
Ethics and Information Technology **3:** 137–150, 2001.

Code and moral values in cyberspace

Richard A. Spinello
Carroll School of Management, Boston College, Chestnut Hill, MA 02467 USA
E-mail: richard.spinello@bc.edu

Abstract. This essay is a critique of Larry Lessig's book, *Code and other Laws of Cyberspace* (Basic Books, 1999). It summarizes Lessig's theory of the four modalities of regulation in cyberspace: code, law, markets, and norms. It applies this theory to the topics of privacy and speech, illustrating how code can undermine basic rights or liberties. The review raises questions about the role of ethics in this model, and it argues that ethical principles must be given a privileged position in any theory that purports to deal with the shaping of behavior in cyberspace. Finally, it proposes a philosophy of ethical self-regulation instead of an over-reliance on government policy to deal with certain improprieties and negative externalities that tend to disrupt the Net.

Key words: anonymity, black holes, code, copyright, core values, cyberspace, encryption, freedom, free speech, internet architecture, internet filters, invisible regulation, liberty, privacy, regulation, self-regulation, spam, values, zoning

Larry Lessig ends his book, *Code and other Laws of Cyberspace*, on an ominous note. In a brief concluding chapter called "What Declan doesn't get" we hear unmistakable echoes of the death knell tolling for a free and open cyberspace. Cyberspace was originally a place where people could move about and speak freely. It was a place without boundaries, unencumbered by the regulations and restrictions that typify the real world. But this anarchic environment seems to be living on borrowed time thanks to the growing commercialization of the Web and the concerns of some anxious governments. What could take its place is an internet with some unattractive features: a depleted intellectual commons, pervasive filtering, the disappearance of privacy and anonymity, and a preponderance of precarious borders established by nervous sovereignties. In a few years it may be difficult for many of us to recognize the Net of 2001.

Declan McCullagh is a libertarian columnist who writes for *Wired News*. According to Lessig, he, like most libertarians, is misguided about what it will take to preserve an open and free-spirited internet with unfettered access. Declan believes that government is the enemy of the Net's vitality and openness. But, in reality, government policy will be needed as a corrective to those private parties on the Net who seek to undermine this liberating technology, especially through the use of software programs that are changing the Net's character. The message in this chapter is clear: cyberspace is destined to change and not for the better, as it migrates from an architecture of freedom to an architecture of the panopticon. But there is some chance that this transformation can be tempered and moderated if it is guided by government policy sensitive to human rights and freedom-enhancing values. This is what Declan "doesn't get."

Are these dark concerns really well-founded, or are they merely exaggerated? Should we be as apprehensive about the Net's future as Professor Lessig? Is commercialization and private action rather than government control the real villain? And is government policy a critical deterrent to the excesses that threaten the Net's future?

These are some of the difficult questions, suggested by this extraordinary book, that will be addressed in this essay. Although sympathetic with the broad lines of Lessig's argument, we will offer a different perspective on several salient themes in *Code*. Our disagreement with Lessig's analysis will center on two interrelated concerns. First, why is there no explicit treatment of ethics or morality in a book that talks so much about "constraints" and "regulating behavior?" What role does ethics (as opposed to conventional norms and customs) play in shaping our behavior in cyberspace? Lessig discusses "values" but one cannot be sure that they are properly grounded moral values. Second, Lessig assumes that the Net will evolve in a certain way once it is in the firmer grip of commercial forces; he has little faith that responsible behavior is possible in cyberspace without the coercive force of government. Hence he underestimates the feasibility of internet self-regulation. There is a case to be made for allowing a more decentralized approach to the resolution of some social problems in cyberspace as long as one does not lose sight of core moral values that should always guide our behavior no matter where

we are, real space or cyberspace. Why not try *ethical self-regulation* before we craft a plethora of new laws and restrictive policies that will inevitably encumber our movements in the realm of cyberspace? Why not permit and encourage an order in cyberspace that is primarily emergent rather than one that is imposed, even if that order is more fragile and conflict-laden?

As we will see, this is an important and enlightening book, which deserves the considerable attention it has received since its publication in late 1999. Lessig's evocative arguments are logical and well-conceived, and, for the most part, they are quite plausible. However, although the Net has changed and although there has been a substantial increase in commercial activity, cyberspace still reflects the social and cultural values of open democratic societies. Lessig's bleak vision of the future is probably somewhat exaggerated, but even if it is not, it remains to be seen whether a large dose of government intervention is the right antidote for the potentially deleterious effects of commercialization.

The four constraints

If there is one myth about cyberspace that Lessig seeks to expose, it is the facile and simplistic assumption that the Net has a fixed and unalterable nature. According to libertarian orthodoxy, the essence of cyberspace is liberty itself. This is a place where packets of information can and should flow freely without discrimination or interference. And government should keep its hands off the Net to preserve that liberty.

But this sort of thinking manifests the naturalistic fallacy – it assumes that the Net has some sort of irreducible nature or set of essential qualities that are independent of exogenous forces such as the regulatory schemes of governments. Lessig correctly argues that the Net's nature is not fixed. It is completely dependent on its underlying protocols and software architectures. The Net is no more or less than these protocols such as TCP/IP, HTTP, or FTP. The Net's properties are determined by code, which is written by programmers, and that code can be rewritten.

In order to appreciate precisely what Lessig means by "code" we must consider his compelling analysis of how code has become the most effective regulator in cyberspace. As a basis for that discussion, Lessig first describes the four distinct but interdependent constraints that regulate behavior in the physical world: law, norms, the market, and architecture.

An example will best illustrate how these constraints function. Consider how society attempts to deal with the problem of dangerous drugs, substances like heroin or cocaine. First, regulators and law enforcement authorities rely on laws banning the sale and use of these drugs. These laws are supported by the threat of sanctions, so if one is caught selling drugs one will most likely be sent to jail. Second, the marketplace regulates the use of drugs by means of price. If it costs $50 for a dose of cocaine, a high school student who cannot afford this amount of money, will not be able to make the purchase. Drug users are also constrained by social norms. According to Lessig (1999), "those normative constraints imposed not through the organized and centralized actions of the state, but through the many slight and sometimes forceful sanctions that members of a community impose on each other" (p. 235).[1] There are norms in families and communities against taking drugs and those who do so might be punished or pressured to stop.

Finally, there is the constraint of architecture, simply the way the world is, or as architects themselves call it, "the built environment." Architecture includes the laws of physics as well as technology and it determines and shapes our environment. Quite often, we are powerless to transcend the constraints imposed by nature. There are countless examples of how architecture affects our life: locked doors exclude us from certain places, the great arc of the Swiss Alps shut off the Roman empire on the north from many barbarian invaders, speed bumps slow down speeding automobiles. In the case of illicit drugs there are architectural constraints imposed by the technologies affecting their supply. Natural disasters or man-made actions that destroy poppy fields might be one example of this.

Each of these constraints is a "distinct modality of regulation" (p. 88). Each can support or oppose the others – architecture, for example, could reinforce or undermine law. Also, what particularly differentiates the constraint of architecture from law, norms, and the market is that it is 'self-executing.' People may be involved in constructing a certain architecture but in the end it constrains immediately and directly without the mediation of another human being. The Swiss Alps impeded the progress of Hannibal and his elephants without the intervention of the Roman armies.

