See Answers to Frequently Asked Questions about Usenet* (visited Oct. 5, 1999) <http://www.faqs.org/faqs/usenet/faq/part1/>.

27 Web browsers make this information available, both in real time and archived in a cookie file. *See Persistent Cookie FAQ* (visited Aug. 14, 1999) <http://www.cookiecentral.com/faq.htm>.

28 Web browsers also permit users to turn off some of these tracking devices, such as cookies.

29 PGP, for example, is a program offered both commercially and free of charge to encrypt messages. *See The comp.security.pgp FAQ* (visited Oct. 5, 1999) <http://www.cam.ac.uk.pgpnet/ pgp-faq/faq-01.html>.

30 In some international contexts, for example, encryption is heavily restricted. *See* STEWART A. BAKER & PAUL R. HURST, THE LIMITS OF TRUST 130 (1998) (describing French controls on the export, import, and use of encryption); *Comments by Ambassador David Aaron* (visited Oct. 5, 1999) <http://www.bxa.doc.gov/Encryption/aaron.htm>.

31 A number of scholars are beginning to focus on the idea of the law as embedded in code. *See, e.g.*, Johnson & Post, *supra* note 13, at 1378–87 (1996); M. Ethan Katsh, *Software Worlds and the First Amendment: Virtual Doorkeepers in Cyberspace*, 1996 U. CHI. LEGAL F. 335, 348–54 (1996); Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 EMORY L.J. 911, 917–20; Andrew L. Shapiro, *The Disappearance of Cyberspace and the Rise of Code*, 8 SETON HALL CONST. L.J. 703, 715–23 (1998).

For an exceptional treatment of the same issue in real space, see GERALD E. FRUG, CITY MAKING: BUILDING COMMUNITIES WITHOUT BUILDING WALLS (1999) .

competitive.[32] Thus, to understand how a regulation might succeed, we must view these four modalities as acting on the same field, and understand how they interact.

The two problems from the beginning of this section are a simple example of this point:

(a) Zoning Speech. — If there is a problem zoning speech in cyberspace, it is a problem traceable (at least in part) to a difference in the architecture of that place. In real space, age is (relatively) self-authenticating. In cyberspace, it is not. The basic architecture of cyberspace permits users' attributes to remain invisible. So norms, or laws, that turn upon a consumer's age are more difficult to enforce in cyberspace. Law and norms are disabled by this different architecture.

(b) Protecting Privacy. — A similar story can be told about the "problem" of privacy in cyberspace.[33] Real-space architecture makes surveillance generally self-authenticating. Ordinarily, we can notice if we are being followed, or if data from an identity card is being collected. Knowing this enables us to decline giving information if we do not want that information known. Thus, real space interferes with non-consensual collection of data. Hiding that one is spying is relatively hard.

The architecture of cyberspace does not similarly flush out the spy. We wander through cyberspace, unaware of the technologies that gather and track our behavior. We cannot function in life if we assume that everywhere we go such information is collected. Collection practices differ, depending on the site and its objectives. To consent to being tracked, we must know that data is being collected. But the architecture disables (relative to real space) our ability to know when we are being monitored, and to take steps to limit that monitoring.

In both cases, the difference in the possibility of regulation — the difference in the *regulability* (both collective and individual) of the space — turns on differences in the modalities of constraint. Thus, as a first step to understanding why a given behavior in cyberspace might be different from one in real space, we should understand these differences in the modalities of constraint.

---

[32] Of course, the way they regulate differs. Law regulates (in this narrow sense) through the threat of punishments ex post; norms regulate (if they regulate effectively) through ex post punishment, as well as ex ante internalization; markets and architecture regulate by a present constraint — no ex ante constraint or ex post punishment is necessary to keep a person from walking through a brick wall.

[33] For a far more sophisticated and subtle view than my own, see DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? (1998). Brin details the growing real-space technologies for monitoring behavior, including many that would be as invisible as the technologies that I argue define the web. *See id.* at 5–8.

C. How Modalities Interact

1. Direct and Indirect Effects. — Though I have described these four modalities as distinct, obviously they do not operate independently. In obvious ways they interact. Norms will affect which objects get traded in the market (norms against selling blood[34]); the market will affect the plasticity, or malleability, of architecture (cheaper building materials create more plasticity in design); architectures will affect what norms are likely to develop (common rooms affect privacy[35]); all three will influence what laws are possible.

Thus a complete description of the interaction among the four modalities would trace the influences of each upon the others. But in the account that follows, I focus on just two. One is the effect of law on the market, norms, and architecture; the other is the effect of architecture on law, market, and norms.

I isolate these two modalities for different reasons. I focus on law because it is the most obvious *self-conscious* agent of regulation. I focus on architecture because, in cyberspace, it will be the most pervasive agent. Architecture will be the regulator of choice, yet as the balance of this essay will argue, our intuitions for thinking about a world regulated by architecture are undeveloped. We notice things about a world regulated by architecture (cyberspace) that go unnoticed when we think about a world regulated by law (real space).

With each modality, there are two distinct effects. One is the effect of each modality on the individual being regulated. (How does law, for example, directly constrain an individual? How does architecture directly constrain an individual?) The other is the effect of a given modality of regulation upon a second modality of regulation, an effect that in turn changes the effect of the second modality on the individual. (How does law affect architecture, which in turn affects the constraints on an individual? How does architecture affect law, which in turn affects the constraints on an individual?) The first effect is *direct*; the second is *indirect*.[36]

---

[34] *See, e.g.*, Karen Wright, *The Body Bazaar*, DISCOVER, Oct. 1998, at 114, 116 (describing the proliferation of the sale of blood in recent years).

[35] *See, e.g.*, BARRINGTON MOORE, JR., PRIVACY: STUDIES IN SOCIAL AND CULTURAL HISTORY 7 (1984) (describing how an Eskimo family's sharing of a small igloo makes privacy an "unattainable commodity").

[36] The distinction between "direct" and "indirect" effects has a troubled history in philosophy, *see, e.g.*, Judith Jarvis Thomson, *The Trolley Problem*, 94 YALE L.J. 1395, 1395–96 (1985) (discussing the moral dilemma of a trolley driver who must either stay on course and kill five people through his indirect action, or take direct action to alter his course such that he kills only one person), as well as in law, *see, e.g.*, NLRB v. Jones & Laughlin Steel Corp., 301 U.S. 1, 34–41 (1937) (addressing the degree to which employees of a steel company were directly engaged in interstate commerce). The problems of distinguishing direct from indirect consequences are similar to those arising in the doctrine of double effect. *See* PHILLIPA FOOT, *The Problem of Abortion and the Doctrine of the Double Effect*, *in* VIRTUES AND VICES AND OTHER ESSAYS IN MORAL PHILOSOPHY 19 (1978); *see also* Thomas J. Bole III, *The*

A regulator uses both direct and indirect effects to bring about a given behavior.[37] When the regulator acts indirectly, we can say that it uses or co-opts the second modality of constraint to bring about its regulatory end. So for example, when the law directs that architecture be changed, it does so to use architecture to bring about a regulatory end. Architecture becomes the tool of law when the direct action of the law alone would not be as effective.

Any number of examples would make the point, but one will suffice.

2. Smoking and the Picture of Modern Regulation. — Suppose the government seeks to reduce the consumption of cigarettes. There are a number of ways that the government could effectuate this single end. The law could, for example, ban smoking.[38] (That would be law directly regulating the behavior it wants to change.) Or the law could tax cigarettes.[39] (That would be the law regulating the supply of cigarettes in the market, to decrease their consumption.) Or the law could fund a public ad campaign against smoking.[40] (That would be the law regulating social norms, as a means to regulating smoking behavior.) Or the law could regulate the nicotine in cigarettes, requiring manufacturers to reduce or eliminate the nicotine.[41] (That would be the law regulating the "architecture" of cigarettes as a way to reduce their addictiveness and thereby to reduce the

---

Doctrine of Double Effect: Its Philosophical Viability, 7 SW. PHIL. REV. 1, 91–103 (1991) (discussing and analyzing problems with the doctrine of double effect); Warren S. Quinn, *Actions, Intentions, and Consequences: The Doctrine of Double Effect*, 18 PHIL. & PUB. AFF. 334, 334–41 (1989) (same). The difficulty arises when a line between direct and indirect must be drawn; there is no need in this essay to draw such a line.

37 My point in this sketch is not to represent all the forces that might influence each constraint. No doubt changes in code influence law and changes in law influence code; and so with the other constraints as well. A complete account of how these constraints evolve would have to include an account of these interwoven influences. But for the moment, I am focusing just on intentional intervention by the government.

38 *See, e.g.*, ALASKA STAT. § 18.35.305 (Michie 1990) (banning smoking in public places); ARIZ. REV. STAT. ANN. § 36-601.01 (West 1993) (same); COLO. REV. STAT. ANN. § 25-14-103 (West 1990) (same).

39 *See, e.g.*, 26 U.S.C. § 5701 (1994) (taxing cigarette manufacturers); 26 U.S.C. § 5731 (1994) (same).

40 *See, e.g., Feds Pick Up Arnold Spots*, ADWEEK, Nov. 23, 1998, at 8 (reporting the decision of the U.S. Office of National Drug Control Policy to air nationwide seven youth-oriented anti-smoking commercials initially created for the Massachusetts Department of Public Health); Pamela Ferdinand, *Mass. Gets Tough with Adult Smokers in Graphic TV Ads*, WASH. POST, Oct. 14, 1998, at A3 (describing a series of six 30-second anti-smoking ads, sponsored by the Massachusetts Department of Public Health, on a woman's struggle to survive while slowly suffocating from emphysema).

41 It is unclear whether the Food and Drug Administration (FDA) has authority to regulate the nicotine content of cigarettes. In August 1996, the FDA published in the Federal Register the FDA's *Regulations Restricting the Sale and Distribution of Cigarettes and Smokeless Tobacco to Protect Children and Adolescents*, 61 Fed. Reg. 44,396 (1996) (to be codified at 21 C.F.R. pts. 801, 803, 804, 807, 820, and 897). In *Brown & Williamson Tobacco Corp. v. FDA*, 153 F.3d 155 (4th Cir. 1998), the court found that the FDA did not have jurisdiction to regulate the marketing of tobacco products because such regulation would exceed the intended scope of the Federal Food, Drug, and Cosmetic Act. *See id.* at 176.

consumption of cigarettes.) Each of these actions can be expected to have some effect (call that its benefit) on the consumption of cigarettes; each action also has a cost. The question with each is whether the cost outweighs the benefit. If, for example, the cost of education to change norms about smoking were the same as the cost of changes in architecture, the value we place on autonomy and individual choice may tilt the balance in favor of education.

This is the picture of modern regulation. The regulator is always making a choice — a choice, given the direct regulations that these four modalities might effect, about whether to use the law directly or indirectly to some regulatory end. The point is not binary; the law does not pick one strategy over another. Instead, there is always a mix of direct and indirect strategies. The question the regulator must ask is: *Which mix is optimal*?

The answer will depend upon the context of regulation. In a small and closely knit community, norms might be the optimal mode of regulation; as that community becomes less closely knit, law or the market might become second-best substitutes. In tenth-century Europe, mucking about with architectural constraints might have been a bit hard, but in the era of the modern office building, architecture becomes a feasible and quite effective regulatory technique (think about transparent cubicles as a way to police behavior). The optimal mix depends upon the plasticity of the different modalities. Of course, what works in one context will not necessarily work everywhere. But within a particular context, we may be able to infer that certain modalities will dominate.

This is the case, I suggest, in cyberspace. As I describe more fully in the section that follows, the most effective way to regulate behavior in cyberspace will be through the regulation of code — direct regulation either of the code of cyberspace itself, or of the institutions (code writers) that produce that code. Subject to an increasingly important qualification,[42] we should therefore expect regulators to focus more upon this code as time passes.[43]

My aim in the next two sections is to explore this dynamic more fully. I hope to show (1) that government can regulate behavior in cyberspace (slogans about the unregulability of cyberspace notwithstanding); (2) that the optimal mode of government's regulation will be different when it regulates behavior in cyberspace; and (3) that this difference will raise ur-

---

[42] *See infra* note 105 (discussing open code).

