# The Law of the Horse: What Cyberlaw Might Teach

Lawrence Lessig*

forthcoming, HARVARD LAW REVIEW (fall, 1999)

*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 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, as well as the Stanford and Chicago Legal Theory Workshops. Research assistance, much of it extraordinary, was provided by Karen King, and on an earlier draft, by Timothy Wu.

A few years ago, at a conference on the "Law of Cyberspace" held at the University of Chicago, in a room packed with "cyberlaw" devotees (and worse), Judge Frank Easterbrook told the assembled listeners 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 would just muddle rather than clarify. And that legal academics ("dilettantes") should 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 Easterbrook's welcome.

As is often the case when my then-colleague speaks, the intervention produced an awkward silence, some polite applause, and then quick passage to the next speaker. It was an interesting thought — the 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 didn't seem a helpful thought, two hours into this day-long conference. So unhelpful, it was put away. Talk quickly 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 that the law of cyberspace was something more.

Some of us, however, could not so easily leave the question behind. I am one. I confess that I've spent too much time thinking just what it is that a law of cyberspace could teach. This essay is an introduction.[2] My aim is to show that there is something general about how we might think of regulation — regulation, that is, both there, and here — that cyberspace will teach, and that we see this general feature only by working through some specifics. Or

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

[2] For the complete account, or as complete as it gets, see LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (forthcoming, Basic Books 1999).

put differently, when we come to understand regulation there, we will have come to see something special about regulation here."[3]

My essay moves in five parts. I begin with two problems of regulation that cyberspace might present, as a way to illustrate the issues at stake. I then use these examples to articulate a model of regulation that will apply both to regulation in cyberspace as well as in real space. That's part I and part II. In part III, I consider two examples of how law might regulate cyberspace. My aim is to show the possibility; it is not to argue for any particular regulation. Part IV makes the same point in reverse: I offer two examples of how cyberspace might (in effect) regulate law. These two perspectives suggest a more systematic competition, which I describe in section V. Section VI then draws two lessons from this competition — lessons, I argue, that reach beyond the domain of cyberspace.

I conclude with an answer to Easterbrook's challenge. If my argument sticks, then these two lessons are questions about regulation that should trouble us as much about real space regulation as they trouble us about law in cyberspace. They should, that is, in the words of Judge Easterbrook, "illuminate the entire law"[4] even if drawn from just one domain.

## I. PARADIGM CASES

Consider two cases that will set a paradigm for the problems of regulation that cyberspace presents. They both involve differences in "information" — the first too little, the second too much — but it is not information that makes these problems distinct. Instead, their salience turns on the source of the feature that will make them (for us) distinctive. That source is *code* — the software and hardware that makes this part of cyberspace as it is. As I argue more fully below, the paradigm regulatory question in cyberspace is how to accommodate this difference in code.

### *Zoned Speech*

[3] On 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 (1996).

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

Porn in real space is zoned from kids. Whether by laws (banning the sale of porn to minors), or by norms (shunning those who do), or by the market (porn costs money), it is hard in real space for kids to buy porn because in real space, porn has been *placed* for adults. In the main, not everywhere; hard, not impossible. But on balance, the regulations of real space have an effect which is to keep kids from porn.

These real space regulations hang upon a feature of real space. They depend upon a feature of its design. It is hard in real space to hide that you are a kid. Being a kid in real space is a self-authenticating fact. Sure — a kid may disguise that he is a kid; he might don a mustache or walk on stilts. But costumes are expensive, and not terribly effective. And it is hard to walk on stilts. Thus the kid transmits that he is kid, and so the seller of porn knows he is a kid,[5] and so the seller of porn, either because of laws or norms, knows not to sell. Self-authentication makes zoning in real space easy.

Age is not similarly self-authenticating in cyberspace. Even if the same laws and norms applied in cyberspace, and even if (as they are not) the constraints of the market were the same, any effort to zone porn in cyberspace faces a very difficult problem. In cyberspace, being a kid is not self-authenticating. The fact that one is not a kid is extremely hard to certify. To a web site accepting traffic, all requests are equal. There is no automatic way 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 regulation in the space costly — so costly, the Supreme Court held in *Reno v. ACLU*, that the constitution prohibits it.[6]

### *Protected Privacy*

If you walked into a store, and the guard at the store recorded your name, and if cameras tracked your every step, noting what items you looked at, and what items you ignored; if an employee

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

[6] *See* Reno v. American Civil Liberties Union, 521 U.S. 844, 117 S.Ct. 2329 (1997); Lawrence Lessig, *What Things Regulate Speech: CDA 2.0 vs. Filtering*, 38 JURIMETRICS J. 629 (1998).

followed you around, timing your attention span in any given isle; 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 would make a choice about whether you wanted to shop in such a store. Perhaps the vain would enjoy the attention; perhaps the prices would be significantly lower. Whatever the reason, whatever the consequent choice, you would know enough in real space to know to make a choice.

In cyberspace, you wouldn't. You wouldn't notice this monitoring because this tracking is not similarly visible. As Jerry Kang aptly describes,[7] when you enter a store in cyberspace, it can record who you are; click monitors will track where you browse, how long you watch a particular page; in effect, an employee (if only a bot on a computer) can follow you around, and when you purchase, it can record who you are and from where you came. All this is done in cyberspace, invisibly. Data is collected but without the individual knowing. Thus the individual cannot (at least as easily) make a choice about whether to participate or consent to this surveillance. In cyberspace, surveillance is not self-authenticating. Nothing reveals whether you are being watched,[8] so that there is no real basis upon which to consent to this monitoring.

***

These examples fit a pattern: A feature of the environment of cyberspace that differs from an analogous feature in real space; the question for law is how to respond. Should the law change in response to that different feature? Or should the law try to change that feature, to make it 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 constrain the law's mucking about with this space?

Or again, how should law *regulate*? To many, this question will seem very odd. For many believe that cyberspace simply cannot be regulated. Behavior in cyberspace, this meme suggests, is simply

[7] *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1198-99 (1998).

[8] *See* Privacy Online: A Report to Congress. Federal Trade Commission, June 1998 at <http://www.ftc.gov/reports/privacy3/index.htm>.

beyond government's reach. The anonymity, and multi-jurisdictionality of the space makes control by governments impossible. The nature of the space makes behavior in the space *unregulable.*[9]

This view about cyberspace is wrong — though wrong in an interesting way. It either assumes that the nature of cyberspace is fixed — that its architectures, and the control they enable, can't be changed — or it assumes that government can't take steps to change this architecture.

Neither assumption is correct. Cyberspace has no nature; it has no particular architecture that could not be changed. Its architecture is a function of its design — or as I will describe it in the section that follows, its code.[10] This code could well change, either

[9] *See, e.g.*, *Of* Governance and Technology, INTER@CTIVE WEEK ONLINE (Tom Steinert-Threlkeld ed. 1998); 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 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. (1995).

[10] As I define the term, *code* refers to the software and hardware that constitutes cyberspace as it is — or more directly, the rules and instructions that are imbedded 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" differs dramatically. Some of this code is within the Internet Protocol layer, where protocols for exchanging data on the internet (including TCP/IP) are implemented. Some of this code is above this IP layer, or in 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, and David D. Clark, *End-to-End Arguments in System Design*, in INNOVATIONS IN INTERNETWORKING 195 (Craig Partridge, ed. 1988). More generally, this layer would include any applications that might interact with the network (browsers, email 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. This is because the most sophisticated regulations will occur at this level, given the net's adoption of Saltzer's end-to-end design.

because it evolves in a different way, or because governments push it to evolve in a particular way. It may well be that particular versions of cyberspace can't be regulated. But it does not follow that every version of cyberspace can't be regulated.

My claim is that government can take steps that would increase the regulability of the space. But to see just how, we should think more broadly about this question of regulation. That is the aim of the section that follows.

## II. REGULATING BEHAVIOR

### *Modalities of Regulation*

Behavior, we might say, is regulated by four kinds of constraints.[11] Law is just one of those constraints. Law (in the naive positivist's view) orders people to behave in certain ways.[12] Law tells me not to deduct more than 50% of business meals from my income taxes; it tells me not to drive faster than 55 mph on a highway. It tells me not to buy drugs; not to sell unlicensed cigarettes; not to trade across international borders without first filing a customs form. Law directs in these different ways, by threatening a punishment. In this way, we say, law regulates.

But not only law regulates. Social norms, in this sense, regulate as well. They are a second sort of constraint. Norms say that I can buy a newspaper, but cannot buy a friend. They frown on the racist's jokes; they are unsure about whether a man should hold a door for a woman. Norms too, like law, regulate by threatening punishment ex post. But unlike law, the punishment of norms is not centralized. It is enforced (if at all) by a community, not a government. In this way, norms constrain. In this way, they too regulate.