What does any of this have to do with the Net? Just as in real space so in cyberspace, 'regulations' are also a function of the interaction of these four constraints. Laws, such as those that provide copyright and patent protection, regulate behavior by prescribing or forbidding certain activities and by imposing sanctions for violators. Markets too regulate behavior in various

[1] Unless otherwise indicated, all other references citing Professor Lessig's writings will be to *Code and other Laws of Cyberspace*.

ways – advertisers gravitate to more popular Web sites which enables those sites to enhance their services; the pricing policies of Internet Service Providers determine who gets access to the internet; and so forth. And there are norms that regulate cyberspace behavior, including internet etiquette and social customs. For instance, flaming and spamming represent violations of Net etiquette; they are considered 'bad form' on the internet and those who engage in these anti-social activities will most likely be shunned or rebuked by other members of the internet community.

What parallels real space architectures is described by Lessig as "code," that is, the programs and protocols used on the internet, which also constrain and control activities. Lessig's recognition that this code is an instrument of social and political control is the principal insight of this book. The code writer, the software developer, is the prime architect and the regulator in this strange new place. And code controls or regulates more perfectly and completely than law, without loopholes and ambiguities.

There are countless examples of how code controls our interactions on the Net. Code can limit access to certain Web sites by demanding a username and a password. Encryption code can help to ensure the confidentiality of important communications. Software programs have recently appeared that effectively filter out unsolicited commercial e-mail (or spam). There are no federal laws to contain the persistent activities of spammers, which rankles many users, but there are innovative filtering programs and black holes such as the famous RBL (Realtime Blackhole List) to contain their efforts. Indeed in cyberspace one could argue that we really don't need regulations about spam because the code replaces the law. Or, to put it more emphatically in Lessig's terms, *the code is the law*.

While the power of code is undeniable, Lessig reminds us that governments have not lost their ability to regulate by law. Law can regulate directly by dictating how to behave and by threatening punishment for misbehavior. Or the function of law can be indirect when "it aims at modifying one of the other structures of constraint" (p. 95). Lessig uses the example of discrimination of the disabled to illustrate how the law operates indirectly. Besides making such discrimination illegal, government could insist on educating children about disabilities in order to change social norms, it could subsidize companies that hire the disabled (regulating the market), or it could mandate new building codes so that buildings are more accessible to the disabled (regulating architectures). In these cases, "the government is commandeering the power of another modality – another structure of constraint – to effect its own ends" (p. 98). Thus we should not underestimate the power of law in cyberspace which can also regulate there 'indirectly' by influencing the market or by requiring the deployment of certain forms of code.

One example of this is the United State's concerted efforts to regulate or control encryption code. Although U.S. policies were recently liberalized by the Clinton Administration, for many years the United States government banned the export of sophisticated encryption technology. It consistently demanded that this technology provide a back door so that law enforcement authorities could get access to the communications of terrorists or other criminals if necessary. We see that while the code of cyberspace has sovereignty, it can still be decisively trumped by the regulatory power of real sovereigns, who delineate the parameters for how and where a given piece of code can be utilized.

The architectures of control

We can now begin to comprehend more clearly why cyberspace may be in the throes of a radical transformation. In his writings Lessig differentiates between what he calls "Net95," and the Net of today. Net95 is the original Net, the one that libertarians wistfully idealize. This is the non-commercial Net, characterized by unregulability and liberty. "So long as one had access to Net95," Lessig (2001) writes, "one could roam without identifying who one was ... one's identity, or features, were invisible to the Net then ..." (p. 118). The Net of 1995 gave rise to predictions about the 'twilight of sovereignty,' the rapid demise of government power, and maybe even the withering away of the nation state. But Net95 has changed because the code of the internet has changed. "The architecture is shifting from an architecture of freedom to an architecture of control" (Lessig 2001, p. 120). The internet has evolved into a commercial infrastructure, and commerce does not flourish where there is anarchy.

Lessig is deeply worried about this change, especially since it is being effected primarily by code. He is troubled about the regulatory impact of code, which can be a more perfect and thorough form of regulation than law. In cyberspace, code can perform the same tasks as the law, and maybe even do it more effectively. According to Lessig, "effective regulatory power [shifts] from law to code, from sovereigns to software" (p. 206). This is a significant transformation and we must try to appreciate its broad implications: "In cyberspace we must understand how code regulates – how the software and hardware that make cyberspace what it is *regulate* cyberspace as it is" (p. 6, emphasis in original).

What is so problematic about code-based regulations? One of the most serious problems endemic to the use of code is that its regulatory impact is often occluded, hidden in lines of obscure, proprietary source code. When parents buy a filtering program to protect their children from pornography they may be unaware that the program also blocks out sites dedicated to feminist causes. Code is usually hidden and nontransparent, but law is public. As *Code* suggests, we should be worried about forms of "invisible regulation." This puts users at a great disadvantage and opens the way for all sorts of subtle manipulations.

We would surely have major difficulties with laws or a legislative process that lacked transparency. Lon Fuller's theory of "internal morality" speaks to this issue. Internal morality is a set of norms that must be respected if the mission of a practice such as 'legislating' is to be realized. The internal morality of legislation requires generality, publicity, intelligibility, and constancy. According to Fuller (1969), "no statute should become law until it has been given a specified form of publication" (p. 43). This mandate to publicize the law should itself be a legal requirement, but Fuller also remarks that "a moral duty with respect to publication is also readily imaginable" (p. 43).

While code writing is not legislating in the strict sense Lessig's arguments have demonstrated that there is an analogy between these two proscriptive activities. There is something wrong with law that is not publicly promulgated just as there is something wrong with code that constrains behavior and does so in an opaque or surreptitious manner. In both cases there is a moral flaw in craftsmanship, since transparency helps restrain arbitrary power.

Lessig is certainly not the only one to recognize the power of code as a surrogate for law and to voice these concerns. He cites the work of William Mitchell (1995) who first developed the seminal notion that "code is law." He also notes the influence of scholars like Katsh (1996), Reidenberg (1998), and Boyle (1997) who have been working on similar themes. Shapiro's (1999) influential book, *The control revolution*, has also been instrumental in popularizing this idea. Like Lessig, Shapiro worries that obscure pieces of software code will be manipulated as repressive instruments of social control. Shapiro seems especially disquieted about the potential abuses of code emanating from government authorities: "it is the very obscurity of code regulation that would allow the government to gradually and imperceptibly alter technology to achieve its aims without public scrutiny" (p. 73).

Lessig shares Shapiro's concern that code will be abused by the public sector, but he sees the 'invisible hand' of commerce as the primary villain. It must be recalled that the Net was constructed for research purposes, not for commerce. It evolved as an open and insecure network, but this is not suitable for commercial purposes. As a result, many architectures (e.g., SET, SSL) have been introduced in cyberspace in order to make it more secure. These programs authenticate and verify identities to help reduce fraud. Moreover, many predict that compulsory use of Digital ID's, which will facilitate the traceability of all internet transactions, is probably just on the horizon. This is how commerce is helping the Net to change from an architecture of freedom to an architecture of control. The Net is being inverted, and commerce is the inexorable driving force behind this inversion

The power of code – P3P, filters, and black holes

After explaining his overarching theory, Lessig applies it to three traditional areas of concern: privacy, free speech, and intellectual property. There is too much ground to cover here so we will confine our attention primarily to the issues raised in the sections on privacy and speech. We will consider how code, developed and implemented by private parties, can end up being subversive or insidious, an unmistakable threat to traditional social values.