[43] A recent example is the FBI's effort to get the Internet Engineering Task Force (IETF) to change Internet protocols to make them comply with the Communications Assistance of Law Enforcement Act (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. §§ 1001–1010). The IETF resisted, but the effort is precisely what this model would predict. *See* Declan McCullagh, *IETF Says "No Way" to Net Taps*, Wired News (visited Nov. 17, 1999) <http://www.wired.com/news/politics/0,1283,32455,00.html>.

gent questions that constitutional law has yet to answer well. (What limits should there be on indirect regulation? How far should we permit law to co-opt the other structures of constraint?)

II. INTERACTIONS: LAW AND ARCHITECTURE

A. Law Taming Code: Increasing Cyberspace Regulability.

I noted earlier the general perception that cyberspace was unregulable — that its nature made it so and that this nature was fixed. I argued that whether cyberspace can be regulated is not a function of Nature. It depends, instead, upon its architecture, or its code.[44] Its *regulability*, that is, is a function of its design. There are designs where behavior within the Net is beyond government's reach; and there are designs where behavior within the Net is fully within government's reach. My claim in this section is that government can take steps to alter the Internet's design. It can take steps, that is, to affect the regulability of the Internet.

I offer two examples that together should suggest the more general point.

1. Increasing Collective Regulability: Zoning. — Return to the problem of zoning in Section I. My claim was that in real space, the self-authenticating feature of being a kid makes it possible for rules about access to be enforced, while in cyberspace, where age is not self-authenticating, the same regulations are difficult to enforce.

One response would be to make identity self-authenticating by modifying the Net's code so that, when I connect to a site on the Net, information about me gets transmitted to the site. This transmission would enable sites to determine whether, given my status, I should be permitted to enter.

How?

In a sense, the Net already facilitates some forms of identification. A server, for example, can tell whether my browser is a Microsoft or Netscape browser; it can tell whether my machine is a Macintosh or Windows machine. These are examples of self-authentication that are built into the code of the Net (or http) already.

Another example is a user's "address." Every user of the Net has, for the time she is using the Net, an address known as an Internet Protocol (IP) address.[45] This IP address is unique; only one machine at any one

---

[44] By architecture or "design," I mean both the technical design of the Net, and its social or economic design. As I will describe more fully in note 105 below, a crucial design feature of the Net that will affect its regulability is its ownership. More precisely, the ability of government to regulate the Net depends in part on who owns the code of the Net.

[45] An IP address is:

> a 32-bit number that identifies each sender or receiver of information that is sent in packets across the Internet. When you request an HTML page or send e-mail, the Internet Protocol

time may have a particular address. Devices on the Net use this address to know where to send requested packets of data. But while these addresses are unique, there is no necessary link between an address and a person. Although some machines have "static" IP addresses that are permanently assigned to that machine, many have "dynamic" IP addresses that get assigned only for one session and may change when the machine reconnects to the Internet. Thus, although some information is revealed when a machine is on the Net, the *Internet* currently does not require any authentication beyond an IP address.

Other networks are different. *Intra*nets,[46] for example, are networks that connect to the Internet. These networks are compliant with the basic Internet protocols, but they layer onto these protocols other protocols as well. Among these are protocols that permit the identification of a user's profile by the controller of the intranet. Such protocols enable, that is, a form of self-authentication that facilitates identification. The extent of this identification varies. At one extreme are biometric techniques that would tie a physical feature of the user (fingerprint or eye scan) to an ID, and thus specifically identify the user; at the other extreme are certificates that would simply identify features of the person — that she is over eighteen, that she is an American citizen, etc.

It is beyond the scope of this essay to sketch the full range of these technologies. My aim is much more limited. It is enough here to show that identification is possible, and then to explain how the government might act to facilitate the use of these technologies.

For my claim in this section is this: if these technologies of identification were in general use on the Internet, then the *regulability* of behavior in cyberspace would increase. And government can affect whether these technologies are in general use.

---

part of TCP/IP includes your IP address in the message (actually, in each of the packets if more than one is required) and sends it to the IP address that is obtained by looking up the domain name in the URL you requested or in the e-mail address you're sending a note to. At the other end, the recipient can see the IP address of the Web page requestor or the e-mail sender and can respond by sending another message using the IP address it received.

IP address (Internet Protocol address) (visited Aug. 14, 1999) <http://www.whatis.com/ipaddres.htm>.

[46] Intranets are the fastest growing portion of the Internet today. They are a strange hybrid of two traditions in network computing — one the open system of the Internet, and the other the control-based capability of traditional proprietary networks. An intranets mixes values from each to produce a network that is interoperable but that gives its administrator a great deal of control over user behavior. An "Internet" with control is what our intranet is becoming. *See, e.g.*, Steve Lohr, *Internet Future at I.B.M. Looks Oddly Familiar*, N.Y. TIMES, Sept. 2, 1996, at 37 ("[I]nvestment in the United States in intranet software for servers, the powerful computers that store network data, would increase to $6.1 billion by 2000 from $400 million this year. By contrast, Internet server software investment is projected to rise to $2.2 billion by 2000 from $550 million."); Steve Lohr, *Netscape Taking on Lotus With New Corporate System*, N.Y. TIMES, Oct. 16, 1996, at D2 ("Netscape executives pointed to studies projecting that the intranet market will grow to $10 billion by 2000.").

So focus on the single issue of protecting kids from adult speech on the Net.[47] Congress has now twice tried to enact legislation that would regulate the availability of such speech to "minors."[48] At the time of this writing, it has twice failed.[49] Its failure in both cases came from a certain clumsiness in execution. In the first case, Congress tried to regulate too broadly; in the second, it corrected that problem but burdened the wrong class of users — adults.[50]

Consider a third alternative, which in my view would not raise the same constitutional concerns.[51] Imagine the following statute:

> *1. Kids-Mode Browsing*: Manufacturers of browsers will enable their browsers to browse in "kids-mode" [KMB]. When enabled, KMB will signal to servers that the user is a minor. The browser software should enable password protection for non-kids-mode browsing. The browser should also disable any data collection about the user of a kids-mode browser. In particular, it will not transmit to a site any identifying personal data about the user.
>
> *2. Server Responsibility*: When a server detects a KMB client, it shall (1) block that client from any material properly deemed "harmful to minors"[52] and (2) refrain from collecting any identifying personal data about the user, except data necessary to process user requests. Any such data collected shall be purged from the system within *X* days.

Rhetoric about cyberspace unregulability notwithstanding, notice how simply this regulation could be implemented and enforced. In a world

---

47 *See Developments*, *supra* note 10, at 1637–43 (suggesting code solutions to this problem).

48 *See* Child Online Protection Act (COPA), Pub. L. No. 105-277, 112 Stat. 2681 (1998) (to be codified at 47 U.S.C. § 231); Telecommunications Act of 1996 (Communications Decency Act, or CDA), Pub. L. No. 104-104, §§ 501–502, 505, 508–509, 551–552, 110 Stat. 56, 133–43 (1996).

49 *See* Reno v. ACLU, 521 U.S. 844, 849 (1997) (striking down part of the CDA); ACLU v. Reno, 31 F. Supp. 2d 473, 492–98 (E.D. Pa. 1999) (granting plaintiffs' motion for a preliminary injunction because of the substantial likelihood of success on their claim that COPA is presumptively invalid and subject to strict scrutiny).

50 The CDA regulated "indecent" speech, which the Court has not recognized (outside of the context of broadcasting) as a category of speech subject to Congress's power of proscription. COPA regulates the actions of adults who wish to get access to adult speech. As I describe below, a less restrictive alternative would only slightly burden adults.

51 While this idea has been out there for some time, I am grateful to Mark Lemley for prompting me to recognize it. For a more formal analysis of the question whether this alternative is constitutional, see Lawrence Lessig & Paul Resnick, *The Constitutionality of Mandated Access Controls*, 98 MICH. L. REV. (forthcoming fall 1999). A less obligatory statute might also be imagined — one that simply mandated that servers recognize and block kids-identifying browsers. Under this solution, some browser companies would have a market incentive to provide KMBs; others would not. But to create that incentive, the signal must be recognized.

Note that Apple Computer has come close to this model with its OS 9. OS 9 enables multiple users to have access to a single machine. When the machine is configured for multiple users, each user must provide a password to gain access to his or her profile. It would be a small change to add to this system the ability to signal that the user is a kid. That information could then be reported as part of the machine identification.

52 *See* Ginsberg v. New York, 390 U.S. 629, 641 (1968) ("To sustain state power to exclude material defined as obscenity . . . requires only that we be able to say that it was not irrational for the legislature to find that exposure to material condemned by the statute is harmful to minors.").

where ninety percent of browsers are produced by two companies,[53] the code writers are too prominent to hide. And why hide anyway — given the simplicity of the requirement, compliance would be easy. In a very short time, such a statute would produce browsers with the KMB feature, at least for those parents who would want such control on machines in their home.

Likewise, it would be easy for sites to develop software to block access if the user signals that s/he is a kid. Such a system would require no costly identification, no database of ID's, and no credit cards. Instead, the server would be programmed to accept users who do not have the kids-mode selected, but to reject users that do.

My point is not to endorse such legislation: I think the ideal response for Congress is to do nothing. But if Congress adopted this form of regulation, my view is that it would be both feasible and constitutional. Netscape and Microsoft would have no viable First Amendment objection to a regulation of their code;[54] and websites would have no constitutional objection to the requirement that they block kids-mode browsers.[55] No case has ever held that a speaker has a right not to be subject to any burden at all, if the burden is necessary to advance a compelling state need; the only requirement of *Reno v. ACLU*[56] is that the burden be the least restrictive burden.[57] The KMB burden, I suggest, would be the least restrictive.

---

[53] *See* Greg Meckbach, *Microsoft's IE Tops in New Poll; Browser Gains Edge over its Netscape Competitor as Organizations Warm to Pre-Installed Software*, COMPUTING CAN., July 9, 1999, at 25 (citing findings by Positive Support Review, Inc., that Microsoft's Internet Explorer has 60.5% of the market share compared to 35.1% held by Netscape's Navigator).

I make an important qualification to this argument below. *See infra* pp. 534–36.

[54] *Cf.* Junger v. Daley, 8 F. Supp. 2d 708, 717–18 (N.D. Ohio 1998) (holding that "source code is by design functional" and that "[b]ecause the expressive elements of encryption source code are neither 'unmistakable' nor 'overwhelmingly apparent,' its export is not protected under the First Amendment"). Ultimately, though, the question whether a particular code is expressive or purely functional is decided on a case-by-case basis, and is one over which courts are presently in disagreement. *Compare id. and* Karn v. United States Dep't of State, 925 F. Supp. 1, 9 n.19 (D.D.C. 1996) (stating that "[s]ource codes are merely a means of commanding a computer to perform a function"), *with* Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1141 (9th Cir. 1999), *reh'g granted*, 1999 WL 782073 (concluding that "encryption software, in its source code form and as employed by those in the field of cryptography, must be viewed as expressive for First Amendment purposes"). For a useful article criticizing the breadth of the district court's decision in *Bernstein*, see Patrick Ian Ross, *Computer Programming Language*, 13 BERKELEY TECH. L.J. 405 (1998).

[55] At least so long as *Ginsberg* is the law. *See Ginsberg*, 390 U.S. at 633 (affirming the conviction of a store operator for selling to a minor material harmful to minors).

[56] 521 U.S. 844 (1997).

[57] *See id.* at 874. Thus I agree with the reading of *Reno* offered by Professor Volokh. *See* Eugene Volokh, *Freedom of Speech, Shielding Children, and Transcending Balancing*, 1997 SUP. CT. REV. 141, 141–42 ("Speech to adults may be restricted to serve the compelling interest of shielding children, but only if the restriction is the least restrictive means of doing so.").

The KMB system would also be relatively effective.[58] Imagine that the FBI enabled a bot to spider (search) the Net with a kids-mode browser setting switched on. The bot would try to gain access to sites; if it got access, it would report to the investigator as much of the content as it could extract. This content could then be analyzed, and the content that was arguably adult would then be flashed back to an investigator. That investigator would determine whether these sites were indeed "adult sites"; and if they were, the investigation would proceed against these sites. The result would be an extremely effective system for monitoring access to adult content on the web. It should therefore render COPA unconstitutional, since it represents a less restrictive alternative to the same speech-regulating end.