Finally, when I say that cyberspace "has no nature," I mean that there are any number of possible designs or architectures that might effect the functionality we now see associated with cyberspace. I do not mean that, given its present architecture, there are not features that constitute its nature.

[11] This analysis is drawn from Lawrence Lessig, *The New Chicago School*, 27 J. LEGAL STUD. 661 (1998).

[12] 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.

The same is for markets: Markets, too, regulate. They regulate by price. The market constrains my ability to trade hours of teaching for potatoes; or my kid's glasses of lemonade for tickets to the movies. Of course, the market only constrains so because of other constraints of law, and social norms — markets are constituted by property and contract law; they operate within the domain allowed by social norms. But given these norms, and given this law, the market presents another set of constraints on individual and collective behavior. Or alternatively, it establishes another band of regulation on individual and collective behavior.

And finally, there is a fourth feature that regulates behavior in real space — something we might call "architecture." By "architecture" I mean the physical world as we find it, even if *as we find it* is a way that *has been made*. That I can't see through walls is a constraint on my ability to snoop. That I can't read your mind is a constraint on my ability to know whether you are telling me the truth. That I can't lift large objects is a constraint on my ability to steal. That there is a highway and train tracks separating this neighborhood from that is a constraint on citizens to integrate. These constraints bind in a way that regulates behavior. In this way, they too regulate.

We can represent these four constraints together in a simple diagram. (*fig.* 1) Each ellipse represents one modality of constraint; the circle in the middle represents the entity being regulated; the arrows represent the direct regulatory effect of each modality of regulation. The "net regulation" for any given policy is the sum of the four effects.

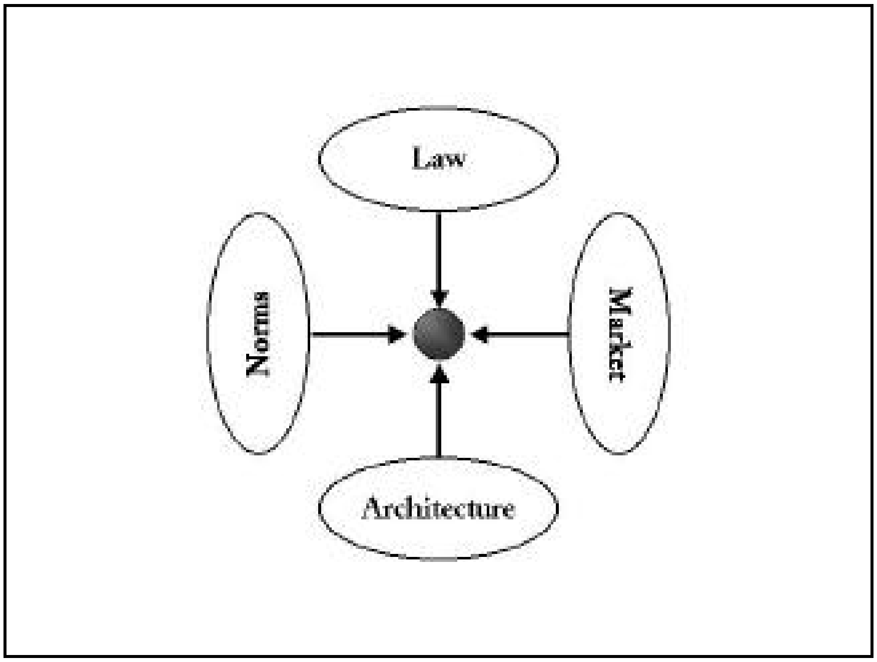

*Figure 1*

Figure 1 describes regulation in real space. The same model, we might say, can also describe the regulation of behavior in cyberspace.

• Law regulates behavior in cyberspace — copyright law, defamation law, and obscenity laws all continue to threaten ex post sanction for the violation of some legal right. How well, or how efficiently, is a separate question — in some cases more efficiently, in some cases not. But whether better or not, law continues to threaten an expected return. Legislatures enact;[13] prosecutors threaten;[14] courts convict.[15]

[13] The ACLU lists 12 states that passed internet regulations in 1995 through 1997. *See* <http://www.aclu.org/issues/cyber/censor/stbills.html#bills>.

[14] *See, e.g.*, the policy of Minn. A.G., http://www.state.mn.us/ebranch/ag/memo.txt.

[15] *See, e.g.*, Playboy Enterprises v. Chuckleberry, 939 F.Supp 1032 (S.D.N.Y. 1996); United States v. Thomas, 74 F3d 701 (6th Cir. 1996); United States v. Miller, 1999 WL 49398 (11th Cir. 1999); United States v. Lorge, 1999 WL 41076 (2nd Cir. 1999); United States v. Whiting, 1999 WL 16388 (8th Cir. 1999); United States v. Hibbler, 159 F.3d. 233 (6th Cir.

• Norms also regulate behavior in cyberspace: Talk about democratic politics in the alt.knitting newsgroup, and you open yourself to flaming; "spoof" someone's identity in a MUD, and you might find yourself "toaded";[16] talk too much in a discussion list, and you're likely to be placed on a common bozo filter. In each case, there is a set of understandings that constrain behavior in this space, again through the threat of ex post (though decentralized) sanctions.

• Markets regulate behavior in cyberspace. Pricing structures constrain access, and if they don't, busy signals do. (AOL learned this quite dramatically when it shifted from an hourly to flat rate pricing plan.[17]) Areas of the web are beginning to charge for access, as online services have for some time. Advertisers reward popular sites; on-line services drop low population forums. These behaviors are all a function of market constraints, and market opportunity. They are all, that is, regulations of the market.

• And finally *code* regulates behavior in cyberspace. The code, or the software and hardware that makes cyberspace as it is, constitutes a set of constraints on how one can behave. The substance of these constraints may vary, but they are all experienced as conditions on one's access to cyberspace. In some places, one must enter a password before one gains access;[18] in other places, one can enter whether identified or not.[19] In some places, the transactions that

1998); United States v. Fellows, 157 F.3d 1197 (9th Cir. 1998); United States v. Simpson, 152 F.3d 1241 (10th Cir. 1998); United States v. Hall, 142 F.3d 988 (7th Cir. 1998); United States v. Hockings, 129 F.3d 1069 (9th Cir. 1997); United States v. Lacy, 119 F.3d 742 (9th Cir. 1997); United States v. Smith, 47 M.J. 588 (Crim. App, 1997); United States v. Ownby, 926 F.Supp. 558 (W.D.Va 1996).

[16] *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*, 1994 ANN. SURV. AM. L. 471 (1994).

[17] *See, e.g., AOL Still Suffering But Stock Price Rises*, NETWORK WK., Jan. 31, 1997; David S. Hilzenrath, *'Free' Enterprise, Online Style; AOL, CompuServe and Prodigy Settle FTC*, WASH. POST, May 2, 1997 at G01; *America Online Plans Better Information About Price Changes*, WALL ST. J., May 29, 1998 at B2.

[18] For example, online services such as America Online.

[19] USENET postings can be anonymous. *See* <http://www.cis.ohio-state.edu/hypertext/faq/usenet /faq/part1/haq.html>.

one engages in produce traces that link the transactions (the mouse droppings) back to the individual;[20] in other places, this link is achieved only if the individual wants.[21] In some places, one can select to speak a language that only the recipient can hear (through encryption);[22] in other places, encryption is not an option.[23] The code or software or architecture or protocols set these features; they are features selected by code writers; they constrain some behavior by making other behavior possible, or impossible. They imbed certain values, or they make certain values impossible. In this sense, they too are regulations, just as the architectures of real space code are regulations.[24]

These four constraints — both in real space and in cyberspace — operate together. For any particular issue, they may complement each other, or they may compete.[25] Thus, to understand how a regulation might succeed, we gain something by viewing these four modalities on the same field. We see something about the possibilities for regulation by understanding how the four interact.

[20] Web browser's make this information available, both in real time, and archived in a cookie file. *See* http://www.cookiecentral.com/faq.htm.

[21] Web browsers also permit users to turn this tracking feature off.

[22] PGP is a program offered both commercially and free to encrypt messages. *See* http://www.cam.ac.uk.pgp.net/pgnet/pgp-faq/.

[23] Encryption, for example, is illegal in some international contexts. *See* the comments of Ambassador David Aaron at http://www.bxa.doc.gov/aaron.htm; STEWART A. BAKER & PAUL R. HURST, THE LIMITS OF TRUST 130 (1998).