Privacy

The problem of privacy erosion in cyberspace is by now quite familiar. Privacy is under siege as never before thanks to the power of digital technologies. The chapter on privacy in this book delineates three conceptions of privacy. The first is the 'utility conception' which identifies privacy with our desire to minimize intrusion. For the most part we want to be left alone so we seek protection that minimizes the extent to which our solitude and tranquility is interrupted. The second conception is 'privacy as dignity.' It holds that certain activities, even if they are only minimally intrusive, are still an affront to one's personal dignity and should not be trivialized. An individual may be completely unaware of a covert search by the state of his or her possessions. But even this type of unobtrusive search may still cause dignitary harm. The state, therefore, must have compelling reasons for initiating such a search. The third conception is more substantive: "privacy as a way to constrain the power of the state to regulate" (p. 148). Privacy is regarded as a limit on the government's power and on the scope of regulations that it can impose.

In today's world one may get different results in making a judgement about whether an activity violates privacy depending upon which conception of privacy is

invoked. The utility conception might support an efficient search that would not be allowed by the dignity and substantive conceptions. However, at the time the U.S. Constitution was written in the 18th century, these three conceptions would not yield different conclusions. Thanks to technology the context has changed: technologies can search without disturbing, without being the least bit intrusive, and this raises a conflict about what is protected by the Fourth Amendment. And because the framers did not work out "what the amendment would protect in a world where perfectly noninvasive searches could be conducted" (p. 149), we are forced to make choices.

Threats to privacy are rampant in cyberspace. According to Lessig, the major threat comes from monitoring, collecting data about an individual's day-to-day activities. This data might include credit card records, purchases made at the supermarket, web sites visited, or even a toll booth's electronic records. Thanks to monitoring, "your life becomes an ever increasing record; your actions are forever held in storage, open to being revealed at any time, and therefore at any time demanding a justification" (p. 151).

It is especially troubling that the Web's underlying architectures have altered the material causality of privacy invasions. Code is undermining the very possibility of privacy on the Web. On one level, there are "intrinsic privacy vulnerabilities" that can be traced to the way Tim Berners-Lee developed the Web (Hamilton 2000, p. B1). Consider how HTTP operates: for a Web server to know where to send its Web page it needs an Internet Protocol (IP) address. This address identifies one's unique location on the Net, and browsers must provide that information to the server when a Web site is requested. Thus, in most cases an internet user's IP address can be used to track his or her activities on the Web. Also, according to Hamilton, "other vulnerabilities lurk in technologies that weren't originally part of the Web, but that have since become ubiquitous" (p. B1). For example, cookies and Web bugs keep track of one's Web browsing activities. And smart microchips represent another architecture that is designed to invade one's personal space.

What's wrong with this assault on personal privacy? Lessig cites three values that are put in jeopardy. The first is the "benefit of innocence." As Rosen (2000) puts it, there is something unfair about being "judged out of context" (p. 8). There are many innocent facts about us that become part of the searchable record produced by this ceaseless monitoring. Some of this data may be ambiguous especially when looked at as discrete elements and taken out of context; the burden is now on the data subject to demonstrate his innocence. The second value threatened is our ability to live in separate communities or separate "normative spaces" which is enabled by our ability to control data about ourselves. A gay man living in a small town with a provincial outlook may need privacy to protect himself. Privacy "disables the power of one dominant community to norm others into oblivion" (p. 153). The third value emanates from concerns about profiling which can lead to subtle forms of discrimination in cyberspace. For example, certain perks or products are available only to those who fit a certain profile as determined by the collection and synthesis of certain data.

What is the optimal solution to this threat to our personal privacy? Is it the European solution, an extensive array of laws that solidly protect citizens against the misuse of their data by insisting on informed consent? Or is industry self-regulation a better approach? This would be a normative solution emphasizing corporate self-restraint, and implemented though industry codes of conduct. Lessig is understandably wary of such an approach. What might work, he says, is an architecture like P3P, that would protect privacy rights. P3P stands for Platform for Privacy Preferences Project. It is a technological framework that relies on predefined standards set by the user to negotiate with Web sites about how that user's information will be utilized and distributed to third parties.

However, such an architecture needs the backing of law. That law, according to Lessig, should enforce a property right in privacy, that is, in one's personal information. A property regime would allow people to value their privacy in different ways – some might place a premium on their privacy and insist on a high level of confidentiality, while others may be willing to sell their information for the right price or exchange it for some other benefit. An architecture like P3P would facilitate the negotiation with the web site or other source seeking one's data. The value of endowing personal information with a property right is that those who want information for possible reuse must negotiate and compensate accordingly before they can collect it. Code threatens privacy but perhaps code can be part of the solution. Code and law working in tandem have the potential to promote choice while still safeguarding a user's privacy rights.

Speech

Another threatened value in cyberspace is free speech. The internet has provided an extraordinary forum for anyone to exercise his or her free speech rights. But not all forms of speech are welcomed in cyberspace. There are problematic forms of speech on the Web which lead to curbs on free expression. Thanks to anonymity, encryption technologies and the Net's decentralized

structure, it is immensely difficult to control speech in cyberspace. This has been an exceptional and welcome challenge for repressive regimes throughout the world – they are impotent in the face of a system that empowers dissenters and promotes democratic values. As Lessig observes, "We have exported to the world, through the architecture of the Internet, a First Amendment *in code* more extreme than our own First Amendment *in law*" (p. 167, emphasis in original).

But how should we contain truly perverted forms of speech such as hate speech, often laced with racist rhetoric, and pornography, often graphic and violent. Pornography is difficult for young children to acquire in real space, but in cyberspace where the default is anonymity there are fewer limits on its distribution. The architecture of the Net makes pornography much more accessible even for children. How do we prevent impressionable children from viewing the many disturbing sites that have proliferated through cyberspace? What is the right mix of law, norms, the market, and code? In the United States the first instinct was to try a legislative solution. Hence, there was an effort to criminalize the transmission of indecent material to minors. This was the Communications Decency Act (CDA) of 1996, which was ruled unconstitutional by the Supreme Court in its controversial *Reno* v. *ACLU* decision. The CDA, which made it a felony to transmit "indecent material" on the Net to a minor, was deeply flawed. It was too vague and imprecise, and it did not define "indecent speech." Hence it seemed to be in direct conflict with the First Amendment.

After this defeat of the CDA, some schools, libraries, and parents turned to code-based solutions. They began adopting various software programs, such as filters and blocking mechanisms, to protect children from explicit pornographic material. This is a prime example of how private parties have sought to legislate their environment through code, instead of relying on the law.