For the purposes of zoning adult speech, this change would fundamentally alter the regulability of the Net. And it would do so not by directly regulating children, but by altering one feature of the "architecture"[59] of the Net — the ability of a browser to supply certain information about the user. Once this facility was built into browsers generally, the ability of suppliers of adult speech to discriminate between adults and kids would change. This regulation of code would thus make possible the regulation of behavior.

2. Increasing Individual Regulability: Privacy. — Zoning porn is an example of top-down regulation. The state, presumably with popular support, imposes a judgment about who should get access to what. It imposes that judgment by requiring coders to code in conformance with the state's rules. The state needs to impose these rules because the initial architecture of the Net disables top-down regulation. (That's a virtue, not a vice, most might think. But the state is not likely one of the "most.") That architecture interfered with top-down control. The response was to modify that architecture.

---

58 My claim is not that the regulation would be perfectly effective, because of course no regulation is perfectly effective. Kids often know more about computers than their parents and can easily evade the controls their parents impose. The relevant question, however, is whether the ability to evade parental control is easier with the adult-ID system than with the kids-ID system. To evade the adult-ID system, kids would need only a valid credit card number — which would clear them in some cases without charging the credit card site. More importantly, the existing state of parental knowledge is not a fair basis on which to judge the potential effectiveness of a system. Parents would have an incentive to learn if the technologies for control were more simply presented.

The question of effectiveness also arises in the context of foreign sites, as many foreign sites are unlikely to obey a regulation of the United States government. But again, the relevant question is whether they are more likely to respect an adult-ID law or a kids-ID law. My sense is that they would be more likely to respect the least restrictive law.

59 My use of the term "architecture" is somewhat idiosyncratic, but not completely. I use the term as it is used by Charles R. Morris and Charles H. Ferguson. *See* Charles R. Morris & Charles H. Ferguson, *How Architecture Wins Technology Wars*, HARV. BUS. REV., Mar.–Apr. 1993, at 86. My use of the term does not quite match the way in which it is used by computer scientists, except in the sense of a "structure of a system." *See, e.g.*, PETE LOSHIN, TCP/IP CLEARLY EXPLAINED 394 (2d ed. 1997) (defining "architecture").

The problem with privacy in cyberspace is different. The feature of the Net that creates the problem of privacy (the invisible, automatic collection of data) interferes with bottom-up regulation — regulation, that is, imposed by individuals through individual choice.

Architectures can enable or disable individual choice by providing (or failing to provide) individuals both with the information they need to make a decision and with the option of executing that decision. The privacy example rested on an architecture that did not enable individual choice, hiding facts necessary to that choice and thereby disabling bottom-up control. Self-regulation, like state-regulation, depends upon architectures of control. Without those architectures, neither form of regulation is possible.

But again, architectures can be changed. Just as with the zoning of porn, architectures that disable self-regulation are subject to collective choice. Government can act to impose a change in the code, making self-regulation less costly and thereby facilitating increased self-regulation.

Here the technique for imposing this change, however, is a traditional tool of law. The problem of protecting privacy in cyberspace comes in part from an architecture that enables the collection of data without the user's consent.[60] But the problem also comes from a background regime of entitlement that does not demand that the collector obtain the user's consent. Because the user has no property interest in personal information, information about the user is free for the taking. Thus architectures that enable this taking are efficient for the collector, and consistent with the baseline legal regime.

The trick would be to change the legal entitlements in a way sufficient to change the incentives of those who architect the technologies of consent. The state could (1) give individuals a property right to data about themselves, and thus (2) create an incentive for architectures that facilitate consent before turning that data over.[61]

The first step comes through a declaration by the state about who owns what property.[62] The government could declare that information about individuals obtained through a computer network is owned by the

---

[60] *Cf.* JOEL R. REIDENBERG & PAUL M. SCHWARTZ, 2 ON-LINE SERVICES AND DATA PROTECTION AND PRIVACY — REGULATORY RESPONSES 65–84 (1998) ("[T]ransparency is one of the core principles of European data protection law. This standard requires that the processing of personal information be structured in a fashion that is open and understandable for the individual. Moreover, transparency requires that individuals have rights of access and correction to stored personal information.").

[61] *Cf.* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1092 (1972) (arguing that when the state protects an entitlement with a property rule, "someone who wishes to remove the entitlement from its holder must buy it from him in a voluntary transaction in which the value of the entitlement is agreed upon by the seller").

[62] There is an important constitutional issue that I am ignoring here — whether the state can grant a property interest in private "data."

individuals; others could take that information, and use it, only with the consent of those individuals. This declaration of rights could then be enforced in any number of traditional ways. The state might make theft of such information criminal, or provide special civil remedies and incentives to enforce individual rights if such information is taken.

This first step, however, would be useful only if it induced the second — this time, a change in the architecture of the space, and not just in the laws that govern that space. This change in the architecture would aim to reduce the costs of choice, to make it easy for individuals to express their preferences about the use of personal data, and easy for negotiations to occur about that data. Property regimes make little sense unless transactions involving that property are easy. And one problem with the existing architectures, again, is that it is hard for individuals to exercise choice about their property.

But there are solutions. The World Wide Web Consortium, for example, has developed a protocol, called P3P,[63] for the control of privacy data. P3P would enable individuals to select their preferences about the exchange of private information, and then enable agents to negotiate the trade of such data when an individual connects to a given site. If, for example, I never want to visit a website that logs my IP address and the pages I have visited, P3P could express this preference. When I visit a site, an agent would negotiate with the site about my access preferences.

P3P functions as a language for expressing preferences about data and as a framework within which negotiations about those preferences could be facilitated. It would, in other words, be a framework within which individuals could better regulate their lives in cyberspace.[64]

But without state intervention, it is not clear that such a framework could develop. P3P creates burdens that websites will not assume in a world where they can get the same information for free. Only by changing the incentives of these sites — by denying sites free access to this information — can we expect to create a sufficient incentive for them to adopt technologies that facilitate purchase. Establishing a property interest in privacy data would create such an incentive; and it is the government that then facilitates that interest.

There are plenty of problems with P3P, and there are alternatives that may function much better.[65] But my purpose has not been to endorse a

---

[63] *See Platform for Privacy Preferences (P3P) Syntax Specification: W3C Working Draft* (visited Aug. 14, 1999) <http://www.w3.org/TR/WD-P3P10-syntax/>.

[64] *See Developments*, *supra* note 10, at 1645–48 (describing P3P). My approach sees the solutions of both law and code as inextricably linked. The change in legal entitlement is necessary, in my view, to create the incentives for the code solution to emerge.

[65] P3P has been the object of a number of criticisms and concerns. First, P3P by itself does nothing to ensure that web service providers will comply with the privacy agreements reached through P3P negotiations. *See* Graham Greenleaf, *An Endnote on Regulating Cyberspace: Architecture vs. Law?*, 21 U. NEW S. WALES L.J. 593, 615 (1998). Second, P3P might actually lead to an increase in the exploita-

particular solution. My purpose has been to show the possible need for collective action, even simply to enable individual control. Existing architectures disable the incentives necessary to protect privacy; existing architectures benefit consumers of private information, while disabling choice by the individuals who provide private information. The success of a policy of enabling choice will therefore require collective action.

* * *

3. Conclusions Regarding Architecture and Regulability. — Regulations can come from either direction — some from the top, others from the bottom. My argument in this section has been that the regulability of either form depends upon the architecture of the space, and that this architecture can be changed.

The code of cyberspace might disable government choice, but the code can disable individual choice as well. There is no natural and general alignment between bottom-up regulation and the existing architecture of the Internet. Enabling *individual* choice may require collective modification of the architecture of cyberspace, just as enabling *collective* choice may require modification of this architecture. The architecture of cyberspace is neutral; it can enable or disable either kind of choice. The choice about which to enable, however, is not in any sense neutral.

B. Code Displacing Law

The argument so far is that law can change the constraints of code, so that code might regulate behavior differently. In this section, I consider the opposite claim — that code might change the constraints of law, so that law might (in effect) regulate differently. The key is the qualifying phrase *in effect*, for in my examples the code does not achieve an actual change in the law. The law on the books remains the same. These in-

---

tion of personal information by allowing popular websites to condition entry on the revelation of highly personal information, thus giving web users the less than desirable choice of forgoing the sites altogether or caving in to overly intrusive requests for information. *See* Simson L. Garfinkel, *The Web's Unelected Government*, TECH. REV., Nov.–Dec. 1998, at 38, 44; Greenleaf, *supra*. Third, P3P will most likely entail the social cost of increased access fees since "much of the personal information that is gathered online is used to target Internet advertising and because advertising is a major source of revenue for site providers, the concealment of personal information may limit site providers' ability to attract advertising and thus impair a major source of revenue." *Developments*, *supra* note 10, at 1648 (footnotes omitted). Fourth, "[t]he online concealment of real-space identity . . . [made possible by P3P] may create a disincentive [for web users] to cooperate and may encourage socially reckless behavior." *Id.* (footnotes omitted). Another concern with P3P involves the:

> critical question . . . [of] [w]hat will be the default settings provided to users[.] Few computer users ever learn to change the preference settings on their software. Therefore, the way a Web browser equipped with P3P sets itself up by default is the way the majority of the Internet population will use it.

Garfinkel, *supra*, at 44, 46. There are also a number of private solutions to the problem of privacy in data. For a variety of anonymizers, infomediaries, and secure servers and browsers, see *Online Privacy Alliance: Rules and Tools for Protecting Personal Privacy Online* (visited Sept. 30, 1999) <http://www.privacyalliance.org/resources/rulesntools.shtml>.

stead are examples of the code changing the effectiveness of a law. They are, in other words, examples of how indirect effects of the code might alter the regulation or policy of the law.

In such cases, lawmakers face a choice. Where architectures of code change the constraints of law, they in effect displace values in the law. Lawmakers will then have to decide whether to reinforce these existing values, or to allow the change to occur. In the examples I select here, my bias is in favor of the values of the law, although there are many examples that go the other way too. My point is not that the law should always respond; often the market will be enough. My point is only to show why it might need to respond.

My examples are drawn from the law of intellectual property and from the law of contract. In both examples, I identify public values that get displaced by the emerging architectures of cyberspace. These architectures, I argue, enable a system that too perfectly protects intellectual property and too completely disables the influence of public law in contracts. Code here threatens to displace public law values, forcing a choice whether to permit this potential displacement.

1. Code Displacing Law: Intellectual Property. — We have special laws to protect against the theft of autos, or boats.[66] We do not have special laws to protect against the theft of skyscrapers. Skyscrapers take care of themselves. The architecture of real space, or more suggestively, its real-space code, protects skyscrapers much more effectively than law. Architecture is an ally of skyscrapers (making them impossible to move); it is an enemy of cars and boats (making them quite easy to move).

On this spectrum from cars to very big buildings, intellectual property is somewhat like cars, and quite unlike large buildings. Indeed, as the world is just now, intellectual property fares far worse than cars and boats. At least if someone takes my car, I know it; I can call the police, and they can try to find it. But if someone takes an illegal copy of my article (copying it without paying for it), then I do not necessarily know. Sales might go down, my reputation might go up (or down), but there is no way to trace the drop in sales to this individual theft, and no way to link the rise (or fall) in fame to this subsidized distribution.

When theorists of the Net first thought about intellectual property, they argued that things were about to get much worse. "Everything [we know] about intellectual property," we were told, "is wrong."[67] Property could not be controlled on the Net; copyright made no sense.[68] Authors

---

66 Under the Model Penal Code, on which many state criminal codes are modeled, the theft of an automobile, airplane, motorcycle, motor boat or "other motor-propelled vehicle" is a felony. MODEL PENAL CODE § 223.1(2)(a) (1962).

67 John Perry Barlow, *The Economy of Ideas*, WIRED, Mar. 1994, at 84.

68 *See, e.g.*, Esther Dyson, *Intellectual Value*, WIRED, July 1995, at 136, 138–39 ("Controlling copies . . . becomes a complex challenge. You can either control something very tightly, limiting distribution

would have to find new ways to make money in cyberspace, because the technology had destroyed the ability to make money by controlling copies.[69]

The reasons were plain: the Net is a digital medium. Digital copies are perfect and free.[70] One can copy a song from a CD into a format called MP3. The song can then be posted on USENET to millions of people for free. The nature of the Net, we were told, would make copyright controls impossible. Copyright was dead.