[24] This idea of the law in code is beginning to be the focus of a number of scholars' work. *See, e.g.*, Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 EMORY L.J. 911 (1996); David Johnson & David Post, *Law and Borders-The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); M. Ethan Katsh, *Software Worlds and the First Amendment: Virtual Doorkeepers in Cyberspace*, 1996 U. CHI. L. FORUM 335 (1996); Andrew L. Shapiro, *The Disappearance of Cyberspace and the Rise of Code*, 8 SETON HALL CONST. L.J. 703 (1998).

[25] Though 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 simultaneous constraint — one doesn't walk through a brick wall only to be punished later on.

The two puzzles from part I are a simple example of this point:

*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. The architecture of real space makes age (relatively) self-authenticating. Where age is not self-authenticating, other architectures (in the odd sense I mean here) as well as real space norms makes it possible at a relatively low cost to verify one's age.

But in cyberspace, this ability is not so easily available. In cyberspace, the basic internet architecture doesn't enable the self-authentication of age. The basic architecture permits the attributes of users to remain invisible. So norms, or laws, that turn upon a consumer's age in cyberspace are relatively more difficult to enforce.

*Privacy:* A similar story accounts for the "problem" of privacy. Real space architecture makes plain much of the surveillance of others.[26] Ordinarily, one can notice if another is following you, or one is aware if data from an identity card is being collected. Knowing this enables one to decline giving information if one doesn't want that information known. Thus, real space architecture enables only consensual collection of data about one's commercial behavior.

But the architecture of cyberspace doesn't similarly enable this choice. One wanders through the spaces of cyberspace, unaware of the technologies that gather and track one's behavior. One can't assume that everywhere one goes such information is collected. Collection practices differ, depending on the site and its objectives. To choose, one must know, but the architecture disables (relative to real space) one's ability to know when one is 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* of the space — turns on differences in these modalities of constraint. Thus, a first step to understanding why a given behavior in cyberspace might be different,

[26] 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 technologies for monitoring behavior, including many that would be as invisible as the technologies that I argue define the web.

we should understand these differences in the modalities of constraint.

### *How Modalities Interact*

Though I have described them separately, modalities don't operate independently. Instead, in obvious ways, these modalities interact. Norms will affect what objects get traded in the market (we used to have a norm against selling blood; in many places that norm has changed[27]); the market will affect the plasticity of architecture (cheaper building materials, more plasticity in design); architectures will affect what norms are likely (common rooms will affect norms of privacy[28]); and all three will influence what laws are possible.

Thus, complete description of the interaction of these four modalities would trace the influences of the four upon each other. Some of these influences would be direct — norms making a particular market possible, for example. Some would be indirect — an architecture that facilitated a norm that made a given market possible. But whether direct or indirect, the four depend upon each other. Each influences the other, but in a complex that belies any simple description.

There are two dependencies in particular, however, that I will isolate in the account that follows. One is the effect that law might have on the other three modalities of regulation; the other is the effect that architecture might have on the other three modalities of regulation.

I isolate these two for two very different reasons. I focus on law, because law is the most obvious *self-conscious* agent of change. I focus on architecture, because in cyberspace at least, architecture is the most significantly different modality of regulation. It will be law that we first think about when we think about changing behavior in cyberspace. (We can't help it; we are lawyers.) It will be architecture, or code, that we will first notice as being most significantly different.

[27] *See, e.g.*, Karen Wright, *The Body Bazaar; the Market in Human Organs is Growing*, DISCOVER, No. 10, Vol. 19, October 1998, at 114 (describing recent history).

[28] *See, e.g.*, BARRINGTON MOORE, JR., PRIVACY: STUDIES IN SOCIAL AND CULTURAL HISTORY (1984).

With both modalities, there are two distinct effects that we could track. One is the direct effect of each modality on the individual being regulated. (Law acts directly by threatening a consequence if a certain behavior is not engaged. Code acts directly by giving the individual an experience which but for the code she could not have.) The second is the indirect effect of each modality *upon other modalities of regulation*. By acting upon another modality, either law or code can change that modality; and by changing that modality, law or code can indirectly change behavior.[29] In these cases, law or code *uses* these other structures of constraint; they co-opt these other structures of constraint, to bring them in line with the objectives of the law.

Any number of examples would make the point. But one about law will suffice.

*Smoking*: Say the government's objective is to reduce the consumption of cigarettes. There are a number of ways that the government could select to this single end. A law could, for example, ban smoking.[30] (That would be law regulating the behavior it wants to change directly.) Or the law could tax cigarettes.[31] (That would be the law regulating the market for the supply of cigarettes, to decrease the consumption of cigarettes.) Or the law could fund a public ad campaign against smoking.[32] (That would be the law

[29] My point in this drawing is not to represent all the forces that might influence each constraint. No doubt changes in code influence law as well as law influencing code; and the same 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 the intentional intervention by government.

[30] *See, e.g.*, ALA.CODE § 18.35.305; ARIZ.REV.STAT. ANN. § 36-601.01; COLO.REV.STAT. § 25-14-103 (public health laws banning smoking in certain public places).

[31] *See, e.g.*, 26 U.S.C.A. § 5701 (1998); 26 U.S.C.A. § 5731 (1998).

[32] *See, e.g.*, Pamela Ferdinand, *Mass. Gets Tough with Adult Smokers in Graphic TV Ads*, WASH. POST, Oct. 14, 1998 at A3 (describing the series of six 30 second documentary-style anti-smoking ads on Pam Laffin's struggle to survive while slowly suffocating from emphysema, sponsored by the state Department of Public Health); *Feds Pick Up Arnold Spots*, ADWEEK, Nov. 23, 1998 at 8(1) (Seven youth-oriented anti-smoking commercials created for MA Department of Public Health were chosen by the U.S. Office of National Drug. Control Policy to air nationwide as public service announcement starting Dec. 15.).

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.[33] (That would be the law regulating the "code" of cigarettes, as a way to reduce their addictiveness, as a way to reduce the consumption of cigarettes.) Each of these actions by the government can be expected to have some effect (call that its benefit) on the consumption of cigarettes; each action has a cost; the question with each means is whether the costs outweigh the benefits.

In this example, the law is functioning in two very different ways. In one way, its operation is direct; in the other, indirect.[34] When it is direct, it tells individuals how they ought to behave. It threatens a punishment if they deviate from that directed behavior. When it is indirect, the law aims at changing the burden of one of these other modalities of constraint. The law can regulate each individually, or it can regulate all three simultaneously. It selects among these various techniques in pursuing the end it wants to achieve. Which it selects depends upon the return from each, and the values implicit in the selection of one over another.

We can represent the point through a modification of Figure 1:

[33] In August 1996, the Food and Drug Administration ("FDA") published in the Federal Register "Regulations Restricting the Sale and Distribution of Cigarettes and Smokeless Tobacco to Protect Children and Adolescents." 61 Fed. Reg. 44,396 (1996). In Brown & Williamson Tobacco Corp. v. FDA, 153 F.3d 155 (4th Cir., 1998), the court found that the FDA lacked jurisdiction to regulate tobacco products as customarily marketed, because such regulation was inconsistent with both terms of Federal Food, Drug, and Cosmetic Act and intent of Congress. Federal Food, Drug, and Cosmetic Act, §§ 201 (g)(1)(C), (h)(3), 520(e), as amended, 21 U.S.C.A. §§ 321 (g)(1)(C), (h)(3), 360j(e).

[34] The distinction between "direct" and "indirect" has a troubled history in philosophy, *see* Judith J. Thomson, *The Trolley Problem*, 94 YALE L.J. 1395, 1395-96 (1985), as well as law, *see* National Labor Relations Board v. Jones & Laughlin Steel Corporation, 301 U.S. 1, 57 S. Ct. 615 (1937). Its troubles are similar to troubles with the Double Effect Doctrine, discussed in PHILLIPA FOOT, THE PROBLEM OF ABORTION AND THE DOCTRINE OF DOUBLE EFFECT, IN VIRTUES AND VICES 19-32 (1978). *See also* W. Quinn, *Actions, Intentions and Consequences: The Doctrine of Double Effect*, 18 PHIL. & PUB. AFF. 334-351 (1989); Thomas J. Bole III, *The Doctrine of Double Effect: Its Philosophical Viability*, 7 SW. PHIL. REV. 1, 91-103 (1991). But the difficulty in these cases comes when a line between direct and indirect must be drawn; there is no need here to draw such a line.