Lessig describes two architectures that control speech: zoning architectures and filtering architectures. There are several sorts of zoning solutions but one that might pass 'constitutional muster' would be based on what Lessig calls a "kids-ID" solution. In this case browsers would enable users to set up profiles, and that profile would include an indication of whether or not the user is a minor (parents would need to complete the profile for their children). The adult profiles on the same machine would be secured by a password, so they could not be accessed by children. Each member of the family would navigate the Web according to the rules of his or her profile. If a "kid-identified" user tries to access a pornographic web site, the minor would be denied access. The benefit of this zoning solution is that "the burden on the child (or, more accurately, the burden on his parents) would be slight, and the burden on the Web site would also be slight" (p. 176).

There are also architectures that filter speech. One such architecture is PICS, which stands for Platform for Internet Content Selection. PICS is a protocol for rating and filtering content on the Net. It divides the task of filtering into two activities: labeling, which involves rating the content of a site, and then filtering the content based on those labels. PICS provides a standard format and supports multiple labeling schemes or rating services. Internet content providers can embed a label within their own Web site or third parties could rate that Web site independently. In either case a common labeling vocabulary is available for use. Users would be free to pick their filtering software and an appropriate rating system. If a user were concerned about pornography the user might choose the rating system of the Christian Coalition and purchase a browser such as Netscape which incorporates a PICS-compatible filter.

Lessig is tolerant of zoning architectures if they are properly implemented, but he has major objections to filtering technology. For Lessig, PICS epitomizes all that is wrong with the constraints imposed by code: "Blocking software is bad enough – but in my view, PICS is the devil" (1997, p. 96). There are a number of problems with PICS. First, it is a universal censorship system, which can be used to censor any kind of material, not just pornography and hate speech. As a result, PICS can be adopted to block access to unpopular political speech or dissenting viewpoints. Also, PICS cannot aspire to neutrality or pure impartiality – to some degree it will always reflect the biases and tendentious opinions of those who are the content labelers. Finally, rating systems of third parties will need constant updating and revision, and hence they will have a difficult time keeping up with the rapid pace of change on the Net.

But the fundamental problem from Lessig's viewpoint is that we are ceding to those who rate content (private industry, public interest groups, etc.) the government's role as an arbiter of speech rights. Companies and computer programmers are making decisions about what Web sites children should see or not see. In addition, filtering, unlike zoning, especially when it happens upstream at the level of an ISP, is often untransparent to the end user.

There is one more problem with filtering architectures: they work too thoroughly and too perfectly. Thanks to PICS, users can filter out vast amounts of online speech and tailor content to their own liking. But, as Lessig remarks, "there is also value in confronting the unfiltered" (p. 180). Broad exposure

to the reality around us makes us well-rounded individuals and more informed citizens. Excessive content filtering is also incompatible with a rich and diverse intellectual culture that most countries seek to foster. These same arguments are echoed in Shapiro (1999) who describes the "ignorance and narrow-mindedness" of the control revolution which is manifest in activities like filtering (p. 107).

Lessig is much more amenable to zoning, which does not yield the same externalities as filtering. This may seem odd since filtering promotes choice, while zoning is a form of censorship, and in the chapter on privacy Lessig has exalted P3P because it facilitates such choice. In his estimation, filtering provides choice but it takes that choice too far, since it enables users to perfectly order and control their environments by allowing them to exclude vast amounts of content. And this exclusivity of content is damaging for the common good. But the zoning solution, which looks like censorship, is more focused since control is in the hands of content providers who will not be prone to excesses since they want as many customers as possible. They will only block those customers when there is a legal requirement to do so such as the mandate to prevent children from getting access to speech that is harmful to minors.

Pornography is not the only form of speech on the internet which users seek to control in some manner. There is also 'spam,' that is, unsolicited commercial e-mail. It surely does not have the same noxious effects as pornography and hate speech but it is a nuisance. Spam also imposes costs on the recipient and on the internet infrastructure. The biggest cost associated with spam is the consumption of computer resources. For example, when someone sends out spam the messages must sit on a disk somewhere, and this means that valuable disk space is being filled with unwanted mail. Also, many users must pay for each message received or for each disk block used. Further, when spam is sent through Internet Service Providers (ISP's) they must bear the costs of delivery. This amounts to wasted network bandwidth and the utilization of system resources such as disk storage space along with the servers and transfer networks involved in the transmission process.

Once again we are faced with a policy question about how to deal with this seemingly intractable problem of spam. Do we turn to the law? Will the invisible hand of the market inevitably correct this market failure by driving spammers out of business? Can norms be helpful? And, of course, there is the option of reverting to code.

The first option is to handle spam through policy, to craft laws at a state or federal level that would put conditions on the transmission of spam or even make it illegal. Some state laws have already been passed that prohibit falsification of the spammers' return address. Falsification helps to thwart those filters that are trying to block messages from known spam addresses. But there are several hurdles. Spam is difficult to define. Is it strictly commercial e-mail or should it include non-commercial bulk mail? Does any nonconsensual commercial e-mail constitute spam? Another hurdle for the legal solution is the problem of regulatory arbitrage – U.S. laws against spam will be difficult to enforce against spammers living in foreign countries.

There is also a more bottoms-up approach to spam. We can allow users and corporations to deal with this nuisance junk mail through code. There is a plethora of programs like Mail Essentials with anti-spam capabilities. This particular program blocks messages by looking to see if the originating domain is on the 'list' of known spammers, and it also scans for certain key words or phrases that indicate the likelihood of spam.

In addition to filtering mechanisms there are also 'black holes' such as Paul Vixie's MAPS (Mail Abuse Prevention System) RBL (Realtime Blackhole List). The MAPS-RBL is a blacklist of internet protocol addresses determined to be spammers. The list is managed and verified by a private organization which is operated by Mr. Vixie. Network providers who subscribe to MAPS-RBL will block e-mail coming from any account on the networks which are on the RBL list. All mail from the blacklisted providers is blocked, not just mail from the accounts known for sending spam.

But once again the use of code by private parties to solve a market failure like spam triggers major questions and concerns. Should this *private* organization have the prerogative to determine whether millions of e-mail messages reach their final destination in cyberspace? Should we tolerate the use of code for this sort of 'vigilantism?' As one might expect by this point, Lessig has strong objections to vigilante solutions like MAPS-RBL. According to Lessig (1998),

> Certainly spam is an issue. But the real problem is that vigilantes and network service providers are deciding fundamental questions about how the Net will work – each group from its own perspective. This is policy making by the 'invisible hand.' It's not that policy is not being made, but that those making the policy are unaccountable . . . This is not how policy should be made. We know this, but we don't know what could replace it.

From Lessig's perspective the problem with these solutions to problematic forms of speech is that we have private individuals and organizations making choices for the rest of us, effectively making unauthorized

policy decisions that will have a tremendous impact on the landscape of the Web.