There was something odd about this argument, even at its inception. It betrayed a certain is-ism — "the way cyberspace is is the way it has to be." Cyberspace was a place where "infinite copies could be made for free." But why exactly? Because of its code. Infinite copies could be made because the code permitted such copying. So why couldn't the code be changed? Why couldn't we imagine a different code, one that better protected intellectual property?

At the start of this debate, it took real imagination to envision these alternative codes. It wasn't obvious how a different architecture could enable better control over digital objects. But we're far enough along now to see something of these alternatives.[71]

Consider the proposals of Mark Stefik of Xerox PARC. In a series of articles,[72] Stefik describes what he calls "trusted systems" for copyright management. Trusted systems enable owners of intellectual property to control access to that property, and to meter usage of the property perfectly. This control would be coded into software that would distribute, and hence regulate access to, copyrighted material. This control would be

---

to a small, trusted group, or . . . eventually your product will find its way to a large nonpaying audience — if anyone cares to have it in the first place."); John Perry Barlow, *A Cyberspace Independence Declaration* (Feb. 9, 1996) <http://www.eff.org/barlow> ("Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are based on matter, There [sic] is no matter here.").

[69] *Cf.* Dyson, *supra* note 68, at 141 (suggesting, for example, that in the age of the Internet, "[s]uccessful [software] companies are adopting business models in which they are rewarded for services rather than for code;" and that "[t]he real value created by most software companies lies in their distribution networks, trained user bases, and brand names — not in their code").

[70] *See* NICHOLAS NEGROPONTE, BEING DIGITAL 58 (1995) ("In the digital world, not only the ease [of making copies] is at issue, but also the fact that the digital copy is as perfect as the original and, with some fancy computing, even better."); Barlow, *supra* note 67 ("In our world, whatever the human mind may create can be reproduced and distributed infinitely at no cost."); Dyson, *supra* note 68, at 137 ("[The Net] allows us to copy content essentially for free . . . ."); Nicholas Khadder, Project, *Annual Review of Law and Technology*, 13 BERKELEY TECH. L.J. 3, 3 (1998) ("Recently, for example, the Internet has enabled users to distribute and sell information very widely at a negligible marginal cost to the distributor.").

[71] *See Developments*, *supra* note 10, at 1650–51 (describing "[r]ights-management containers" as one such alternative).

[72] *See* Mark Stefik, *Letting Loose the Light: Igniting Commerce in Electronic Publication*, *in* INTERNET DREAMS: ARCHETYPES, MYTHS, AND METAPHORS 219, 226–27 (Mark Stefik ed., 1996); Mark Stefik, *Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing* [hereinafter Stefik, *Shifting the Possible*], 12 BERKELEY TECH. L.J. 137, 139–407 (1997); Mark Stefik, *Trusted Systems*, SCI. AM., Mar. 1997, at 78, 78–81.

extremely fine-grained and would enable the copyright holder an extraordinary control over copyrighted material.

Think of it like this: Today, when you buy a book, you have the "right" to do any number of things with that book. You can read it once, or 100 times. You can lend it to a friend. You can Xerox pages from it, or scan it into your computer. You can burn it. You can use it as a paperweight. You can sell it. You can store it on your shelf and never open it once.

Some of these things you can do because the law gives you the right to do so — you can sell the book, for example, because the copyright law explicitly gives you that right.[73] Some of these things you can do because there is really no way to stop you. A book seller might sell you the book at one price if you promise to read it once, and at a different price if you want to read it 100 times. But there is no way for the seller really to know whether you read it once or 100 times, and so there is no way for the seller to know whether you have obeyed the contract. In principle, the seller could include a police officer with each book, so that the officer followed you around and made sure that you used the book as you promised. But the costs of that are plainly prohibitive. The seller is stuck.

But what if each of these rights could be controlled, and each unbundled and sold separately? What if, that is, software could regulate whether you read the book once, or read it 100 times; whether you could cut and paste from it, or simply read it without copying; whether you could send it as an attached document to a friend, or simply keep it on your machine; whether you could delete it; whether you could use it in another work, for another purpose; or whether you could simply leave it on your shelf?

Stefik describes a network where this unbundling of rights is possible. He offers an architecture for the network that would allow owners of copyrighted materials to sell access to those materials on terms that the owners set, and an architecture that would enforce those contracts.

The details of the system are not important here.[74] The essence is simple enough to understand. Digital objects would be distributed within protocols that are layered onto the basic protocols of the Net. This more sophisticated system would function by interacting selectively with other systems. So a system that controlled access in this more fine-grained way would grant access to its resources only to another system that controlled access in the same fine-grained way. A hierarchy of systems would develop; and copyrighted material would be traded only within that system that controlled access properly.

Stefik has turned airplanes into skyscrapers — he has described a way to change the code of cyberspace to make it possible to protect intellectual property in a far more effective way than is possible in real space.

---

[73] *See* 17 U.S.C. § 109 (1994).

[74] For the technical details, see Stefik, *Shifting the Possible*, cited above in note 72, at 139–44.

Now imagine for a moment that a structure of trusted systems emerged. How would this change in code change the nature of copyright law?

Copyright law is an odd bird. It establishes a strange sort of property, at least in relation to other property. The Copyright Clause of the United States Constitution gives Congress the power to grant "Authors" an exclusive right over their "Writings" for "limited Times."[75] At the end of that time, the right becomes non-exclusive. The work enters the public domain. It is as if the ownership you have over your car were a lease, extending for four years, and then expiring, at which time your car is up for grabs.

The reasons for this limitation on copyright protection are many, though the reasons don't fully overlap. Some reasons are economic, and ultimately pragmatic. Property systems (costly and complex) are justified only if they produce some social good. In the case of tangible goods, the social good is obvious. The law protects my enjoyment of tangible property, such as my car. If you used it without my permission, I could not use it. If everyone could use it without my permission, there would be little reason for me to own it. By giving me the power to control its use, the law creates a benefit to my ownership, and therefore an incentive for me to seek ownership.

Intangible property is significantly different. Unlike your enjoyment of my car, your enjoyment of my poem will not interfere with my enjoying it at all. Intangible goods are non-rivalrous. When an idea is disseminated, its usefulness does not diminish. As Thomas Jefferson wrote: "[N]o one possesses the less, because every other possesses the whole of it. He who receives an idea from me, receives instruction himself without lessening mine; as he who lights his taper at mine, receives light without darkening me."[76] Thus while the law needs to protect tangible property both so that there is an incentive to produce, and also so that the owner can enjoy it, the law needs to protect intangible property only in order to create the incentive to produce.

But economics is not the only justification for limiting the "property-like" protection for intellectual property. Constitutional law is another.[77] Regulations of copyright are regulations of speech. The copyright law gives the copyright owner the power to control not only the exact copies, but also derivative works and performances of some works. These regulations of speech are in tension with the understanding that the law should

---

[75] U.S. CONST. art. I, § 8, cl. 8.

[76] Letter from Thomas Jefferson to Isaac M'Pherson (Aug. 13, 1813), *in* 6 THE WRITINGS OF THOMAS JEFFERSON 175, 180 (H.A. Washington ed., 1854).

[77] In the interest of disclosure, I am currently representing a client pro bono in a case which raises the question of the First Amendment limitations on the Copyright Clause. *See* Eldred v. Reno, No. 1:99CV00065 (D.D.C. 1999).

leave speech free. A compromise is found in the concept of a restricted copyright — one that protects a copyrighted work to the extent necessary to induce creation, but no more. As the Supreme Court said in *Harper & Row, Publishers, Inc. v. Nation Enterprises*,[78] the Framers intended copyright to serve as an "engine of free expression."[79] It is justified only so long as it serves as such an engine.

Finally, and relatedly, the limits on intellectual property reflect a commitment to an intellectual commons.[80] It is true that some commons face tragedies.[81] But once the incentive problem is solved, intellectual commons need face them no longer. The limitations on the scope of intellectual property law serve to fuel this intellectual commons — to generate a resource upon which others can draw.[82]

The essential nature of a commons is that each individual is free to use the commons without the permission of anyone else.[83] Or more narrowly, it is a commons if the individual is free from any content-based, viewpoint-based, or discretion-laden judgment about whether the commons can be used. I might have to pay a small fee to enter the park, but if I pay the fee, I have the right to enter. The park is a resource open to everyone. It is a space that individuals may occupy without asking the subjective permission of anyone else.[84]

These three justifications for limits on intellectual property overlap, but they are not coextensive. They all, for example, would justify some form

---

[78] 471 U.S. 539 (1985).

[79] *Id.* at 558.

[80] *See* Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354, 360–63 (1999); David Lange, *Recognizing the Public Domain*, 44 LAW & CONTEMP. PROBS., Autumn 1981, at 157, 175–76, 178 (likening intellectual property to terrain that can be spoiled by colonization); Jessica Litman, *The Public Domain*, 39 EMORY L.J. 965, 967, 1023 (1990) (noting that the "public domain is the law's primary safeguard of the raw material that makes authorship possible" and, thus, "permits the law of copyright to avoid a confrontation with the poverty of some of the assumptions on which it is based").

[81] *See* Garrett Hardin, *The Tragedy of the Commons*, 162 SCIENCE 1243 (1968), *reprinted in* PERSPECTIVES ON PROPERTY LAW 132, 133 (Robert C. Ellickson, Carol M. Rose & Bruce A. Ackerman eds., 2d ed. 1995).

[82] *See* Mark A. Lemley, *The Economics of Improvement in Intellectual Property Law*, 75 TEX. L. REV. 989, 1083–84 (1997) (arguing that "intellectual property represents a 'delicate balance' between the rights of intellectual property owners and the rights of users, among them the next generation of owners," and that certain limitations on the rights of intellectual property owners are therefore necessary to encourage improvements); Litman, *supra* note 80, at 968 ("The public domain should be understood not as the realm of material that is undeserving of protection, but as a device that permits the rest of the system to work by leaving the raw material of authorship available for authors to use."); Stephen M. McJohn, *Fair Use and Privatization in Copyright*, 35 SAN DIEGO L. REV. 61, 66 n.32 (1998) ("The public domain is itself a key resource for the further production of creative works.").

[83] *See, e.g.*, Hardin, *supra* note 81, at 133–34.

[84] *See* Benkler, *supra* note 80, at 360–64.

of "fair use" — a defense that the law of copyright gives users of copyrighted material.[85]

From an economic perspective, fair use can be justified either because the use is small relative to transaction costs of charging for the use, or because certain uses tend to increase the demand for copyrighted work generally. The right to use excerpts in a book review benefits the class of book authors generally, since it enables reviews of books that in turn increase the total demand for books.[86]

From a free speech perspective, the reach of a justification for fair use would depend upon the speech at issue. Melville Nimmer, for example, hypothesized a case in which First Amendment interests would justify fair use beyond the scope provided by copyright law.[87]

But from the perspective of the commons, what is important about fair use is not so much the value of fair use, or its relation to matters of public import. What is important is the right to use without permission. This is an autonomy conception. The right guaranteed is a right to use these resources without the approval of someone else.[88]

"Fair use" thus balances the rights of an individual author against the rights of a user under any of the justifications for the law of copyright. But it is clear, again, regardless of the justification, that the development of trusted systems threatens to change the balance. From the economic perspective, it threatens to empower individual authors against the interests of the class; from the constitutional perspective, it threatens to bottle up speech regardless of its relation to matters of public import; and from the perspective of the commons, it fundamentally changes the nature of access.

---

[85] *See* 17 U.S.C. § 107 (1994). Fair use guarantees that users of copyrighted material have a right to use that material in a limited way, regardless of the desires of the copyright owner. Thus, for example, I may parody a copyrighted work even if the author objects. For a discussion of the limits of parody as fair use, see Lisa Moloff Kaplan, Comment, *Parody and the Fair Use Defense to Copyright Infringement: Appropriate Purpose and Object of Humor*, 26 ARIZ. ST. L.J. 857, 864–82 (1994). *See also* McJohn, *supra* note 82, at 86–87, 94–95 (using the courts' application of fair use doctrine to parody as support for an argument that the role of fair use is broader than just a solution to the high transaction cost of licensing).