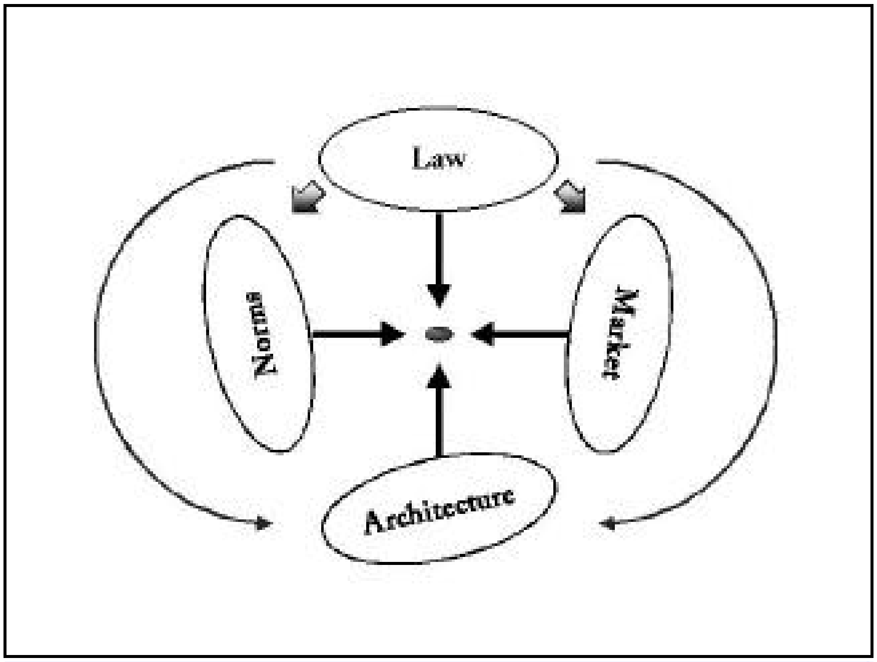

*Figure 2*

This is the picture of modern regulation. Regulation here is always a choice — a choice between the direct regulations that these four modalities might effect, and the indirect regulations that they also might effect. The point is not binary; it is not that law picks one strategy over another. Instead, there is always a mix between direct and indirect. The question the regulator must ask is, *Which mix is optimal*?

The answer depends 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 10th century Europe, mucking about with architectural constraints might have been a bit hard, but in the modern modular office building, architecture becomes quite an effective technique (think about transparent cubicles as a way to police behavior). The optimal mix in any context depends upon the plasticity of the different modalities. This plasticity obviously differs. What works in one context won't necessarily work everywhere.

But while context matters, we may well be able to generalize. While in principle, any modality might work, in fact, depending upon the context, some modalities might 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 — either direct regulation of the code of cyberspace itself, or of the institutions (code writers) that produce that code, so that code regulates individuals differently.

My aim in the next two sections is to explore this dynamic more fully. My hope is 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 make more urgent a question that constitutional law has yet to answer well: What limits should there be on indirect regulation? How far should the law be permitted to co-opt these other structures of constraint?

## III. LAW REGULATING CYBERSPACE

Whether cyberspace can be regulated depends upon its architecture.[35] 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. The difference is a difference in design, and its design is not given to us by nature.

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 its regulability. I offer two examples which together should suggest the more general point.

### *Increasing 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 made it possible for rules about access to be enforced, while in cyberspace, because being a kid is not self-authenticating, the same regulations were not easy.

[35] By "design" or architecture, I mean both the technical design of the net, and its social, or economic design. As I will describe more fully in note 65 below, a crucial feature of the design 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.

One response would be to make identity self-authenticating by making it such that, when one connects to a site on the net, features about oneself get transmitted to the site, so that the site can make a determination about whether, given the status of the individual, admitting the individual is permitted.

In a sense, this already occurs. The net already facilitates some identification. A server for example can tell whether my browser is a Microsoft or Netscape browser; some can tell whether my machine is a Macintosh or Windows machine. These are examples of self-authentication that are built within the code of the net.

Another example is a user's "address." Every user of the net has, for the time they are using the net, an address.[36] This IP address is unique; only one machine at any one time may have the same 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. While some machines have "static" IP addresses which 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, while something is revealed when a machine is on the net, the *inter*net as it is just now does not require any authentication beyond the supply of an IP address.

*Intra*nets are different.[37] Intranets are networks that connect to the internet; they are networks that are compliant with the ba-

[36] "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 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." http://www.whatis.com/ipaddress.htm.

[37] 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. Intranets mix values from each to produce a network that is interoperable, but that gives its controller a great deal of control. An "internet" with control is what our internet is becoming. *See, e.g.,* Steve

sic internet protocols. But they layer onto these protocols other protocols as well. And among these are protocols that enable the identification of who someone is by the controller of the intranet. They enable, that is, a form of self-authentication that facilitates identification. The depth of this identification varies. At one extreme are biometric techniques to identify a particular user; at the other extreme, certificates to identify features of the person. The one extreme guarantees that the system knows who someone is; the other extreme guarantees that the system knows that a person holds certain attributes.

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 for me to show how identification is possible, and to show that the government can act to enable the use of some of these technologies of identification. For if these technologies of identification existed generally, then my claim is the regulability of cyber-behavior would increase.

So focus on the single issue of zoning kids from adult speech on the net. Congress has now twice tried to enact legislation that would regulate the supply of such speech to "minors."[38] At the time of this writing, it has twice failed.[39] Its failure in both cases comes from a certain clumsiness in execution. In the first case, it tried to regulate too broad a category of speech; in the second, while correcting that problem, it has burdened the wrong class of users — adults.

Lour, *Netscape Taking on Lotus With New Corporate System*, N.Y. TIMES, Oct. 16, 1996 at D5. ("Netscape executives pointed to studies projecting that the intranet market will grow to $10 billion by 2000."); Steve Lour, *Internet Future at IBM Looks Oddly Familiar*, N.Y. TIMES, Sept. 2, 1996, at I5 ("[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.").

[38] *See* Telecommunications Act of 1996, Pub. L. No. 104-104, Title V, 110 Stat. 56, 133-43 (1996) (Communications Decency Act); Child Online Protection Act, Pub. L. No. 105-277, 112 Stat. 2681 (1998) (to be codified at 47 U.S.C. §231).

[39] *See* Reno v. ACLU, 117 S.Ct. 2329 (1997) (striking part of CDA); ACLU v. Reno, 31 F. Supp.2d 473 (E.D. Pa. 1999) (granting plaintiffs' motion for preliminary injunction because of substantial likelihood of success on claim that COPA is presumptively invalid and is subject to strict scrutiny).

Consider a third alternative, that in my view would not raise the same constitutional concerns.[40] Imagine the following statute:

1. *Kids-Mode-Browsing:* Manufacturers of browsers will enable those browsers to browse in "kids-mode." When enabled, "kids-mode" 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 shall not transmit to a site any identifying data about the user.

2. *Server Responsibility:* When a server detects a kids-mode client, it shall (1) block that client from any material properly deemed "harmful to minors" and (2) refrain from collecting any identification data about the user, except data necessary to process user requests. Any such data collected shall be purged from the system within X days.

Both this regulation, and the change in browser code it requires, would be trivial to implement. In a world where 90% of browsers are produced by two companies, the code writers are too prominent to hide. And why hide – given the simplicity of the requirement, the regulation would be easy to comply with. In a very short time, such a statute would produce browsers that enabled kids-mode browsing, at least for those parents that would want such control on machines in their home.

Likewise would it be easy for sites to develop software to block access if the user enters transmitting that he is a kid. Such a system would require no costly identification; no database of IDs would be built, or maintained; no use of the credit card system would be required. Instead, the software would be programmed to accept users who didn't have the kids-mode selected, but reject users that did have the kids-mode selected.

Whether one supports such legislation or not, my point is its feasibility and constitutionality. Netscape and Microsoft would have no first amendment objection to a regulation of its code; and web sites would have no substantial objection to the requirement

[40] While this idea has been out there for sometime, I am grateful to Mark Lemley for pushing me to see it. For a more formal analysis, *see* Lawrence Lessig and Paul Resnick, *The Constitutionality of Mandatory Access Controls* (unpublished 1992).

that it block kids-mode browsers. And no case has ever held that a speaker has a right to have no burden imposed at all to advance a compelling state need; the only requirement of *Reno* is that the burden be the least restrictive burden. This burden, I suggest, would be the least restrictive.

It would also be quite effective. For imagine the FBI now enables a bot[41] to spider the net with a kid-mode browser setting switched on. The bot would then try to gain access to sites on the net; if it got access, then it would report 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 then determine whether these sites were indeed "adult sites"; and if they were, it would proceed against these sites. The result would be a system that could extremely effectively monitor access to adult content on the web.