It is instructive to compare Lessig's different approaches to the problems of privacy and speech. In the case of privacy he argues on behalf of code that would allow users to negotiate the terms for the collection or sharing of their personal data. But he is unequivocally opposed to code-based solutions for speech like filtering. The problem is that unlike code such as P3P, filters regulate too perfectly and this is perilous. This may seem inconsistent but in both cases he is arguing against "centralized structures of choice" (p. 186), and, in the case of filters, against structures that are too individualized and too effective. He wants users to be able to exercise their own free choice about privacy and about speech. Filters often undermine choice, since they tend to be much too exclusive and end up dangerously narrowing the user's perspective, sometimes without his or her awareness. P3P is a more neutral and benign architecture that enhances choice, but a filter is an architecture that usually incorporates someone else's choices about what web sites should be seen or not seen.

Constitutional values

As we have seen, much of this book is devoted to a *descriptive* account about what regulates or constrains us, the four modalities of regulation, i.e., norms, laws, the market and architectures (or code). While most rational beings realize that we need such constraints, those constraints can sometimes be extreme or unjust. For example, they can threaten basic liberties in a significant way if they are the product of repressive sovereigns. This raises a normative question about how a constraint like law should be formulated. How do we assess the validity of these constraints, and how do we determine whether they affirm our basic liberties and further the common good? How can we be sure that they do not assert an arbitrary regulatory power?

Although one does not find a satisfactory answer to this issue in *Code*, Lessig does imply that what is fundamental and directive for the development of law are constitutional values. Lessig describes himself as a *constitutionalist*. He believes that liberty comes from the state and that "we build liberty . . . by setting society upon a certain *constitution*" (p. 5, emphasis in original). The term 'constitution' should not be interpreted in a literal sense. It does not mean a legal document but "an architecture . . . a way of life that structures and constrains social and legal power, to the end of protecting fundamental *values* – principles and ideals that reach beyond the compromises of ordinary politics" (p. 5, emphasis in original). Thus, constitutionalism incorporates certain normative ideals such as the 'rule of law' or due process. For a government to be constitutional there must be some traditional standards, some organizational principles, which are commonly recognized and embraced as fundamental by a given society.

In the United States these 'constitutional values' are expressed in a fundamental legal text, the Bill of Rights to its Constitution. They include free speech, privacy, and due process, values that are central to the legal systems of most democratic governments. This constitution serves to protect citizens against arbitrary or repressive federal and state laws that might undermine these values.

However, applying the Constitution, which was written in 1787, under dynamic and evolving circumstances is not always a straightforward process. It sometimes requires 'translation,' that is, the process whereby the meaning of the Constitution is translated into a new context or applied to new technologies. Lessig cites Justice Brandeis' decision in the 1928 *Olmstead* v. *United States* case. During the period of Prohibition the government had been surreptitiously wiretapping the phones of suspected liquor dealers. There was no physical trespass, so the government's lawyers argued that the 4th Amendment had not been violated. Brandeis recognized that the 4th Amendment applied only to physical trespass but he claimed that it was the Court's responsibility to preserve the meaning of this Amendment in this new context (i.e., telecommunications). Hence he found the government's wiretapping to be in violation of the 4th Amendment. The presumption, then, is that although the founders of the constitution knew nothing about the internet they provided us with a tradition, with a set of values, that could be translated into new domains and contexts.

Translation is one way to deal with the problems presented by cyberspace, but translation isn't always effective. According to Lessig, there are sometimes "latent ambiguities" that impede translation. One such ambiguity concerns the use of filters to selectively control speech. Are these filters consistent with the First Amendment? Cass Sunstein, for example, maintains that the framers of the U. S. Constitution embraced a Madisonian conception of the First Amendment that would preclude the possibility that the variety of speech we see should be a function of individual choice. Others argue that perfect filtering deployed by individuals or by private organizations is not inconsistent with the First Amendment.

In these cases where the Constitutional Amendments are difficult to apply, where translation fails us, choices must be made. Lessig argues that these choices about the values we embed in architectures should be

made through the political process, through collective decision-making. The problem is that there is widespread antipathy to government that is often reflected in inflammatory libertarian rhetoric about the need to keep the Net free of government influence.

Lessig's real concern, then, is twofold: (a) we are disabled from making these choices through the deliberative democratic process of collective decision-making due to our dissatisfaction with government; and (b) since the internet's architectures are private, that is, constructed by corporations and universities, they are outside the scope of constitutional accountability and the jurisdiction of the courts. The constitutional values such as privacy, equality, and anonymous speech do not apply in cyberspace since this is a 'private' place, and the Constitution is concerned with 'state action.' This raises some troubling questions – "is it more faithful to our tradition to allow these structures of control, the functional equivalent of law, to develop outside the scope of constitutional review? Or to extend constitutional review to the structures of private regulation, to preserve those fundamental values within our tradition?" (pp. 217–218)

Lessig has made it abundantly clear throughout this book that we ignore the Constitution's ultimate constraint at our peril, since collective values should be regulating private action. But this does not seem to be the case. Instead, the "courts are disabled, legislatures pathetic, and code untouchable" (p. 221).

From code to ethics

Now that we understand the essentials of Lessig's thesis we must consider how ethics fit into all of this. What role does it play in Lessig's model? While Lessig talks at great length about "norms" and "collective values," there is no explicit mention of ethics or moral values, and no reference to notions with a moral connotation like the 'common good.'

But does ethics, the domain of inquiry that systematically considers issues of right and wrong, have any relevance in this book about law and regulatory structures? A primary theme in *Code* is the different ways in which our behavior is shaped or regulated. Ethical values certainly shape our behavior and constrain us: they hold in check our self-interest since they require one to act with respect for others. Kant, for example, summed up the moral law in his categorical imperative, which precludes arbitrary self-preference in the pursuit of our ends or objectives. It also requires that humanity, my own humanity and those of others, must be respected in every action. Kant (1959) says that this imperative is "the supreme limiting condition in the pursuit of all means" (p. 45), so it clearly regulates our behavior. For Aristotle, on the other hand, ethics is about cultivating *phronesis* or prudence, an ability to judge what is in keeping with the requirements of justice and the good life. A person is not endowed with *phronesis* if she cares only for herself. There must be a sense of concern for others and a sense of measure concerning the public matters of the *polis*. Thus like norms, laws, and code, ethics is prescriptive: it guides and limits our conduct and shapes our basic behavioral patterns.

More recent accounts of ethics tend to focus on one's moral responsibility and 'the moral point of view,' which, according to Goodpaster (1984) has two components: rationality and respect. Rationality implies that one pursues his or her goals with careful attention paid to alternatives, consequences, and the means necessary to achieve a given end. "Respect," according to Goodpaster, "involves consideration of the perspectives of other persons in the pursuit of one's rational projects and purposes." Respect amounts to a "self-imposed restraint on rationality," a recognition that the worth of our projects does not supercede the worth of other human beings (p. 301). It is not uncommon, then, for ethics to be construed as a regulatory force in shaping people's lives, though these 'regulations' are imposed from within because of a sense of duty or obligation.

How then do ethical ideals, the imperatives of justice and respect, fit into Lessig's modalities of regulation? This is hard to determine from the text itself. Actually, one searches in vain for *any* reference to ethics in this book even where one might expect at least an allusion to the categories of right and wrong. For example, in a discussion seeking to illuminate distinctions between these four modalities, Lessig remarks that breaking and entry into someone's house is obviously against the law. He also points out that "norms constrain you as well – it's unneighborly to break into your neighbor's house" (p. 237). Of course, it's not just "unneighborly" to break into someone's house, it's immoral! Lessig has clearly understated the case against trespass. Trespass with the use of force inflicts harm on others and on their property and this violates a moral standard according to any of the traditional moral frameworks. We can and should make a more forceful argument against breaking and entry rather than merely labeling it "unneighborly."