[86] *See* RICHARD A. POSNER, LAW AND LITERATURE 407 (2d ed. 1998); William M. Landes & Richard A. Posner, *An Economic Analysis of Copyright Law*, 18 J. LEGAL STUD. 325, 358–59 (1989).

[87] *See* Melville B. Nimmer, *Does Copyright Abridge the First Amendment Guarantees of Free Speech and Press?*, 17 UCLA L. REV. 1180, 1197–98 (1970) (arguing that the First Amendment would protect reprinting of photographs of the My Lai massacre even if barred by copyright law); *see also* Triangle Publications, Inc. v. Knight-Ridder Newspapers, Inc., 626 F.2d 1171, 1184 (5th Cir. 1980) (Tate, J., concurring) (arguing that "under limited circumstances, a First Amendment privilege may, and *should* exist where utilization of the copyrighted expression is necessary for the purpose of conveying thoughts or expressions"); Sid & Marty Krofft Television Prods., Inc. v. McDonald's Corp., 562 F.2d 1157, 1171 (9th Cir. 1977) ("There may be certain rare instances when first amendment considerations will operate to limit copyright protection for graphic expressions of newsworthy events."); Wainwright Sec. Inc. v. Wall St. Transcript Corp., 558 F.2d 91, 95 (2d Cir. 1977) (quoting Nimmer, *supra*, at 1200) ("Some day, [certain cases] may require courts to distinguish between the doctrine of fair use and 'an emerging constitutional limitation on copyright contained in the first amendment.'").

[88] *See supra* p. 528.

Within a structure of trusted systems, access is always and only with permission. The baseline is control, regardless of how far that control is exercised.

This is a problem particular to cyberspace. In real space, the law might guarantee me the right to fair use, or to make use of a work in the public domain. It guarantees me this right by giving me a defense if the owner of copyrighted work tries to sue me for taking her property. The law in effect then denies the owner any cause of action; the law withdraws its protection, and leaves the property within the commons.

But there is no similar guarantee with property protected by trusted systems.[89] There is no reason to believe that the code that Stefik describes would be a code that guaranteed fair use, or a limited term. Instead, the code of trusted systems could just as well protect material absolutely, or protect material for an unlimited term.[90] The code need not be balanced in the way that copyright law is. The code can be designed however the code writer wants, and code writers have little incentive to make their product imperfect.[91]

Trusted systems, therefore, are forms of privatized law. They are architectures of control that displace the architectures of control effected by public law. And to the extent that architectures of law are balanced between private and public values, we should worry if architectures of code become imbalanced. We should worry, that is, if they respect private values but displace public values.

It is impossible to predict in the abstract whether this will be the result of trusted systems. There is good reason to expect it, and little to suggest anything to the contrary. But my aim here is not to predict; my aim is to isolate a response. If privatized law displaces public values, should the public do anything?

2. Code Displacing Law: "Contracts." — Trusted systems are one example of code displacing law. A second is the law of contracts. There has been a great deal of talk in cyberspace literature about how, in essence, cyberspace is a place where "contract" rather than "law" will govern people's behavior.[92] AOL, for example, binds you to enter your name as you enter

---

89 *See* Stefik, *Shifting the Possible*, *supra* note 72, at 139–41.

90 *See id.* at 147.

91 *See Developments*, *supra* note 10, at 1649–56 (describing possible problems with a code solution to copyright infringement and arguing that, although government should not intervene in such solutions until the problems become manifest, legislative actions are appropriate if code solutions do in fact upset the balance of copyright law).

92 *See, e.g.*, Trotter Hardy, *Property (and Copyright) in Cyberspace*, 1996 U. CHI. LEGAL F. 217, 237 (1996) (concluding that "cyberspace should be at least as much, if not a more hospitable environment for transacting over property rights than 'real' space"); Raymond T. Nimmer, *Article 2B: An Introduction*, 16 J. MARSHALL J. COMPUTER & INFO. L. 211, 220 (1997) (arguing that contract should govern transactions about digital information because "[legislative or judicial] regulation of terms is unacceptable contract law in the information age").

its system. This is "like" a contract, these theorists say,[93] since you are bound by a set of constraints agreed to when you signed up for service with AOL. It is as if you simply promised to identify yourself as you entered AOL, and when you didn't identify yourself, AOL would then have a claim for breach of contract. It is "as if" but better: the obligation is imposed and enforced more efficiently than the same obligation imposed and enforced by contract law.

As a contracts professor, I find these claims odd. For code constraints alone are *not* "contracts." Sure, they are "like" contracts, in that they are both self-imposed constraints, but "like" is not "is." A "lion" is like a "cat," but you would be quite foolish to let your kid play with a lion. So too would you be foolish to assume code contracts are equally benign.

The dissimilarity is this: with every enforced contract — with every agreement that subsequently calls upon an enforcer to carry out the terms of that agreement — there is a judgment made by the enforcer about whether this obligation should be enforced. In the main,[94] these judgments are made by a court. And when a court makes such judgments, the court considers not just the private orderings constituted in the agreement before it, but also issues of public policy, which can, in some contexts, override these private orderings. When a court enforces the agreement, it decides how far the power of the court can be used to carry out the agreement. Sometimes the agreement will be carried out in full; but often, the agreements cannot be fully effected. Doctrines such as impossibility or mistake will discharge certain obligations. Rules about remedy will limit the remedies the parties can seek. Public policy exceptions will condition the kinds of agreements that can be enforced. "Contracts" incorporate all these doctrines, and it is the mix of this set of public values, and private obligations, that together produce what we call "a contract."

When the code enforces agreements, however, or when the code carries out a self-imposed constraint, these public values do not necessarily enter into the mix.[95] Consequences that a court might resist (forfeitures, for example[96]), the code can impose without hesitation. The code writer operates free of the implicit limitations of contract law. He or she can construct an alternative regime for enforcing voluntary constraints. And

---

[93] *Cf.* Nimmer, *supra* note 92, at 228–31, 234–35 (1997) (recommending changes in contract law that would make these types of arrangements enforceable contracts).

[94] Of course there are two important exceptions here that I have not yet worked through — arbitration agreements and alternative dispute resolution practices.

[95] My claim is not that carrying out contract-like commitments always involves values properly considered public. I don't think there is a constitutional issue raised every time my son trades the chore of doing the dishes with my daughter. But given the extent of commerce affected by Internet transactions, the fact that some contracts are really "private" does not mean cyberspace contracts generally are "private."

[96] *See* RESTATEMENT (SECOND) OF CONTRACTS: EXCUSE OF A CONDITION TO AVOID FORFEITURE § 229 (1979).

nothing requires or ensures that this alternative regime will comport with the values of the background regime we call "contract."

This is not necessarily to criticize the self-imposed constraints of code. Most of these constraints are, no doubt, harmless; and most would most likely be enforceable if translated into real contracts.

But it *is* to resist the opposite implication — that if these obligations are "like" contract, then they are as immune from questioning as the equivalent real-space obligations constituted by contract.

For again, in real space, one might well believe that a set of obligations imposed through contract was untroubling. Conditioned by antitrust law, limited by principles of equity, cabined by doctrines of mistake and excuse — the obligations would be checked by a court before the constraints were made effective. There is a structural safety check on obligations of this sort, which ensures that the obligations don't reach too deep. When intervening to enforce these obligations, a court would carry with it the collection of tools that contract law has developed to modify, or soften, the obligations that contract law might otherwise enforce.

The cyberspace analog has no equivalent toolbox. Its obligations are not conditioned by the public values that contract law embraces. Its obligations instead flow automatically from the structures imposed in the code. These structures serve the private ends of the code writer; they are a private version of contract law. But as the Legal Realists spent a generation teaching, and as we seem so keen to forget: contract law is *public* law. "Private public law" is oxymoronic.[97]

In a sense, this point about contracts is the same as the point about copyright. In both contexts, the *law* serves public values; in both contexts, a privatized regime for establishing a related protection is effected; in both contexts, we should ask whether this substitute should be allowed to displace those public values.

My answer in each case is no. To the extent that these code structures displace values of public law, public law has a reason to intervene to restore these public values. Whether and how are a different question. My point so far is just about identifying a reason to do so.

C. Law Regulating Code

My examples from the last section were instances in which code would displace values imbedded in the law. The examples in this section are familiar instances in which law can displace values in code. The two sets of examples suggest a more general point: Modalities compete. The values

---

[97] This is a familiar view. For a sample of such arguments, see Morris R. Cohen, *The Basis of Contract*, 46 HARV. L. REV. 553, 585–92 (1933); Morris R. Cohen, *Property and Sovereignty*, 13 CORNELL L.Q. 8, 21–30 (1927); and Robert L. Hale, *Bargaining, Duress, and Economic Liberty*, 43 COLUM. L. REV. 603, 626–28 (1943); Robert L. Hale, *Coercion and Distribution in a Supposedly Non-Coercive State*, 38 POL. SCI. Q. 470, 488–91 (1923).

implicit in a given modality of constraint, or in a given instantiation of that modality, may compete with the values in a different modality of constraint. This competition can induce a response. As code displaces law, law might respond to reclaim the values displaced. As law regulates code, code writers might respond to neutralize the effect of law.[98] Each modality functions as a kind of sovereignty. Each sovereignty competes with the others.

I've already sketched a couple examples of this competition. There are more examples of law regulating code.

Digital Telephone: When telephone networks went digital, governments lost an important ability to tap phones; the architecture of the digital network made tapping difficult, but the government has simply responded by mandating a different architecture, with a different design.[99]

Digital Audio Technology: DAT is a code that makes digital copies of digital audio. These digital copies are, in principle, perfect and limitless. Thus the code makes the control of copies difficult. Congress responded with regulations that required the code to limit the number of serial copies it could make and lower the quality if the number of copies exceeded some limit.[100]

Anti-Circumvention: Trusted systems, as I have described them, are systems that enable control over the distribution of digital objects through encryption technologies that make unauthorized use difficult. These technologies, however, are not perfect; there is code that could crack them. Thus the threat of this code is a threat to these systems of control. Last year, Congress responded to this threat by enacting an anti-circumvention provision in the Digital Millennium Copyright Act.[101] This provision makes it a felony to crack a protection regime, even if the use of the underlying material is not itself a copyright violation.[102]

V-Chip: The V-Chip modifies the code of television transmissions to facilitate ex ante discrimination in the shows available for viewing. Before the V-Chip, the code of television was unable to discriminate automatically based on the content of the show. This code made it difficult for

---

[98] For example, code writers might make their code available as open code, *see infra* note 105, or they might publish the relevant application programming interfaces (APIs) that make it simple to evade the government's regulation.

[99] *See* Communications Assistance of Law Enforcement Act (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. §§ 1001–1010) (requiring telephone companies to select a network architecture that facilitates wiretapping).

[100] *See* Audio Home Recording Act, 17 U.S.C. § 1002 (1994) (describing the requirement of conforming with a system that limits serial copying); *see also* U.S. DEP'T OF COMMERCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS 189–90 (1995) (briefly describing the newly required system).

[101] Digital Millennium Copyright Act § 1201, Pub. L. No. 105-304, 112 Stat. 2860, 2863–72 (1998).

[102] *See id.*

parents to exercise control over what their kids watched. Congress responded by requiring the use of television code that can recognize, and block, content on the basis of industry-generated ratings.[103]

Encryption: The government has conducted a long campaign to limit access to encryption technologies out of fear that encryption will make hiding evidence of a crime too easy. To address the problem of uncrackably encrypted messages, Congress has toyed with regulating encryption code directly. In September 1997, the House Commerce Committee came one vote shy of recommending a statute that would have required encryption technologies to allow law enforcement to intercept and decrypt information protected by the technology.[104]

These examples show that architectures of cyberspace can enable or disable the values implicit in law; law, acting on architectures in cyberspace, can enable or disable the values implicit in code. As one displaces the other, a competition could develop. Authors of code might develop code that displaces law; authors of law might respond with law that displaces code.

East Coast Code (written in Washington, published in the U.S. Code) can thus compete with West Coast Code (written in Silicon Valley, or Redmond, published in bits burned in plastic). Likewise authors of East Coast Code can cooperate with authors of West Coast Code. It is not clear which code one should fear more.[105] The conflict displaces values in both spheres, but cooperation threatens values as well.