For the purposes of zoning adult speech, this change would fundamentally alter the regulability of the net. It would do this not by directly regulating kids. It would do this instead by altering one feature of the "architecture" of the net — namely the ability of a browser to identify a feature of its user. Once this facility were built into browsers generally, the ability of suppliers of adult speech to discriminate would change. This regulation of code would make possible the regulation of behavior. Or again, it would increase the regulability of this behavior, by regulating the code.

### *Increasing Regulability: Privacy*

Zoning porn is an example of top-down regulation. The state, perhaps with bottom-up support, imposes a collective judgment about who can get access to what. It imposes that judgment by requiring those who write code to write code that conforms to the state's rules.

The second example in section I was different. The disability there affected bottom-up regulation — regulation, that is, imposed by individuals through individual choice. Architectures can enable or disable individual choice, by providing individuals with the information they need to make a decision, and the option to exercise that decision, or not. The privacy example rested on an architec-

[41] A "bot" is a computer program that acts as an agent for a user, performing a task, usually remotely, in response to a request. *See, e.g.*, http://www.whatis.com/bot.htm.

ture that did not enable individual choice. It hid facts necessary to that choice, and thereby disabled bottom-up self-regulation.

But again, these architectures can be changed. Just as with the zoning of porn, these architectures are open to collective modification. Government can act to facilitate a change in this code, and thereby act to facilitate increased self-regulation.

Here the technique, however, is a traditional tool of law. The problem comes from an architecture that enables the collection of data without the customer's consent.[42] But the problem also comes from a regime of entitlement that does not demand that the collector get the customer's consent. Because the customer has no property interest in personal information, information about them 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 that was 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 them, and thus create an incentive (2) for architectures that facilitate consent before turning that data over.

The first step comes through a declaration by the state about who owns what property.[43] Government would declare that information about individuals is owned by individuals; others can take it, and use it, only with the consent of those individuals. This declaration of rights could then be supplemented in any number of traditional ways. The state might make theft of such information criminal, or provide special civil remedies, and incentives to enforce them, if such information is taken.

[42] *See* Joel R. Reidenberg, Paul M. Schwartz, ON-LINE SERVICES AND DATA PROTECTION AND PRIVACY — REGULATORY RESPONSES, Vol. II, 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.").

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

This first step, however, would be useful only if it induced a second change — this time, a change in the architecture of the space, and not in the laws that govern that space. This change in the architecture would aim at reducing the costs of choice. The objective would be to make it easy for individuals to express their preferences about the use of data about them, and easy for negotiations to occur about that data. Property regimes make little sense where transactions about that property are not permitted — unless, of course, the property is by design not to be alienated. 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 for the control of privacy data.[44] P3P is a design that 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 I, for example, never want to give out my credit card number, then I could use P3P to express that preference, and when I visited a site, an agent would negotiate with the site about my preference, and about access to the site.

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 the regulability by individuals of life in cyberspace would increase.

But without state intervention, it is not clear that such a framework could develop. P3P creates burdens on sites that would collect data; these burdens make no sense in a world where these sites can get the same information for free. Only by changing the incentives of these sites — by denying that they can get this information for free — can one expect to create a sufficient incentive for them to adopt technologies that facilitate purchase. Establishing a property interest in privacy data would be such an incentive; and it is the government that then facilitates that interest.

***

[44] *See* Platform for Privacy Preferences (P3P) Syntax Specification. W3C Working Draft, July 2, 1998 at http://www.w3.org/TR/WD-P3P10-syntax/.

My claim so far is simply a possibility claim. It is that the government's power to regulate this space turns not just on whether it can regulate behavior directly; rather its power turns as well on the ability to regulate *code*. By regulating code, it can regulate behavior, by changing the incentives that the code would otherwise produce. Law can act directly on code writers (as the zoning example suggests) or indirectly on code writers (as the privacy example suggests) so as to effect changes in the behavior of people within the net.

## IV. CODE REGULATING 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 here is *in effect*, for these are not examples where the code achieves a change in the law. The law on the books remains constant. These instead are examples of the code shifting the effectiveness of a given law. They are indirect effects of the code that might alter the regulation or policy of the law.

Where architectures displace the values of the law, lawmakers will face a choice, whether to reinforce the law, or allow the change. In the examples I select here, my bias is in favor of the law, though of course there are many examples where my bias would be elsewhere. My point is not that law should always respond; it is only to show why it might need to respond.

### *Code replacing Law: Intellectual Property*

We have special laws to protect against the theft of autos, or planes.[45] We don't have special laws to protect against the theft of skyscrapers. Skyscrapers take care of themselves. The architecture of real space, or more suggestively, their 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 planes (making them quite easy to move).

On this spectrum from cars to very big buildings, intellectual property (IP) is on the side of cars, and quite unlike large buildings.

[45] The Model Penal Code (§223.1(2)(a)) constitutes the theft of an automobile, airplane, motorcycle, motor boat or "other motor-propelled vehicle" a felony.

Indeed, as the world is just now, IP fares far worse than cars and planes. 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 don't necessarily know. Sales might go down, my fame might go up, 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."[46] Property could not be controlled on the net; copyright made no sense. Authors would have to find new ways to make money in cyberspace, because the technology has destroyed the ability to make money by controlling copies.

The reasons were plain: The net is a digital medium. Digital copies can be perfect and free. One can scan a copyrighted photo into a digital file, and then post it on USENET to millions of people for free. The nature of the net, we were told, would make copyright controls impossible. Copyright was dead. Long live copyright.

There was something odd about this argument, even at the start. It betrayed a certain is-ism ("the way cyberspace is is the way it has to be") about cyberspace. Cyberspace was a place where "infinite copies could be made for free." But why exactly? Infinite copies could be made because the code permits such copying. So why couldn't the code be changed? What reason was there that we couldn't imagine a different code that better protected intellectual property?

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

Consider the proposals of Mark Stefik of Xerox PARC. In a series of articles,[47] Stefik describes what he calls "Trusted Systems"

[46] John Perry Barlow, *The Economy of Ideas*, WIRED, Mar. 1994, at 85.

[47] *See* Mark Stefik, *Trusted Systems*, SCIENTIFIC AMERICAN 78 (March 1997). See also Mark Stefik, *Shifting the Possible: How Trusted Systems and*

for copyright management. Trusted systems enable owners of intellectual property perfectly to control access to that property, and perfectly to meter usage of the property that they control.

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 loan it to a friend. You can Xerox pages in it, or scan it into your computer. You can burn it. You can use it as a paper weight. 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 these things — you can sell it, for example, because the copyright law explicitly gives you that right.[48] And 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 sell a police officer with each book, so that the officer followed you around, and made sure you used the book as you promised. But the costs of that are plainly prohibitive. So the seller is stuck.

But what if each of these rights could be controlled, and each unbundled and sold separately? What if, that is, the software itself 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, or not; whether you could use it in another work, for another purpose, or not; or whether you could simply have it on your shelf, or have it and use it as well.

Stefik describes a network where this unbundling of rights is possible. He describes an architecture for the network that would allow owners of copyrighted materials to sell access to those mate-

*Digital Property Rights Challenge Us to Rethink Digital Publishing*, 12 BERKELEY TECH. L.J. 137 (1997); MARK STEFIK, LETTING LOOSE THE LIGHT, IN INTERNET DREAMS: ARCHETYPES, MYTHS, AND METAPHORS, 226-229 (Mark Stefik ed., 1996).

[48] 17 U.S.C.A. § 109.

rials on terms that they wished, and an architecture that would enforce those contracts, as they have been agreed to.

The details of the system are not important here.[49] The essence is simple enough to understand. Digital objects would get distributed within protocols that are layered onto the basic protocols of the net. And the more sophisticated system would function by discriminating in the intercourse it has 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 this more finely grained way. A hierarchy of systems would develop; and copyrighted material would be traded only within that system that controlled access properly.

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

Now imagine for a moment that a structure of trusted systems emerged. Whether it would or not isn't important, though note that nothing would require that it be the only such system. Trusted systems could well interact, and one would expect, if the pattern of the net generally is to be followed, that it would.

But if such a system would emerge, how would that affect copyright law? 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 when compared to other property. The copyright clause of the United States constitution gives "authors" an exclusive right for "a limited time."[50] At the end of that time, the right becomes non-exclusive. It is as if the ownership you have over your car was a lease, extending for 4 years, and then expiring.

The reasons for this limitation are many. But they all reflect an important feature of intellectual property, and they all express a fundamental value that intellectual property not be fully proper-

[49] *See* Mark Stefik, *Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing*, 12 BERKELEY TECH. L.J. 137 (1997).

[50] U.S. CONSTITUTION, Article I, § 8.

tized. There is a commons for intellectual property, and the constitution is committed to feeding that commons. For the commons is a resource for other creators later on. And the commitment of the constitution is that there be lots later on.