It would appear from this and other passages that ethical standards are somehow bundled together with these conventional norms, one of the four major constraints. Lessig does not precisely define what he means by "norms," but we can infer that they include customs, etiquette, manners, and social conventions. It is not unusual, especially for moral relativists, to regard ethical imperatives on the same level as custom

and social convention. They too are prescriptive and offer guidance for conduct, but their authority is equivalent to the authority of local customs. They are not fixed or reliable standards, since they are relative to a specific social or cultural context.

If, as it appears, Lessig is conflating customs and the rules of cyberspace etiquette with moral standards, he is mistaken. The former are fleeting and culturally conditioned whereas the latter are endowed with permanence and transcendence. This is no place to make a case against moral relativism, but most philosophers who have written about ethics would steadfastly reject any claim that would reduce ethical principles to an extension or mapping of our customs and manners. If there is a common humanity we can deduce that there must be some moral standards we all share. According to Philippa Foot (2001),

> Granted that it is wrong to assume identity of aim between people of different cultures; nevertheless there is a great deal that all men have in common. All need affection, the cooperation of others, a place in the community, and help in trouble. It isn't true to suppose that human beings can flourish without these things – being isolated, despised or embattled, or without courage or hope. We are not therefore simply expressing values that we happen to have if we think of some moral systems as good moral systems and others as bad (pp. 195–196).

Another important reason to insist on the distinction between ethical standards and norms is the need to recognize that true ethical values can sometimes conflict with social norms and mores. They can be at odds with what society thinks, and this leads men and women of moral conviction to sometimes dissent from prevailing beliefs. Lessig associates his norms with the social pressure to conform. Violating social mores brings dishonor and shame and so one feels compelled to moderate their behavior accordingly. We follow *ethical norms*, however, not because of social or peer pressure or because they reflect the current customs, but because our conscience has judged that a particular action is the right thing to do even if it flouts conventional standards. The ethical person acts out of a sense of duty and obligation. Social conventions, such as those that legitimized slavery in the ante-bellum South, sometimes violate basic moral principles.

Given the vital importance and the autonomy of ethical values such as justice and respect for others isn't it erroneous to link these moral ideals with social norms and mores? Shouldn't such values be accorded a different status within the modalities of regulation identified by Lessig?

Lessig's brief discussion of constitutional values may begin to give ethics its due, since it appears that he is providing some sort of higher principle for judging the modalities of regulation. A constitution is all about values for Lessig: "to speak of a constitution is not to describe a one-hundred-day plan. It is instead to identify the values that a space should guarantee" (p. 6). But he does not categorize these values as "moral" ones and hence their origin and legitimacy is not completely clear. He argues that these values developed and protected by the state are "beyond the compromises of politics." But are they rooted in core human goods that are independent of and prior to the state? If there were a country called 'New Oz' that developed a constitutional tradition shunning certain values like personal liberty and due process would there be something fundamentally wrong with its constitution? Do these values transcend cultural differences or are they completely cultural and contextual?

These questions remain largely unanswered here, and perhaps this is due to space and time constraints. Also, in fairness to Professor Lessig, we must keep in mind that this is not a philosophy text and he is not a philosopher, so perhaps we should not expect him to address these lofty issues. Nonetheless, his failure to clarify the nature of these key values and his apparent reluctance to regard them as somehow connected to "moral" principles leaves some unclarity in his otherwise thorough analysis.

This issue about the affinity of the law and constitutions to 'moral values' is an offshoot of a protracted debate between those who embrace the natural law tradition and those who embrace positivism. The former group argues that law is inextricably connected to morality, that a legal rule or doctrine is defective if it does not serve the ends of justice. Positivists, on the other hand, underline the distinction between what is legal and what is just. There is no connection between law and morality – a legal rule is a given, the outcome of a legislative act or a judicial decision, and it may or may not be justified on moral grounds.

Obviously we cannot pursue a discussion of this great debate, but suffice it to say that most traditional moralists would feel more comfortable with the appealing notion that there are core moral goods that should serve as a foundation of all constraints including law, norms, code and even the market. Lessig would agree, I think, that the starting point and the basis for thinking about what regulates human beings is a set of values, because we do need a way to objectively judge those laws and social norms. If they are arbitrary and oppressive and do not promote the common good we know they are deficient. Recall Lessig' major worry: when we look at the trajectory of cyberspace's evolution it is quite likely that "values that we consider fundamental will not necessarily

remain; freedoms that were foundational will slowly disappear" (p. 6).

I prefer to regard those "values" as moral ones and as independent of a specific constitutional tradition within a particular society. To be sure, we need the state and constitutional traditions to realize and fully protect those values, but a constitution that does not recognize or safeguard fundamental freedoms, security, due process, etc., would be seriously defective and its notion of fundamental human rights impoverished. There are principles of justice reflecting the absolute rights of humans that can never be overridden, and these norms and rights must be the foundation of any legitimate constitution. If this is what Lessig means by constitutional values, we are in complete agreement.

How might we define these fundamental values? Phillipa Foot gave us some inkling about how to proceed. Also, Jim Moor identifies a set of core values (or core goods), which are shared by the vast majority of human beings. These values include life (avoidance of pain and death), happiness, ability, freedom, knowledge, resources, and security. According to Moor (2001), "these values are articulated in different ways in different cultures but all cultures place importance on these values to some extent . . . No culture or individual human could continue to exist and disregard the core values entirely" (p. 46). In order to behave ethically we must not allow opportunism to dominate decision-making, and we must reason from principles grounded in these core goods that affirm integrity and fellowship.

In my estimation we need to revise Lessig's model into a hierarchy that gives a privileged position to these core moral values. These values alone provide the necessary framework for assessing the efficacy of the constraints proposed by Lessig. They help us judge the adequacy of specific laws and policies along with the suitability of different cultural norms. They also suggest which values should be embedded in the code we develop. If cyberspace becomes a place where freedom is limited and where our security and privacy is threatened by the invisible hand and the architectures of control, this would be a dreadful turn of events since basic core goods are not being respected. How then should we prevent this from happening?

Preserving moral values in cyberspace

As we mentioned earlier, Lessig regards commercial forces as the main culprit in this transformation of cyberspace from an architecture of freedom to one of control. For example, he writes that "market forces encourage architectures of identity to facilitate online commerce . . . If anything is certain, it is that an architecture of identity will develop on the Net – and thereby fundamentally transform its regulability" (p. 58).

However, Lessig is making some critical assumptions here that need more careful scrutiny. He assumes, for instance, that business is a monolithic movement orchestrating the development of a uniform code that will put a stranglehold on cyberspace in order to promote commercial activity. But will commercial institutions really act in concert in cyberspace? The plausibility of the position that they will is certainly open to some question.