My aim in this essay is not to work out the full range of this interaction.[106] Nor is it to predict which side will prevail. Instead, my objective here is to use the account so far to suggest the lessons that might be learned from a more complete account.

This conflict between code and law should push us to consider principle. We should think again about the values that should guide, or constrain, this conflict between authorities. In the last part below, I want to

---

103 *See* Implementation of Section 551 of the Telecomm. Act of 1996, Video Programming Ratings, Fed. Communications Comm'n, 13 F.C.C.R. 8232 (1998); Technical Requirements to Enable Blocking of Video Programming Based on Program Ratings, Fed. Communications Comm'n, 13 F.C.C.R. 11248 (1998).

104 *See* Security and Freedom Through Encryption (SAFE) Act, H.R. 695, 105th Cong. (1997).

105 I have made an important simplifying assumption in this analysis, which I do not make in other writings. *See* Lawrence Lessig, *The Limits in Open Code: Regulatory Standards and the Future of the Net*, 14 BERKELEY TECH. L.J. 759 (1999). My assumption is that these code writers — the targets of this regulation by the state — are writing closed, as opposed to open, code. Closed code is code that does not travel with its source code, and it is not easily modified. If a standard or protocol is built into this closed code, it is unlikely that users, or adopters of that code, can undo that standard. Open code is different. If the government mandated a given standard or protocol within an open code software design, users or adopters would always be free to accept or reject the government's portion of the design. Thus, if application space is primarily open-source software, the government's regulatory power is diminished.

106 *See id.* at 767–68 (elaborating on the conflict).

sketch two principles. These are by no means the only principles that ought to concern us; they are simply the two whose remedies seem least obvious. And they are two that might show us something about what a law of cyberspace might teach more generally.

III. LESSONS

I have sketched the story of an inevitable competition between a set of values aspired to by the law, and a set of values extant within a particular architecture of code. My claim has not been that the values in either are ever fully intended by any person or institution, nor that they are consistently understood. But whether the values are intended and however incompletely they are seen, they will unavoidably conflict. This conflict will often induce a response — often by law, at least, and sometimes by architects of code. My claim is that we can learn something from this response.

In this final section, I want to suggest three lessons that arise from this competition. The first is a lesson about limits on the power of law to regulate code. Not only is behavior more regulable under some architectures than others, but architectures themselves can be more or less regulable. This difference is a function less of code than of organizational design. As I will argue, how the code is *owned* will affect whether it can be regulated.

This lesson echoes a familiar point about political philosophy, with its valence inverted. In political philosophy, the argument is that property is a check on government; in the context of cyberspace, my claim is the opposite.

The second lesson is about transparency. It has long been a value in liberal constitutional regimes that regulation be transparent. The choice between regulating through law and regulating through code puts extraordinary pressure on that value. As others have noted, but as cyberspace will make systematically apparent, non-transparency can be an effective aid to regulation. Cyberspace will make non-transparency a constant option.

Finally, the third lesson is about tailoring. There are only a few contexts in constitutional law in which the government must narrowly tailor its regulation to a given state end. Laws involving speech and status are the two primary examples. But cyberspace will make far more salient the concern about the scope of an otherwise legitimate regulation. Regulation of architectures is sensitive and foundational, much like regulating the make-up of DNA. Tinkering ramifies.

A. The Limits on Regulability

I have argued that cyberspace is not inherently unregulable; that its regulability is a function of its design. Some designs make behavior more regulable; others make behavior less regulable. Government, I have claimed, can influence the design of cyberspace in ways that enhance government's ability to regulate.

There is an increasingly significant limit on the government's power to regulate. In an odd way, the power depends upon who owns the code. To the extent that the "application space" code of cyberspace is private — in a sense that I will describe below — government's power is increased. To the extent that the "application space" code of cyberspace is not private, but is instead held in a "commons," government's power is reduced.

By private, I mean that "application space" code is developed in the way in which most commercial code is now designed. Software companies design this code and sell it as a complete package. The product that they license does not contain the source code. The license does not give the user the right to modify the source code; the product is sold as is, and is expected to be used as is. The application's content and function are set by the seller; the user is not intended to have any role in its design. Though distributed through contract (licenses), this code is effectively the seller's property. The seller maintains an exclusive right over its design and development.

The alternative to this "commercial" model is the model of software development initially championed by the Free Software Foundation and, more recently, by the "Open Source" movement.[107] In this model, software is distributed with its source. Users are entitled to modify that source. Depending upon the license, they may be entitled to use that modified source in other commercial ventures. If a particular feature of a popular application is disagreeable, then users in this model would be entitled — and because the code comes with its source, able — to remove it.

This form of organization produces "commons code" — code that is neither owned privately nor owned by the state, but is instead held in a commons.[108] The essence of a commons is that no single person exercises an exclusive right over the code. Within the terms set by a range of licenses, anyone is free to take this code and develop it as he or she wishes.

---

[107] *See* Robert W. Gomulkiewicz, *How Copyleft Uses License Rights to Succeed in the Open Source Software Revolution and the Implications for Article 2B*, 36 HOUS. L. REV. 179, 182–85 (1999); Richard Stallman, *The GNU Operating System and the Free Software Movement*, *in* OPEN SOURCES: VOICES FROM THE OPEN SOURCE REVOLUTION 53, 56–57, 60–61, 69–70 (Chris DiBona, Sam Ockman & Mark Stone eds., 1999) [hereinafter OPEN SOURCES].

[108] This is not technically accurate, but the spirit of the metaphor is correct. To protect code from capture, software licenses place many conditions on the use of open code. Some conditions might seem technically inconsistent with the idea of a commons. Perhaps a better description would involve a self-enforcing commons. *See* Chris DiBona, Sam Ockman & Mark Stone, *Introduction* to OPEN SOURCES, *supra* note 107, at 1, 2–3 (describing the General Public License (GPL) issued to consumers of open source code). According to this description, GPL:

> basically says that you may copy and distribute the software licensed under the GPL at will, provided you do not inhibit others from doing the same, either by charging them for the software itself or by restricting them through further licensing. The GPL also requires works derived from work licensed under the GPL to be licensed under the GPL as well.

Id.

There is an extraordinary amount of literature about this Free Software or Open Source movement.[109] My aim here is to make one small point. To the extent that "application space" code is commons code, government's power to regulate it is weak; to the extent that "application space" code is private, government's power to regulate it is strong. Government's power, in this sense, depends upon the *organization* of the code that constitutes cyberspace — not just upon its architecture, but also upon who controls that architecture.

The reason is straightforward. Government regulates by getting people to behave in certain ways. When it regulates "code," it regulates by getting coders to write different code. When I described a regulation that might better zone "harmful to minors" speech, that scheme depended significantly upon the fact that a large portion of the browser market is controlled by a small number of firms. Because Netscape and Microsoft are large companies with real assets, they are easy targets of regulation.

But when no single organization or small number of organizations controls the code, or when the code, even if initially controlled by a company, is open and therefore modifiable, then the government has less ability to regulate the code. An unpopular requirement imposed upon commons code will simply be removed by people not so easily targeted by government. Expanding the number of people who can control the code thus contracts the power of government to regulate the code. Commons code is less easily controlled than private code.

Nothing in this claim is absolute. I am not arguing that organization of the code is the only factor that matters. Nor am I arguing that government can have no effect on commons code.[110] But an effect does exist, if only on the margin.

But the argument does suggest something important about the value of a commons, at least to those who would check the power of government to regulate. If code is conceived of as private property, and if strong property rights are given to the owners of that code, then the regime will enhance the government's power to regulate. The power to regulate would be still greater if the state controlled the code, for state code would be more regulable than private code. But state code would also be less efficient. We

---

109 *See id.*; Esther Dyson, *Open Mind, Open Source*, RELEASE 1.0, Nov. 1998, at 1; Gomulkiewicz, *supra* note 107; Lessig, *supra* note 105; Glyn Moody, *The Wild Bunch*, NEW SCIENTIST, Dec. 12, 1998, at 42; Tim O'Reilly, *Lessons from Open-Source Software Development*, COMM. ACM., April 1999, at 33; Larry Seltzer, *Software Returns to Its Source*, PC MAG., Mar. 23, 1999, at 166; Jeff Ubois, *Open-Source Tools Gain Credibility*, INFORMATIONWEEK, Mar. 22, 1999, at 1A; Rawn Shah, *Open Source Software for Windows NT: Developers of the World, Unite! You Have Nothing to Lose But Proprietary Control*, WINDOWS TECHEDGE (Feb. 1999) <http:// www.windowstechedge.com/wte/wte-1999–02/wte-02-oss_p.html>; Brough Turner, *Open Source Software Infuses CTI*, CTI MAG. (Mar. 1999) <http://www.tmcnet.com/articles/ctimag/0399/ 0399horizon.htm>.

110 *See* Lessig, *supra* note 105, at 767–68.

are beyond the days when bureaucrats produce; production is better left to the market.

Relative to commons code, however, private code is more regulable. For if property law allocates the right to control, then private property makes the right exclusive; commons property makes the right non-exclusive. Commons property identifies no single entity with an exclusive right to control. Thus, commons code produces many sources of control, and constrains the power of government to regulate.

Private property has often been thought of as a way to check state power. It has been criticized for creating its own problem of concentrated power, but many believe that to be a less dangerous power. Whether or not that is true, understanding the role the code might play in the regulation of behavior in cyberspace throws into relief an observation about property that might otherwise be missed. Exclusive rights may be necessary to create incentives for creative activity within cyberspace; these rights may be justified by an increase in efficiency. But they also help rationalize a power of control. To the extent that a constitution aims at checking such government power, it must reckon with the increase in this power that exclusive rights in cyberspace will generate.

B. Questions About Law's Regulation of Code

To the extent that the organization of code remains subject to the influence of government, there are two issues that cyberspace will render more salient. One is the reach of such regulation — the question whether it is narrowly tailored to a legitimate end. The other is the transparency of this regulation — whether government-imposed constraints are recognized as constraints, and as constraints imposed by the government.

My claim has not been that this form of regulation (through architecture as well as law) is new with cyberspace; my claim, at most, is that its significance is new. Although in the past, in limited contexts, the state has had an opportunity to regulate in a way that would itself increase regulability,[111] it has not had this opportunity in such a fundamental way.

---

[111] *See, e.g.*, Robert L. Stern, *The Commerce Clause Revisited — The Federalization of Intrastate Crime*, 15 ARIZ. L. REV. 271, 274–76 (1973) (discussing United States v. Five Gambling Devices, 346 U.S. 441 (1953), in which the Court struck down § 3 of the Johnson Act, 64 Stat. 1135 (1951), which required manufacturers and dealers to file monthly records of sales and deliveries and to register annually with the Attorney General). The authority for the "required records doctrine," which exempts "required records" from Fifth Amendment protection, is *Shapiro v. United States*, 335 U.S. 1, 7–15 (1948); but the doctrine has been limited by *Albertson v. Subversive Activities Control Board*, 382 U.S. 70, 77–78 (1965), which restricted the application of the required records/self reporting doctrine to genuine regulatory purposes. *See also* Haynes v. United States, 390 U.S. 85, 95–100 (1968) (finding reporting requirements in violation of the Fifth Amendment because they were not regulatory in nature); Grosso v. United States, 390 U.S. 62, 66–69 (1968) (same); Marchetti v. United States, 390 U.S. 39, 54–57 (1968) (same).

1. Over-Inclusiveness. — The first question that code regulation raises is a general question of over-inclusiveness. For a given objective, there are any number of ways to craft a code solution. Some will be narrower than others. By narrow, I mean less generalizable — these code solutions will solve one problem, but not enable the regulation of many others. And one "constitutional" question is whether there is a value in narrowing the scope of regulation-enabling regulations.

Two examples will make the point. In the Digital Millennium Copyright Act, Congress included an "anti-circumvention" provision.[112] This provision regulates efforts to circumvent technologies designed to protect copyrighted material. If you attempt to evade these technologies, you will have committed a felony. Or analogously, if you try to pick the lock, you will have committed the trespass.