The limitation in term is not the only constraint on copyright holders. Another is the defense of fair use.[51] Fair use is a statutorily grounded right that users of copyrighted material have, to use that material in a limited way, regardless of the desires of the copyright owner. I may parody a copyrighted work without the permission of the owner; just as I may quote a limited portion without the permission of the owner.

Fair use, too, is a recognition of the commons of intellectual property. Like the first, it represents a space where one can use without permission. Copyright is a balance between expression that owners can control, and expression that is left open to the commons. And its objective is to assure that this balance be maintained.

Trusted systems threaten to change this balance. It threatens to erase this space for the commons. For trusted systems gives owners of copyrightable material not only the protection that the law might give, but also the protection that limited term, and fair use, try to take away. In real space, the law might guarantee me the right to fair use, or to take when a work falls into 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 its property. The law in effect then denies the owner any cause of action; it withdraws its protection, and leaves the property within the commons.

But there is no similar guarantee with property protected by trusted systems.[52] There's no reason to believe that the code that Stefik describes would be code that guaranteed fair use, or limited term. Instead, the code of trusted systems could just as well protect material absolutely, or protect material for an unlimited term. The code need not be balanced in the way that copyright law is. The

[51] 17 U.S.C.A. § 107.

[52] *See* Carol M. Rose, *The Several Futures of Property: Of Cyberspace and Folk Tales, Emission Trades and Ecosystems*, 83 MINN. L. REV. 129, 144-162 (1998).

code can be designed however the code writer wants, and code writers have little incentive to make their product imperfect.

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

Whether this will be the result of trusted systems one cannot know in the abstract. 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, what should the public do?

In my view, if the public values get displaced, then law should respond. If the system of protecting intellectual property becomes too protective of property — whether too protective because the law is too strong, or because the code is too effective — then the law needs to insist on a balance to this effect. The challenge in such a world is not to preserve copyright, but to understand a copyduty. To protect copyright's commons, by limiting the protection that code might provide.

### *Code replacing Law: "Contract"*

Trusted systems is one example of code displacing law. A second is drawn from the law of contracts. There has been lots of talk in cyberspace literature about how in essence, cyberspace is a place where "contract" rather than "law" will govern people's behavior.[53] AOL, for example, will bind you to enter your name as you enter its system. This is "like" a contract, these theorists say,[54] since one is bound by a set of constraints agreed to when one signed up for service with AOL. It is as if one simply promised to identify oneself as one entered AOL, and when one didn't, AOL would then have a claim for breach of contract. It is "as if" but better: since the obligation is imposed and enforced more efficiently than the same obligation imposed and enforced by contract law.

[53] *See, e.g.*, Trotter Hardy, *Property (and Copyright) in Cyberspace*, 1996 U. CHI. LEGAL F. 217 (1996).

[54] *See, e.g.*, Raymond T. Nimmer, *Article 2B: An Introduction*, 16 J. MARSHALL J. COMPUTER & INFO. L. 211 (1997).

As a contracts professor, I find these claims odd. For code constraints alone are *not* “contracts.” Sure, they are “like” contracts, (they are both self-imposed constraints) but “like” is not “is.” A “lion” is like a “cat”, but one would be quite foolish to let one's kid play with a lion. And so too would one be foolish to assume code contracts 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,[55] 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, that 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 carried out in full. 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, or when the code carries out a self-imposed constraint, these public values do not necessarily enter into the mix. Consequences that a court might resist (forfeitures, for example[56]), 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 nothing requires or assures that this alternative regime will comport with the values of the regime we call “contract.”

[55] For of course there is an important exception here that I have not yet worked through — arbitration agreements, and alternative dispute resolution practices.

[56] *See* RESTATEMENT (SECOND) OF CONTRACTS §229 (Excuse of a Condition to Avoid Forfeiture).

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 an equivalent real space structure constituted by contract. The point is to resist the implication that these structures are necessarily benign, just because an analogous real space structure of obligations imposed through contract would be benign.

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 assures 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 might enforce.

The cyberspace analog has no such equivalent toolbox. Its obligations are not conditioned by the public values that contract 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 realists spent a generation teaching, and as we seem so keen to forget: Contract law is *public* law. "Private public law" is oxymoronic.[57]

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

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

My answer in each case is again no. To the extent these code structures displace values of public law, public law has reason to intervene to restore these pubic values.

## V. COMPETITION AMONG REGULATORS

These two perspectives on the relationship between law and code suggest a more general point: Modalities compete. The values implicit in a given modality of constraint may complete 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.[58] Each modality has a kind of sovereignty. Each sovereignty competes with the others.

I've already sketched a couple examples of this competition. There are more:

*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.[59]

*Digital Audio Technology*: DAT is a code that could make digital copies of digital audio. These digital copies are in principle perfect, and limitless. Thus the code makes difficult the control of copies. Congress responded to this code with regulations that required the code to be different — that required, that is, that it limit the number of serial copies it could make, and if requested beyond some limit, then the quality of the copies would decline.[60]

[58] For example, code writers might make their code available as open code, *see infra* note 65, or they might publish APIs that make it simple to evade the government's regulation.

[59] *See* Communications Assistance of Law Enforcement Act ("CALEA"). PL 103-414, 108 Stat 4279, 47 U.S.C. § 1001 et seq. And in scattered sections of 18 U.S.C. (requiring telephone companies to select a network architecture that facilitates wiretapping).

[60] *See* Audio Home Recording Act, 17 U.S.C. §1002 (1994) (describing the Serial Copy Management System). *See also* United States Department of Commerce, Intellectual Property and the National Information Infrastructure: Report of the Working Group on Intellectual Property Rights 179 (1995).

*Anti-Circumvention:* Trusted systems, as I've described them, are systems that enable control over the distribution of digital objects. They enable this control through encryption technologies, that themselves make unauthorized use extremely hard to effect. These technologies, however, are not perfect; there is code that could succeed in cracking it. And hence the threat of this code is a threat to these systems of control. Congress has responded to this threat, by enacting last year an anti-circumvention provision in the Digital Millennium Copyright Act. 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.[61]

*V-Chip*: The V-Chip is a modification of the code of television, to facilitate ex ante discrimination in the shows that can be seen. Before the V-Chip, the code of televisions was unable automatically to discriminate based on the content of the show. This made it difficult for parents to exercise control over what their kids watched. Congress responded by changing the code of television, to require that it recognize, and block, content on the basis of self-generated ratings.[62]

*Encryption*: There has been a long standing campaign by the government to limit access to encryption technologies. The government's concern is crime; the fear is that encryption will make hiding a crime too easy. To avoid this problem of the uncrackably encrypted messages, Congress has toyed with the regulation of encryption code directly. In September, 1997 the House Commerce

[61] *See* Digital Millennium Copyright Act of 1998. Pub. L. No. 105-304, 112 Stat. 2860-2918, (1998).

[62] *See* In the Matter of Implementation of Section 551 of the Telecommunications Act of 1996, Video Programming Ratings, Federal Communications Commission, CS Docket No. 97-55, FCC 98-35; In the Matter of Technical Requirements to Enable Blocking of Video Programming Based on Program Ratings, Federal Communications Commission, ET Docket No 97-206, FCC 98-36, both at <http://www.fcc.gov/vchip>. *See also* J.M. Balkin, *Media Filters, the V-Chip, and the Foundations of Broadcast Regulation*, 1996 DUKE L.J. 1131 (1996); ACLU, *Violence Chip*, at <http://www.sclu.org/library/aavchip.html>; Kevin Saunders, *The V-Chip: Coming Up Short or Constitutional Overreaching?*, <http://www.wvjolt.wvu.edu/wvjolt/current/issue1/articles/saunders/saunders.htm>; Steven D. Feldman, *The V-Chip: Protecting Children from Violence or Doing Violence to the Constitution?*, 39 HOW. L.J. 587 (1996); David V. Scott, *The V-Chip Debate: Blocking Television Sex, Violence, and the First Amendment*, 16 LOY. L.A. ENT. L.J. 741 (1996).

Committee came 1 vote shy of recommending a statute that would have made it a crime to distribute encryption technologies that did not include within it an ability for law enforcement to intercept and decrypt the content of the technology.[63] Again, this was a regulation of code to enable stronger regulation by government.