Consider Lessig's analysis of trusted systems, which provide protection for online intellectual property such as music and books. These literary works are encrypted and made available only to paying customers. Proponents of copyright management systems contend that they are necessary for the enforcement of copyright laws in cyberspace. But these systems threaten 'fair use,' that is, the right to quote a few lines from a book or to reproduce them in a critical article. It is unclear whether such systems can be designed and coded in a way that preserves fair use. According to Lessig:

> But what happens when code protects the interests now protected by copyright law? . . . Should we expect that any of the limits will remain? Should we expect code to mirror the limits that the law imposes? Fair use? Limited term? Would private code build these 'bugs' into its protections? The point should be obvious: when intellectual property is protected by code, nothing requires that the same balance be struck. Nothing requires the owner to grant the right of fair use . . . Fair use becomes subject to private gain (p. 135).

But is it really inevitable and self-evident that *all* developers and users of trusted systems will eviscerate fair use? Isn't there a chance this value will be preserved in some version of a trusted system? Doesn't Lessig's prediction seem too pessimistic about humanity's capacity for practical moral reasoning?

My point is that some authors and some developers of trusted systems will realize that there are moral issues at stake here and they will work to preserve fair use or its equivalent in their systems. When Lessig says so emphatically that "*nothing requires* . . ." he overlooks the role of conscience and morality in making these decisions about justifiable limits on copyright protection. If a convincing moral case can be made that authors should respect fair use because of what it contributes to the intellectual commons and the common good, then there will be a moral imperative to honor the fair use requirement, regardless of what

the code allows us to do. *Some* people will feel obliged to respect values like fair use, and so they will make the proper choice and act accordingly. In addition, the market is not completely moribund in all of this. Online book dealers who provide fair use and the ability to browse will most likely be rewarded with customers. Thus, it is likely that for several reasons there will be trusted systems incorporating fair use, assuming its technical feasibility. It is not a foregone conclusion that fair use will be systematically excluded from all trusted systems code by a monolithic commercial force. If there are heterogeneous and diverse architectures, there is a reasonable chance that some of them will respect the collective value of fair use. Private choices are not always motivated by pure self-interest. Why not give corporate conscience and the free market a chance before rushing in with premature regulations?

This discussion on the voluntary preservation of fair use raises a larger question – is it even remotely possible that instead of relying so heavily on the political process, on laws and regulations, to protect important values, we can rely at least to some extent on ethical behavior and responsible conduct? Lessig is pessimistic about this, and he dismisses the possibility of some level of ethical self-regulation or responsible self-organizing in cyberspace. But is he being too presumptive about the need for more laws and government involvement? Is ethical self-regulation a better prescription for resolving certain social issues in cyberspace rather than relying so extensively on political solutions?

Unlike the libertarians, I recognize that some of the more formidable market failures identified by Lessig (such as privacy erosion in certain sectors) will need to be resolved through the deliberative democratic process. On the other hand, it just might be possible to handle other problems, like spam and pornography, through bottoms up regulation. Why this hesitancy on my part to rely exclusively on the law and regulatory infrastructure? Consider why citizens are so disenchanted with government and the political process in the first place – they feel powerless in the face of a highly centralized political bureaucracy. As Taylor (1992) remarks, "the operation of the market and the bureaucratic state . . . favor an atomist and instrumentalist stance to the world and to others" (p. 111). The more we regulate and create necessary enforcement mechanisms for those regulations, the more dominant and burdensome that bureaucracy becomes. Bureaucracies tend to concentrate power as they extend their control. This makes people even more alienated from the public sphere, and it reinforces those feelings of impotence that contributes to political paralysis. We surely cannot abolish government's regulatory role in cyberspace, but we should avoid excessive regulation and give the Net's stakeholders a chance to responsibly correct some of the Net's market failures so long as they have the tools to accomplish such a task.

This last point brings us back to the most effective tool, which is code. Lessig's book helps us appreciate that "code" greatly expands the possibilities for such effective self-regulation. Thanks to raw materials like filters, tags, firewalls, encryption software, and so forth, code-based regulations are a feasible alternative in some cases to top-down controls. Knowledgeable users can effectively organize their own environments with less need for the government's public policies. But, as Lessig's arguments have demonstrated, code is a two edged sword – thanks to code the possibility of self-regulation is greatly enhanced but so are the dangers like the risk of a myopic perspective through excessive filtering or other types of collateral damage.

There are some legal scholars who share this view. Professor Post (2001) has taken a similar stance and has argued "against dismissing too quickly the notion that there are some problems that are best solved by these messy, disordered, semi-chaotic, unplanned, decentralized systems . . ." (p. 141). Discussions on the suitability of self-regulation, however, overlook the ethical dimension of this activity, and this is unfortunate. It is possible to have some degree of measure and order on the Net through decentralized controls and self-regulation as long as these 'regulatory' activities give primacy to the virtues of prudence and justice. *Ethical self-regulation* links rational self interest with the moral point of view which positively regards the wants, needs, interests, and concerns of others.

There are several levels involved in such a decentralized scheme of ethical self-regulation. First, users and organizations who frequent cyberspace must exercise proper self-restraint. As moral agents initiating transactions and interacting in cyberspace, they must abide by commonly accepted moral principles and respect the interests and rights of others even when the relevant law is inchoate or ambiguous. For example, while it may be legal to transmit spam, that is, unsolicited automated e-mail, there is certainly a compelling moral imperative against doing so. Spamming, or similar activities that violate the spirit of cooperative interaction on the Net, is a prime example of opportunistic behavior based on one's narrow self-interest instead of the wider interests of the internet community. There will of course be moral disagreements about some situations, but if users adopt the moral point of view and act conscientiously and with impartiality, moral judgements will tend to converge in most cases.

Of course there will always be those who do not comply with the Net's ethical standards. Thus, ethical self-regulation also entails protecting or shielding one's environment from the anti-social and disruptive activities of others. This includes activities like using filters to protect children from pornographic or virulent hate speech Web sites, deflecting unwanted junk mail, or safeguarding one's privacy upon a visit to a commercial Web site. In these transactions internet stakeholders are on the defensive seeking to limit the ability of irresponsible moral agents to inflict harm. But even in these defensive transactions they must behave with prudence and responsibility. They must seek to avoid or at least minimize the collateral damage that can sometimes accompany code-based solutions designed to handle externalities (such as filtering pornography or blocking out junk e-mail.) This will often involve choosing the optimum architecture and implementing it responsibly. We must encourage ethical vigilance for how some types of code designed to protect one's environment may produce negative effects and possibly infringe on the rights of others. If code is law, it would seem to follow that it must be applied with the same care, publicity, and fairness as the law itself.

Finally, it would also seem to follow that software developers, ISP's, and others who function as gateways to the internet have a special obligation. They write the code that regulates the Net and they set the rules of access. They are shaping the internet's future architecture and are obligated to do so in a way that is attentive to core moral values. If self-regulation is to work effectively, 'code writers' must aspire to greater accountability for their work along with the *moral competence* to write code as carefully as lawmakers formulate and execute laws. This means, for example, that code should be as open and transparent as possible so that the user's autonomy and capacity for informed consent is fully respected. Also, code should be written so that it preserves traditional social and moral values such as anonymous free speech or 'fair use' of copyright material.