The problem with this structure, however, is that it gives more protection than would the underlying copyright law. As critics of the anti-circumvention law pointed out,[113] the law makes it a felony to circumvent these technologies even when the use made of the underlying material would not have been a copyright violation.

Yet the anti-circumvention provision punishes a circumvention that simply enables a fair use. The law protects the code, then, more than the law protects the underlying copyrighted material.

It would have been simple to construct a circumvention law that was not overbroad in this way. The law, for example, could have made circumvention an aggravating factor in any prosecution for copyright violation. But by protecting the code more than the copyright, the law creates an incentive for the privatized copyright that I described in Part II. The law protects, that is, schemes whose ultimate effect may well be to displace the balance that copyright law strikes.

Some may justify this form of regulation as a kind of trespass law. Under this conception, anti-circumvention simply protects property owners from unauthorized access to their property. But the metaphor here is dangerous. If the anti-circumvention provision reached only efforts to hack into a computer system, then "trespass" would be a useful metaphor. But to the extent that the provision aims at rendering intellectual property more like real property by protecting against access to information, rather than against access to computers, then the metaphor of "trespass" is not helpful. I do not trespass on your idea merely because I think it.

A second example of narrow tailoring is more troubling. I described in Part II a scheme for facilitating the zoning of speech in cyberspace. In my

---

[112] *See* Digital Millennium Copyright Act § 1201, Pub. L. No. 105-304, 112 Stat. 2860, 2863–72 (1998).

[113] *See, e.g.*, Pamela Samuelson, *The Digital Rights War*, WILSON Q., Autumn 1998, at 48, 52–53; Pamela Samuelson, *A Look at . . . Whose Ideas, Anyway? Facing a Pay-Per-Use Future*, WASH. POST, Nov. 1, 1998, at C3.

view, the law could steer the architecture of cyberspace toward an ID-enabled space. By creating the incentive for individuals to carry digital IDs, or by mandating systems that check for digital IDs, the law could induce the supply of IDs, and thereby increase regulability.

There are many possible designs for an ID-enabled cyberspace, however. These various designs generally have different consequences for the regulability of cyberspace. I described in Part II one version of a kids-ID. This would be a browser that hid personal information about the user, but signaled that the user was a minor. The design would make it possible for servers with adult material to identify the client as a kid, and thus deny access; it would also enable sites that collect data to comply with laws banning the collection of data from kids.

An alternative ID-enabled cyberspace would be one that created incentives for users to carry digital IDs.[114] These digital certificates would verify certain facts about the holder of the certificate — for example, the name, age, citizenship, and sex of the holder.

For purposes of controlling adult content, the only essential fact of the certificate would be age. And just as the kids-ID might enable other regulations related to being a kid, so too would an age-ID enable other regulations related to being an adult, such as regulations of gambling or voting.

But to the extent that such IDs certify more than age, they facilitate a vastly increased scope for regulation. If they certify citizenship or residence, they enable regulations that would condition access on these features. The more the IDs certify, the more zoning the system enables.

If the narrow aim of a regulation by Congress were to protect kids, then the least restrictive means of doing so would be the kids-mode browser. But if the Court disagrees, then overbreadth may become a problem. For by creating the incentives for broader IDs, the state could create the incentives necessary to facilitate much broader regulation of behavior in cyberspace. Such regulation would extend beyond the state's legitimate interests in regulation, and facilitate regulation far beyond efforts to limit access to adult material.

In the anti-circumvention and the KMB examples, the structure of potential regulation is the same. In both, at least two changes in architecture might accomplish a state end. One change facilitates that end alone; the other facilitates that end and, as a byproduct, creates the opportunity for regulation beyond that end. In the case of anti-

---

114 The government is already exploring this idea, but in my view, not very well. *See GSA's Federal Technology Service Issues ACES RFP* (visited Oct. 4, 1999) <http://www.gsa.gov/ aces/rfpannc.html> ("ACES [Access Certificates for Electronic Services] is intended to provide identification, authentication, and non-repudiation via the use of digital signature technology as a means for individuals and business entities to be authenticated when accessing, retrieving, and submitting information with the government.").

circumvention, that additional regulation is private regulation; in the case of IDs, that additional regulation is public regulation.

The question in each case is whether anything tilts in favor of the narrower rather than the broader regulation. Within the context of speech regulation, the value of free speech obviously does. But ID regulation is ambiguously related to speech. ID regulation could be advanced for reasons unrelated to speech. And if it were — for example, to facilitate online banking or credit card use — then the same question about by-products would remain. The government might have a legitimate need to regulate to encourage identification, but the consequence of increased identification might be to flip the unregulability of the space generally.

2. Transparency. — A second problem with the law's regulation of code is the lack of transparency. When the state demands that individuals behave in a given way, the individuals recognize that it is the state that is regulating. If they don't like that regulation, they can elect representatives who will repeal it. Regulation is thereby checked by the political process.[115]

Transparency, traditionally, has also been a value that constrains the promulgation of regulation. Although the Framers kept their deliberations secret, and although the Senate preserved this secrecy until 1795,[116] the rule of law has always required that a law be public before it goes into effect. The Administrative Procedure Act (APA) pushed this value even further — in response to the emerging administrative state, the APA established procedures that demanded openness in the administrative process.[117]

But what if regulation could be secret — or more precisely, what if the fact that a government was regulating in a certain way could be kept secret? Then this constraint of political accountability would disappear. Because it would be unclear that the source of the regulation is the government, the government could achieve its goal without paying the political price or diminishing the effectiveness of the regulation.

The case of *Rust v. Sullivan*[118] is an example of the power of nontransparency. The Reagan Administration was opposed to abortion. One class of women who might be deterred from abortion consisted of those who

---

115 *Cf.* JOHN RAWLS, A THEORY OF JUSTICE 133 (1971) ("A third condition [for a concept of right] is that of publicity . . . . The point of the publicity condition is to have the parties evaluate conceptions of justice as publicly acknowledged and fully effective moral constitutions of social life."); Meir Dan-Cohen, *Decision Rules and Conduct Rules: On Acoustic Separation in Criminal Law*, 97 HARV. L. REV. 625, 667–73 (1984) (assessing arguments for transparency while concluding that transparency also carries significant costs).

116 *See* RICHARD ALLAN BAKER, THE SENATE OF THE UNITED STATES: A BICENTENNIAL HISTORY 24–25 (1988).

117 *See* Administrative Procedure Act, 5 U.S.C. § 553 (1994) (requiring legally binding rules to be promulgated through a notice and comment procedure).

118 500 U.S. 173 (1991).

visited family planning clinics. Obviously, given *Roe v. Wade*,[119] the government is constrained in the means it might select to deter abortions. Though the government need not fund abortion, it cannot ban all abortion. Although it might argue against abortion — for example, by posting signs reading "the Administration believes choosing life is better than choosing abortion" in any government-funded family planning clinic — these postings would likely be ineffective. Warnings from the government would be treated merely as warnings from the government — the product of politics, many would believe, and little more.

Thus the Reagan Administration chose a different and more effective technique. It prohibited doctors in family planning clinics from recommending or discussing abortion as a method of family planning. Instead, if asked, these doctors were to say that the program did "not consider abortion an appropriate method of family planning and therefore [did] not counsel or refer for abortion."[120]

Now the genius of this method of regulation is that it effectively hides the government's hand. As Laurence Tribe argued before the Supreme Court,[121] it permits the government to transmit its message without tying the message to the government. Many women are likely to conclude that it is their doctor who is steering them away from abortion — since it is the doctor who is saying or not saying something about abortion. The government achieves its objective by undermining transparency. The success of the program turns upon defeating transparency.

Cyberspace presents the opportunity for *Rust* writ large. For it is a feature of people's experience of cyberspace that they are unlikely to associate any particular constraint with a choice made by a coder. When one enters a chat room on AOL that allows only twenty-three people in the chat room, one is likely to believe that this constraint is in some sense compelled by the nature of the space. But of course, twenty-three is arbitrary; it could as well have been 230. The difference is a choice, and the reasons for the choice are not given.

This creates an extraordinary opportunity for government. For to the extent the government can hide its choices in the code of the space, it can, like the Reagan Administration in *Rust*, avoid the political consequences of its choices. To the extent it can use architecture to effect its choices, it can achieve its goals more quickly and easily than by pursuing them openly.

My claim is not that this opportunity is new, nor that every regulation through architecture is non-transparent. When Robert Moses built bridges to Long Island that blocked buses, and thereby kept bus riders —

---

119 410 U.S. 113 (1973).

120 *Rust*, 500 U.S. at 180 (quoting 42 C.F.R. § 59.8(b)(5) (1989)).

121 *See* Transcript of Oral Argument, *Rust*, 500 U.S. 173 (Nos. 89-1391, 89-1392), *available in* 1990 WL 601355, at *3–*27 (Oct. 30, 1990).

and thus the less wealthy — off public beaches,[122] that was a regulation through architecture, and that regulation hid its motives well. But when the state builds a speed bump on an air-terminal access ramp, that is also regulation through architecture. That regulation in no way hides its policy — no one believes that nature or coincidence has placed the speed bump in the middle of the road.

The difference between cyberspace and real space is again one of degree. The opportunities for non-transparent regulation are multiplied in cyberspace, and the fundamental, or constitutional, question is whether we should be concerned. Should our belief in the value of transparency steer us away from regulations through code that hide their policy? Should we demand that the state announce its purpose, or make plain its hand?

Cyberspace raises the question of transparency in a new context. When the government regulates indirectly, through the regulation of cyberspace's code, should it be required to make the regulation transparent?[123] My strong sense, consistent with our tradition, is that the answer should be yes.[124] But it is also my strong view that nothing in our present array of constitutional principles would actually require government to do so. If the constitution is to catch up to the problems of cyberspace, it must be able to address these questions.

C. Questions About Code's Regulation of Law

Law, I have argued, is vulnerable to the competing sovereignty of code. Code writers can write code that displaces the values that law has embraced. And if the values of law are to survive, law might well have to respond.

My examples in Part II describe two particular cases in which the values of a legal regime are being displaced. But we can describe this displacement more generally. Generally, the values that the present architecture enables are values of bottom-up control — except, as I noted, in the case of privacy. They enable control from bottom-up structures, such as contract-like or property-like systems. They interfere with the top-down imposition of rules that users would not choose for themselves.

---

122 *See* ROBERT A. CARO, THE POWER BROKER: ROBERT MOSES AND THE FALL OF NEW YORK 318 (1974).

123 For a powerful attack on the failure of the government to maintain transparency in its regulation, see A. Michael Froomkin, *It Came from Planet Clipper: The Battle Over Cryptographic Key "Escrow"*, 1996 U. CHI. LEGAL F. 15.

124 How affirmatively the government must do so is a harder question. We can at least be clear about what it should not do. For example, in a recent proposal to relax encryption controls, the administration was still clear about the desire to maintain the secrecy of investigative techniques used to track behavior online. *See* Transcript of White House Press Briefing (Sept. 16, 1999) <http://www.epic.org/crypto/legislation/cesa/briefing.html>. While some techniques will no doubt properly be confidential, the extent and nature of the government's control over the architecture of encryption should not be.

This does not mean that government can't regulate, for as I have described, government can use indirect techniques to create incentives that will affect bottom-up behavior. But it does highlight a weakness in the potential for Internet self-regulation.

There is a political economy for the Net's self-regulation, just as there is a political economy for regulation generally. As with any political economy, some interests gain more individually from a particular architecture than do others. These interests fund a given evolution of the Net's bottom-up design, and can be expected to prevail in that evolution even if the net gain from their design is less than the net gain from another design.

This obvious point suggests a second. Users need a way to act collectively in the relatively small number of cases where bottom-up regulation leaves some important legal value unprotected, or where the evolution of this bottom-up design threatens some important legal value. As it is now, this collective regulation is resisted by many on the Net.[125] But we should resist simpleton distinctions — the choice has never been between anarchy and totalitarianism, or between freedom and control. Some regulations can enhance individual choice, even if others constrain choice to some collective end.

There are two obvious illustrations of this point. The first, privacy, I have already introduced and will address in more detail now. The second, spam, I describe below.