These examples of law regulating code can be balanced with examples of code displacing law. Consider just a few here:

*Taxation*: As internet commerce grows, the ease with which people can transact increases. It is now easier to buy books or airplane tickets from vendors on the net than it is to buy them at the local bookstore, or travel agent. This means that both the quantity of online commerce has increased, and the average price of online commerce has decreased. In 1998, there was plenty of mail-order; there was not as much mail-order for very inexpensive items. This increase, and decline, has made it harder for taxing authorities to collect taxes on the underlying transactions. The change here has disabled tax collection that would have been easier when located geographically.[64]

*Content:* Nations have preferences about the content of speech that their people get exposed to. Before the internet, there were many ways for these nations to effect this constraint. Control on the post, control on TV, control on radio and television broadcast — these were all modes of regulation that facilitated the control of content getting in. The net changes all this. Now it is much more difficult to control who gets access to what, with the result that much less content is controlled. The first amendment, as it were, has been wired into the phones, with a corresponding decline in a nation's control over content.

These examples could be multiplied, but the lesson they teach should be clear enough. An arms race of sorts is inevitable in this

[63] H.R. 695, 105th Congress, The Security and Freedom Through Encryption (SAFE) Act of 1997, Oxley-Manton Amendment.

[64] *See* Sandi Owen, *State Sales & Use Tax on Internet Transactions*, 51 FED. COMM. L.J. 245 (1998); Walter Hellerstein, *State and Local Taxation of Electronic Commerce: Reflections on the Emerging Issues*, 52 U. MIAMI L. REV. 691 (1998); David S. Prebut, *State and Local Taxation of Electronic Commerce: The Forging of Cyberspace Tax Policy*, 24 RUTGERS COMPUTER & TECH. L.J. 345 (1998); Internet Tax Freedom Act, Pub. L. No. 105-277 (1998).

balance between sovereigns, and with no supremacy clause to counteract it, it is unlikely that there will be a resolution of this conflict soon.[65]

This conflict should push us to principle. We should think again about the values that should guide, or constrain, this conflict between authorities. In the last section below, I want to sketch two. These are by no means the only principles that ought to concern us; they are simply the two whose remedy seem least obvious. And they are two that might show something about what a law of cyberspace might teach more generally.

## VI. LESSONS

Two values are at the core of this competition between code and law, though how they intersect depends upon the context. First there is a question about transparency — is the effect of law on code and is the effect of code on law transparent? Second, there is a question of over-inclusiveness — does the regulation effected by law reach more broadly than the justification for the law; does the regulation effected by code reach more broadly than the justification for that code?

My argument is that at least in the case of law regulating code, these values of transparency and avoiding over-inclusiveness should constrain law's effect. And beyond this, my argument is that the same values should constrain code.

### *Questions about law's regulation of code*

The lesson of section II was that there is a range of tools that law might use to bring about a particular behavior; the lesson of

[65] I've made an important simplifying assumption in this analysis, which I relax in other writings. *See* Lawrence Lessig, *The Values in Open Code: Regulatory Standards* (forthcoming, 1999). My assumption is that the code writers in these examples — the target 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; it is not easily modified, or changed. 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 would be 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. This means that a world where the application space is primarily or mainly open source software is a world of diminished regulability.

section III was that the most effective tool that law might use is the regulation of code. By directing code-writers to build into their code features that better enable regulation, government can steer cyberspace in a direction that would make it more regulable.

This form of regulation (through architecture as well as law) is not new to cyberspace; my claim, at most, is that its significance is new. While in the past, in limited contexts, the state has had the opportunity to regulate in a way that would increase regulability,[66] it has not had this opportunity in such a fundamental way.

*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 that a code solution could be crafted. Some will be more narrow than others. By narrow, I mean less generalizable — they 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.

By constitutional question, I don't mean a question presented by the American constitution. This may be a question the American constitution answers. It may not. My point is not that debate. Instead, my aim is a more general question — whether a meta-principle should limit the scope of any liberal government's regulation.

Two examples will make the point. In the Digital Millennium Copyright Act, Congress included an "anti-circumvention" provi-

[66] *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), where the Court struck down Section 3 of the Johnson Act which required manufacturers and dealers to file monthly records of sales and deliveries and to register annually with the Attorney General. *See* Johnson Act, ch. 1194, S 3, 64 Stat. 1135 (1951) (codified as amended at 15 U.S.C. S 1173 (1982))). The authority for the "required records doctrine" is Shapiro v. United States, 335 U.S. 1 (1948), though it has been limited by Albertson v. United States, 382 U.S. 70 (1965) (limits application of required records/self reporting doctrine to genuine regulatory purposes). *See also* Marchetti v. United States, 390 U.S. 39 (1968), Grosso v. United States, 390 U.S. 62 (1968), Haynes v. United States, 390 U.S. 85 (1968) (all finding reporting requirements in violation of the Fifth Amendment because they were not regulatory in nature).

sion.[67] 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 only problem with this structure, however, is that it gives more protection than the underlying copyright law would. As critics of the anti-circumvention law pointed out,[68] the law would make it a felony to develop technologies to circumvent these technologies even where the use made of the underlying material would not have been a copyright violation.

This is because not all uses of copyrighted material are violations of copyright law. As I described in section IV above, fair use is a permissible use of copyrighted material. Yet the anti-circumvention provision would punish a circumvention that simply enabled this 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 in this way overbroad. The law, for example, could have made circumvention an aggregating factor in any prosecution for copyright violation. But by protecting the code more than the copyright, the law creates the incentive for the privatized copyright that I described in section IV. It protects, that is, schemes whose ultimate effect may well be to displace the balance that copyright law strikes.

A second example is more troubling. I described in section III a scheme for facilitating the zoning of speech in cyberspace. In my view, the law could steer the architecture of cyberspace towards an ID enabled space.

But there are many designs for an ID enabled cyberspace. And the consequences of these different designs for the regulability of cyberspace generally are very different. I described in section III a version of a kids ID. This would be a browser that anonymized

[67] *See* Digital Millennium Copyright Act of 1998, §1201, Pub. L. No. 105-304, 112 Stat. 2860, 2863-2872 (1998).

[68] *See, e.g.*, Pamela Samuelson, *A look at…whose ideas, anyway? Facing a Pa-Per-Use Future*, WASH. POST, Nov. 1, 1998, at C03; Pamela Samuelson, *The digital rights war*, WILSON QUARTERLY, Oct. 1, 1998, at 48.

personal information from the user, but that signaled that the user was a minor. The design would make it possible for servers with adult material to know that the client was a kid, and thus facilitate not serving kids-identified clients; it would also enable sites that collect data to comply with laws that banned the collection of data from kids.

A different ID enabled cyberspace would be one that created incentives for users in effect to carry digital IDs.[69] These would be digital certificates that would certify certain facts about the holder of the certificate. These facts could include, for example, the age of the holder, the citizenship of the holder, the sex of the holder, the name of the holder.

Now 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 an age-ID would enable other regulations related to being an adult — gambling, perhaps, or voting.

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

If Congress' aim is to facilitate zoning of adult speech, my view is that a kids-ID would always be a less restrictive means than an adult ID. But if the Court disagrees, then the over-breadth concern becomes pressing. For by creating the incentives for broader IDs, the state could create the incentives necessary to facilitate much broader regulation of behavior in cyberspace. The regulation would extend beyond the state's legitimate interests in regulation, and facilitate regulation far beyond adult speech.

In each example, the structure is the same. In both, there are at least two changes in architecture that might facilitate a state end.

[69] The government is already exploring this idea, and in my view, not well. *See* Access Certificates for Electronic Services (ACES) proposal at <http://www.gsa.gov/aces/default.html>, "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." *Id.*

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

The question in each is whether there is a value that would tilt in favor of the narrower rather than the broader regulation. Within the context of speech regulation, there obviously is. But ID regulation is ambiguously related to speech. It could be advanced for reasons other than for speech. And if it were — for example, to facilitate online banking, or credit card use, etc. — then the same question about by-products would still remain. The government might have a legitimate need to regulate to induce a certain ID, but the consequence of that ID might be to flip the unregulability of the space generally.

*Transparency*

A second problem with the laws' regulation of code is transparency. When the state demands that individuals behave in a given way, the individuals realize that it is the state that is regulating. If they don't like that regulation, they can elect representatives who will repeal it. The regulation is thereby checked by the political process.[70]

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? (If not formally, then at least by effect.) Then this constraint of political accountability would no longer remain. Then the government could achieve its end both without paying the political price, and without reducing the effectiveness of its regulation by its regulation being tied to the government.

The case of *Rust v. Sullivan* is an example.[71] The Reagan administration was opposed to abortion. Some in the administra-

[70] *See* 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."). *See also* Meir Dan-Cohen, *Decision Rules and Conduct Rules: On Acoustic Separation in Criminal Law*, 97 HARV. L. REV. 625 (1984).