The feasibility of ethical self-regulation is enhanced by the user's ability to rely on code to counter some externalities and to protect his or her environment from the intrusions of others. Code should not be a surrogate for conscience, but code can support self-regulation when it is deployed in a conscientious and prudent manner to protect rights such as privacy or to constrain the anti-social behavior of others.

Law, markets, and morals

In the sphere of business ethics there has been a lively debate about the viability of corporate self-regulation. Some scholars have argued passionately that there must be a tight net of laws and nuanced regulations to restrain business and protect unwary consumers. An elaborate regulatory infrastructure is the key to protecting the physical environment and safeguarding human rights in the workplace. Others, like Milton Friedman, following the lead of Adam Smith, have argued that the market itself could impose restraints on corporate ambitions. The market has a way of insisting upon responsiveness to consumer demands and thereby purifying self-interest. As a result, there is at least a minimal level of morality built into the economic system itself. After all, if a business deceives its customers, tramples on privacy rights, or sells unsafe products, it will be punished in the marketplace.

Both of these solutions, however, have glaring deficiencies. The law is not a panacea for solving market failures and imperfections. Frequently, individuals and corporations which depend too heavily on the law to guide their behavior are left floundering when there are 'policy vacuums' or legal ambiguities. Following the law represents an externalization of moral judgement instead of its independent exercise. The law must obviously be respected but this does not preclude making an independent moral assessment about a situation. For example, the law in some countries, like the United States, currently allows employers to read and monitor the e-mail of their employees; but that doesn't mean that such a practice should be blindly accepted. Given the moral significance of privacy in the workplace, executives should carefully weigh the moral arguments for and against such monitoring before making a decision. The law is also reactive and slow especially in the face of rapidly changing technologies. It is often incomplete and vague, formulated quickly to 'fix' a problem of public concern. For evidence of this we need only consider the hastily crafted and imprecise Communications Decency Act. As Stone (1975) writes, the solution to this vagueness is more precision, "but once we have unleashed the regulators to make finer and finer regulations, the regulations become and end in themselves, a cumbersome, frustrating and pointless web for those they entangle" (p. 110).

Similarly, the history of corporate America has demonstrated that a hyper-competitive marketplace does not include the necessary mechanisms for compelling organizations to focus their attention on moral issues. To be sure, there are market pressures for companies to avoid significant ethical lapses and

untoward behavior. But as Goodpaster (1984) writes, "the pressures on the other side are also significant, pressures for single-minded pursuit of profits and even for relatively short-term gains that run rough-shod over moral convictions" (p. 316).

Moreover, if we extend the above argument to include the other elements in Lessig's model, such as code and norms, we will see that they too are inferior to responsible moral conduct. If code is impersonal and 'untouchable,' beyond the pale of legal and social constraints, and if it is in the hands of amoral developers and corporations, there is nothing to ensure that the proper constitutional or moral values are embedded in that code. And norms (excluding ethical norms) are fleeting and unreliable, subject to the whims and caprices of a sometimes fickle Net community. We need some sort of moral authority beyond code and beyond social conventions.

Thus, while the law, the market, social norms and code have definite roles to play in regulating behavior, the ultimate regulator should be ethical standards conscientiously applied to our actions and policies. There is no substitute and no better 'regulator' than the *moral point of view* with its attention to the needs and concerns of others. There are clear benefits to a greater dependence on reflective morality than on an unreflective obedience to law, a misguided faith in the turbulent marketplace, an adherence to social norms based on peer pressure, or the untrammeled use of code.

If we begin to take the process of moral reasoning and education more seriously, ethical self-regulation and decentralized controls may have a chance of working. They may solve some of the Net's more vexing social problems and help to keep it less cluttered by burdensome rules and regulations. If we can educate software developers and others about the parameters of responsible code development, it might be possible to regulate cyberspace with the help of carefully formulated and executed code, such as trusted systems that protect copyright but preserve fair use.

We can infer from Lessig's book that the author would not put much faith in the potential for ethical self-regulation. He seems to prefer the coercive authority of the state to ensure that cyberspace incorporates architectures which will allow liberty to flourish. He has argued here that unless the courts are willing to extend their jurisdiction to 'private' architectures, and unless our legislators begin regulating the Net by making 'hard choices,' architectural constraints on the Net will tend to swallow up cherished values.

I concede that Professor Lessig may possibly be right about certain issues presented here, such as the need for the government's more visible hand in the affairs of cyberspace. But his deterministic viewpoint and his casual treatment of ethical norms lead him to overlook some other tenable options for how the Net can be governed.

References

J. Boyle. Foucault in Cyberspace: Surveillance, Sovereignty and Hardwired Censors. *University of Cincinnati law Review*, 66: 177, 1997.

P. Foot. Moral Relativism. In T. Carson and P. Moser, editors, *Moral Relativism: A Reader*. Oxford University Press, New York, 2001.

L. Fuller. *The Morality of Law*. Yale University Press, New Haven, 1969.

K. Goodpaster. The Concept of Corporate Responsibility. In T. Regan, editor, *New Introductory Essays in Business Ethics*. Random House, New York, 1984.

I. Kant. *Foundations of the Metaphysics of Morals*, L. Beck, trans. Liberal Arts Press, New York, 1959.

E. Katsh. Software Worlds and the First Amendment: Virtual Doorkeepers in Cyberspace. *University of Chicago Legal Forum*, 35: 338, 1996.

D. Hamilton. Web's Design Hinders Goals of User Privacy. *The Wall Street Journal*, April 3, 2000.

L. Lessig. Tyranny in the Infrastructure. *Wired*, 5(7), July, 1997.

L. Lessig. The Laws of Cyberspace. In R. Spinello and H. Tavani, editors, *Readings in Cyberethics*. Jones & Bartlett, Sudbury, MA, 2001.

L. Lessig. The Spam Wars. *The Industry Standard*, December 31, 1998.

L. Lessig. *Code and other Laws of Cyberspace*. Basic Books, New York, 1999.

W. Mitchell. *City of Bits: Space, Place and the Infobahn*. MIT Press, Cambridge, MA, 1995.

J. Moor. Reason, Relativity, and Responsibility in Computer Ethics. In R. Spinello and H. Tavani, editors, *Readings in Cyberethics*. Jones & Bartlett, Sudbury, MA, 2001.

J. Post. Of Black Holes and Decentralized Law-Making in Cyberspace In R. Spinello and H. Tavani, editors, *Readings in Cyberethics*. Jones & Bartlett, Sudbury, MA, 2001.

J. Reidenberg. Lex Informatica: The Formulation of Information Policy Rules Through Technology. *Texas Law Review*, 76: 553, 1998.

J. Rosen. *The Unwanted Gaze: The Destruction of Privacy in America*. Random House, New York, 2000.

A. Shapiro. *The Control Revolution*. Century Foundation Books, New York, 1999.

C. Stone. *Where the Law Ends: The Social Control of Corporate Behavior*. Harper & Row, New York, 1975.

C. Taylor. *Ethics and Authenticity*. Harvard University Press, Cambridge, MA, 1992.