1. Privacy. — I have described a way in which government could, in effect, subsidize architectures for privacy. It should be clear, rhetoric about self-regulation notwithstanding, that without that subsidy, consumer privacy is unlikely to be protected. There are organizations, of course, that are attempting to establish privacy protection. However, their effectiveness is minimal in comparison to the interests and market power of commerce in cyberspace. As the FTC has described,[126] the efforts of these self-regulating bodies have been wholly ineffective in bringing about a change in protections of the space. And nothing on the horizon suggests that the future of consumer privacy will be different from its past.

For values like privacy, bottom-up regulation is unlikely to change an architecture — here, the architecture of commerce — that so significantly benefits a particular powerful class of users. The challenge is to layer onto this bottom-up design structures and incentives that will enable some col-

---

125 *See, e.g.*, Bill Frezza, *Cyberspace Jurisprudence: Who Shall Punish Evil?*, INTERNETWEEK, Feb. 1, 1999, at 25.

126 *See* PRIVACY ONLINE, *supra* note 12, at 41 ("Effective self-regulation remains desirable because it allows firms to respond quickly to technological changes and employ new technologies to protect consumer privacy. . . . To date, however, the Commission has not seen an effective self-regulatory system emerge."). However, in July 1999, the FTC sent a new report to Congress, concluding that "self-regulatory initiatives described [by the report] reflect industry leaders' substantial effort and commitment to fair information practices." FEDERAL TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 12 (1999).

lective choice other than the unorganized cumulative effect of individually expressed preferences.

2. Spam. — Spam[127] is the sending of unsolicited commercial e-mail, usually in bulk, to lists of e-mail accounts across the Internet. These lists are extremely cheap — $500 for 500,000 names from one source;[128] because the price is so low, one could send 10,000,000 e-mails using such a list and reap a profit even if the return per recipient were very small.

The profitability of spam is a function of the design of e-mail. The initial architecture for e-mail did little to authenticate users of e-mail relays. SMTP (Simple Mail Transport Protocol), for example, which is still the dominant mail protocol, allows third-party relays of mail without an account on the primary mail system.[129] With SMTP systems configured to accept third-party relay, I can direct my mail to be sent through these systems even though I don't have an account on these systems. Thus spammers can use third-party relay systems to flood the Net with e-mail.[130]

Third-party relay is not the only technique spammers use. But it is the subject of an important debate about spam on the Internet. For while many have no use for a third-party relay system, some system administrators want the relay channel left open, and they take other steps to ensure the channel is not abused by spammers.[131]

Others on the Net, viewing third-party relay as the biggest cause of spam, want these channels closed. And some of these others have organized blacklists of open relay systems; subscribers use these blacklists to determine whose mail they will bounce.[132] If your e-mail administrator has left your relay open, then your site is likely to be added to these lists; if

---

127 *See Developments*, *supra* note 10, at 1601–03 (describing the problem of spam, the various legal solutions that have been proposed, and the First Amendment implications of those solutions); *see also* Aliza R. Panitz & Scott Hazen Mueller, *Frequently Asked Questions About Spam* (visited Aug. 14, 1999) <http://spam.abuse.net/faq.html> (answering common questions about spam and rebutting common defenses of spam).

128 *See* David E. Sorkin, *Unsolicited Commercial E-Mail and the Telephone Consumer Protection Act of 1991*, 45 BUFF. L. REV. 1001, 1010 n.47 (1997).

129 *See* ALAN SCHWARTZ & SIMSON GARFINKEL, STOPPING SPAM: STAMPING OUT UNWANTED EMAIL AND NEWS POSTINGS 90–91 (1998); Kenneth Cukier, *ISPs and Corporates Overcome by Spam*, COMMUNICATIONSWEEK INT'L, Jan. 19, 1998, at 26.

130 *See* SCHWARTZ & GARFINKEL, *supra* note 129, at 90 (warning that a server "should not allow unknown computers to [relay mail], lest a spammer take advantage of the server to hide his tracks"); *News Briefs: Spammers Still Find Too Many Open Doors*, NETWORK WORLD, July 12, 1999, at 6 (citing a report that found that approximately 17% of e-mail servers remain open to relay traffic).

131 *See* John Fontana, *Slam the Spam Door*, INTERNETWEEK, Aug. 17, 1998, at 1 (observing that "there are those who have no choice but to leave their relays open" and citing a university e-mail administrator who explains that his solution is "'to monitor the hell out of the logs'").

132 *See* Roger Dennis, *Xtra's E-mail Problems Continue*, Christchurch PRESS, May 9, 1998, at 27. ORBS, the "Open Relay Behavior-modification System," maintains such blacklists. *See What is ORBS?* (visited Aug. 14, 1999) <http://www.orbs.org/whatisthis.cgi>.

your site is added to these lists, then your e-mail to sites administered by subscribers to these lists will, in many cases, simply disappear.

This blacklisting is a kind of vigilantism — it is an example of private people taking the law into their own hands.[133] To call it vigilantism is not to criticize the vigilantes. Vigilantes in a state-less nature may be the only people fighting crime, and I certainly believe that relative to the norms of the Net, spam is crime.

But the virtue notwithstanding, vigilantism has its costs. These blacklists create conflicts that reach far beyond the simple listing of a site. Consider one example of a potentially explosive battle.[134]

In 1998, Jeff Schiller, MIT's network administrator, began receiving e-mail from users of the MIT system, complaining that their mail to others outside the MIT domain had been blocked. The mail was being blocked because a spam vigilante, Open Relay Behavior-modification System (ORBS), had decided that the MIT network had "bad e-mail practices." Without notice, MIT was placed on ORBS's blacklist, and subscribers to ORBS began automatically to exclude MIT mail. One company in particular confirmed its policy of blocking according to the ORBS list — Hewlett Packard (HP). Mail from MIT to HP would not go through, MIT was told, until MIT changed its network policy.

MIT was not to be bullied. Its decision not to block automatically all "third-party relay" e-mail (e-mail that the MIT server sends without authenticating that the sender is associated with MIT) made sense for its network and the MIT community. MIT had measures to limit spam by policing the use of its "third-party relay" facility. But its methods were not the methods of ORBS, which made MIT an ORBS enemy.

Rather than cave to the pressure of ORBS, MIT decided to fight. And as tit begets tat, it decided to fight it out with HP. The plan was to bounce all e-mail from HP, until HP stopped bouncing e-mail from MIT.

Until a god of sorts intervened. In response to complaints from other ISPs, ORBS's network services provider, BC Tel, decided that ORBS's "unauthorized relay testing" was a violation of its own network policy

---

133 Other examples of antispammer vigilantism abound. *See* David G. Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace*, 1996 U. CHI. LEGAL F. 139, 163 n.54 (describing Cancelmoose, "a fictitious being operating pseudonymously in cyberspace that has taken a lead in issuing 'cancelbots' — commands that cancel postings to Usenet newsgroups — in response to reported instances of 'spamming'"); Richard C. Lee, Comment, Cyber Promotions, Inc. v. America Online, Inc., 13 BERKELEY TECH. L.J. 417, 417 n.5 (1998) ("[M]any entities related with junk mails [sic] have received paralyzing system attacks, viruses, and even physical threats."); Joshua A. Marcus, Note, *Commercial Speech on the Internet: Spam and the First Amendment*, 16 CARDOZO ARTS & ENT. L.J. 245, 248 (1998) (telling the story of two lawyers from Scottsdale, Arizona whose immensely wide spamming prompted "hate mail, death threats, and anti-Semitic remarks" (citations omitted)).

134 *See* Lawrence Lessig, *The Spam Wars* (visited Aug. 17, 1999) <http://www.thestandard.net/ articles/display/0,1449,3006,00.html>.

agreement. BC Tel in turn bumped ORBS off the Net, and the mail from MIT again flowed to HP. A spam war was averted.

These blacklists are a kind of bottom-up regulation. Like solutions to the privacy problem, they are an imperfect bottom-up regulation. For they cannot directly deal with the real problem that is affecting the Net — namely, spam. To fight spam, blacklists adopt techniques that are both under- and over-inclusive, and for users drawn into a black hole by these techniques, these blacklists invite real conflict.[135]

A simpler and more direct way of dealing with this problem would be a kind of governmental regulation. Trespass law is a first example;[136] a law requiring the labeling of spam would be a second.[137] Both laws could change the incentives of spammers, raising the cost of spam to a level where the benefits would not exceed the cost.[138]

In this view, spam was "caused" by the effect that code had on the market — facilitating low-cost advertising. The response is a law that increases the costs in the market — thus decreasing the incidence of low-cost advertising. In other words, law here would compensate for the change in code.[139] Consensual communication (not spam) would still be cheap; nonconsensual communication (spam) would still be cheaper than in real space.

3. Values in Relief. — My aim in this section has been to highlight a set of values that we should keep in sight as we work through the conflict between regulations of law and regulations of code. These values should restrain both the effect of law on code, and the effect of code on law. To the extent that the law uses code, but non-transparently, we have reason to question the technique of law. And to the extent that law can achieve its ends through code, we have reasons to require that the code be narrowly tailored to serve only legitimate state ends.

---

135 *See* Kimberly Gentile, *U. Texas-Austin's Junk E-mail Service Nixed, Problems Cited*, U. WIRE, Nov. 20, 1998, *available in* LEXIS, Wire Service Stories (reporting that University of Texas computing officials backed away from ORBS after receiving complaints that legitimate e-mails were blocked, and quoting an official who stated that ORBS is "too strict a measure to implement at this time"); Rob Hall, *Here's the Dumbest Idea to Hit the Net*, OTTAWA SUN, Oct. 2, 1998, at 51 (describing ORBS as "much too drastic a method to take").

136 *See Developments*, *supra* note 10, at 1602 (describing a case in which an ISP's claim of trespass against a spammer was sustained).

137 *See id.* (describing some proposed legislation).

138 For commentary on the regulation of spam, see generally Anne E. Hawley, *Taking Spam out of Your Cyberspace Diet: Common Law Applied to Bulk Unsolicited Advertising via Electronic Mail*, 66 UMKC L. REV. 381 (1997); Sorkin, cited in note 128; Lee, cited in note 133; and Steven Miller, Comment, *Washington's "Spam Killing" Statute: Does It Slaughter Privacy in the Process?*, 74 WASH. L. REV. 453 (1999).

139 *See* Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1201 (1998) (observing that "changes [in government regulations] are to be expected when the speed of communication dramatically increases and the cost of communication dramatically decreases").

Likewise the other way around. When a structure of code affects values implicit in the law, there is good reason to ensure that these values don't become displaced. In the general class of cases where bottom-up aggregation of preferences won't produce the ideal mix of regulation, we should check the aggregation made through the bottom-up design of code.

CONCLUSION

At the center of any lesson about cyberspace is an understanding of the role of law. We must make a choice about life in cyberspace — about whether the values embedded there will be the values we want.[140] The code of cyberspace constitutes those values; it can be made to constitute values that resonate with our tradition, just as it can be made to reflect values inconsistent with our tradition.

As the Net grows, as its regulatory power increases, as its power as a source of values becomes established, the values of real-space sovereigns will at first lose out. In many cases, no doubt, that is a very good thing. But there is no reason to believe that it will be a good thing generally or indefinitely. There is nothing to guarantee that the regime of values constituted by code will be a liberal regime; and little reason to expect that an invisible hand of code writers will push it in that direction. Indeed, to the extent that code writers respond to the wishes of commerce, a power to control may well be the tilt that this code begins to take.[141] Understanding this tilt will be a continuing project of the "law of cyberspace."

Nevertheless, Judge Easterbrook argued that there was no reason to teach the "law of cyberspace," any more than there was reason to teach the "law of the horse," because neither, he suggested, would "illuminate the entire law."[142] This essay has been a respectful disagreement. The threats to values implicit in the law — threats raised by changes in the architecture of code — are just particular examples of a more general point: that more than law alone enables legal values, and law alone cannot guarantee them. If our objective is a world constituted by these values, then it is as much these other regulators — code, but also norms and the market — that must be addressed. Cyberspace makes plain not just how this interaction takes place, but also the urgency of understanding how to affect it.

---

140 *See* Robert Fano, *On the Social Role of Computer Communications*, 60 Proc. IEEE 1249, 1253 (1972).

141 This is the core argument in LESSIG, *supra* note 2.

142 Easterbrook, *supra* note 1, at 207.