[71] Rust v. Sullivan, 500 U.S. 173, 111 S. Ct. 1759 (1991).

tion wanted to reduce the incidence of abortion. One class of women who might be persuaded against abortion included those who visited family planning clinics. They might be persuaded to choose life over abortion.

But obviously, given *Roe v. Wade*,[72] the government is constrained in the means it might select. Though it need not fund abortion, it can't ban all abortion. And while it might argue against abortion — erecting warnings, for example, within any family planning clinic that it funded saying "the administration believes choosing life is better than choosing abortion" — these arguments would likely be ineffective. Warnings from the government would be treated as warnings from the government — in this case, the product of politics, many would believe, and little more.

Thus the administration chose a different, and more effective technique. It required that doctors in family planning clinics not recommend or discuss abortion as a method of family planning. Instead, if asked, these doctors were to say, "advice regarding abortion is simply beyond the scope of this program."[73]

Now the genius in this method of regulation is that it effectively hides the government's hand. As Laurence Tribe argued in the Supreme Court,[74] it permits the government to transmit its message without tying the message to the government. Many women would conclude that it was their doctor who was steering them away from abortion — since it would be the doctor who was saying or not saying something about abortion. The government would be achieving its objective by undermining transparency. The success of the program would turn upon defeating transparency.

Cyberspace presents the opportunity for *Rust* writ large. For it is a feature of peoples' 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 23 people in the chat room, one is more likely to believe this con-

[72] Roe v. Wade, 410 U.S. 113, 93 S. Ct. 705 (1973).

[73] Rust v. Sullivan, 500 U.S. 173, 200, 111 S. Ct. 1759, 1776 (1991), "advice regarding abortion is simply beyond the scope of the program".

[74] *See* Oral arguments of the Supreme Court, collected by Northwestern Law School at http://oyez.nwu.edu/cases/cases.cgi?case_id=340&command=show.

straint is in some sense compelled by the nature of the space. But of course, 23 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 avoid some of the cost of those choices.

Now again, my claim is not that this opportunity is new, nor that every regulation through architecture is non-transparent. When Robert Moses built the bridges to Long Island to block busses, so that African Americans (dependant primarily on public transportation) could not easily get to public beaches,[75] that was a regulation through architecture, and that regulation hid well the politics of its regulation. But when the state builds a speed bump on an air-terminal access ramp, that is also regulation through architecture. But that regulation in no way hides its policy — no one believes that nature has placed the speed bump in the middle of the road.

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

Transparency, traditionally, has been a value that constrains the promulgation of regulation. While the framers kept secret their deliberations, and while the Senate perpetuated this secrecy until 1795,[76] the rule of law has always required that a law be public before it is effective. The APA pushed this value even further — in response to the emerging administrative state, the APA es-

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

[76] *See* RICHARD ALLAN BAKER, THE SENATE OF THE UNITED STATES: A BICENTENNIAL HISTORY (1988).

tablished procedures that demanded openness in the administrative process.[77]

Cyberspace raises this question of transparency in yet a new context. When the government regulates indirectly, through the regulation of cyberspace's code, should it be required to make the regulation transparent?[78]

### *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 replaces the values that law has embraced. And if the values of law are to survive, law might well have to respond.

My examples in section IV describe two particular cases where the values of a legal regime are being replaced. But we can describe this displacement more generally. In the general case, the values that the code is embracing are values of bottom-up control. They enable control from bottom-up structures, such as contract-like, or property-like systems. And they interfere with top down impositions of rules that would not otherwise be chosen.

Now again, this does not mean that government can't regulate, for as I've described, government can use indirect techniques to affect 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, there are interests that gain more individually from a particular architecture than 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.

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

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

There are two obvious examples of this point. Privacy is one. I've described a way that government could in effect subsidize architectures for privacy. But 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 effect privacy protection. But their interests pale in comparison to the interests, and market power, of commerce in cyberspace. As the FTC has described,[79] 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 will be different from the past.

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

SPAM, or Unsolicited Commercial Email, is a second example.[80] SPAM is the sending of unsolicited commercial email, usually in bulk, to lists of email accounts across the internet. These lists are extremely cheap — $100 for 10,000,000 names — and this for a very low price, one could send 10,000,000 emails using this list, and hope for even a very small return to make a profit.

This possibility is a function of the design of email. The initial architecture for email did little to authenticate users of email relays. The SMTP (Send Mail Transfer Protocol) protocol, for example, which is still the dominant mail protocol, has a feature that allows third-party relays of mail without an account on the primary mail system. With SMTP systems configured to accept third-party relay, I could 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 email.

[79] *See* Privacy Online: A Report to Congress. Federal Trade Commission, June 1998 at <http://www.ftc.gov/reports/privacy3/index.htm> ("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." (Conclusion of Report)).

[80] *See* <http://spam.abuse.net/spam/faq.html>.

Third party relay is not the only technique spammers use. But it is the location 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 assure the channel is not abused by spammers.

Others on the net, viewing third party relay as the biggest cause of a spam want these channels closed. And some of these others have organized blacklists of open relay systems, which subscribers use to determine whose mail they will bounce. If your email administrator has left your relay open, then your site is likely to be added to these lists; if your site is added to these lists, then email to 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. 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. For these blacklists create conflicts that reach far beyond the simple listing of a site or not.

Consider one example of a potentially explosive battle.[81] This particular skirmish began at MIT (as so much about the Internet begins at MIT). In late 1998, Jeff Schiller, MIT's network administrator, began receiving e-mail from users of the system, complaining that their mail to others outside the MIT domain had been blocked. It took little to discover that the mail was being blocked because a spam vigilante, Open Relay Blocking System (ORBS), had decided that the MIT network had "bad e-mail practices." Without notice, MIT was placed on ORBS's black list, and subscribers to ORBS began automatically to exclude MIT mail.

No one likes to be accused of "bad e-mail practices," especially not a MIT-type. And so it was just salt in the wound when one company in particular confirmed its policy of blocking according to

[81] *See* Lawrence Lessig, *The Spam Wars*, THE INDUSTRY STANDARD, Dec. 31, 1998.

the ORBS list — Hewlett Packard. Mail from MIT to HP would not go through, MIT was told, until MIT changed its network policy.

But MIT was not to be bullied. In Schiller's view, its decision to not automatically block all "third-party relay" e-mail (e-mail sent through the MIT server without authenticating that the sender is associated with MIT) made sense for its network, and the MIT community. MIT is not pro-spam; like any decent network, it adopts measures to limit spam, in particular by policing the use of its "third party relay" facility. But its methods are not the methods of ORBS, which made MIT an ORBS enemy.

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

Until a god of sorts intervened — a network services god, that is. 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 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. But as with privacy, 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, they adopt techniques that are both under and over inclusive, and for those drawn into a black hole by these techniques, they invite real conflict.

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

In this view, spam was "caused" by the effect code had on the market — facilitating low cost advertising. The response is a law that increases the costs in the market — decreasing the incidence of low cost advertising. Law here would compensate for the change in code. Consensual communication would still be cheap; nonconsensual communication would still be cheaper than in real space.

These two examples point to a more general need. Cyberspace needs a way to act collectively, in the relatively small number of cases where bottom-regulation leaves some important legal value unprotected. As it is just now, this collective regulation is resisted by many on the net. But we should resist simpleton distinctions — the choice has never been between anarchy and totalitarianism. The choice is only about the best mix of these two extremes.

***

My aim in this section has been to highlight a set of values to 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 the law can achieve its end through code, with the result that its end is achieved non-transparently, we have reason to question the technique of law. And to the extent the law can achieve its end through code, we have a reason to require that the code be narrowed to just the legitimate state end.

Likewise the other way round. When a structure of code effects values implicit in the law, there is good reason to assure 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 have reason to check the aggregation made through the bottom-up design of code.

## VII. Conclusion

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." This essay has been a respectful disagreement. Whether there is something to be gained by thinking generally about the law of the horse, my argument has been that we learn something general about real space law by thinking in particular about the law in cyberspace. Much more significantly than in real space regulation, the law of cyberspace will be a trade-off among regulators of very different kinds. Understanding that trade-off, and developing principles to help guide, tells us something significant about law, both real and cyber.

At the center of the lesson about cyberspace is an understanding about the place of law. We face a choice about life in cyberspace — a choice about whether the values imbedded there will be the values we want. The code of that space has the power to constitute values that resonate with our tradition. It also has the power to constitute values inconsistent with our tradition.

As the net grows, as its regulatory power increases, as its power as a source of norms becomes established, the values of real space sovereigns lose. In many cases, that is a good thing. But there is no reason to believe that it will be a good thing generally. There is nothing to guarantee that the regime of code will be a liberal regime; and little reason to expect an invisible hand of codewriters to push it in that way.