The Future of eCommerce

*What is the "law of electronic commerce"?*

In this final class, we'll reflect a bit upon the nature of the "law of electronic commerce." What "is" the law of eCommerce? Who makes such a law? (And, should they?)

Read the following short pieces:


Lawrence Lessig, *Code and Other Laws of Cyberspace* (2001) (*Conclusion*)


---

**Notes & Questions**

1. Who's right? How should eCommerce be regulated? Not at all? Minimally? Substantially?

2. Is Easterbrook right about the "Law of the Horse"? Did we learn anything about the law in this class?

3. What does our view of the "law of eCommerce" imply for

Thanks for a great semester, and best of luck with your exams!

COPYRIGHT © 2001 R. POLK WAGNER.
When he was dean of this law school, Gerhard Casper was proud that the University of Chicago did not offer a course in "The Law of the Horse." He did not mean by this that Illinois specializes in grain rather than livestock. His point, rather, was that "Law and . . . " courses should be limited to subjects that could illuminate the entire law. Instead of offering courses suited to dilettantes, the University of Chicago offered courses in Law and Economics, and Law and Literature, taught by people who could be appointed to the world's top economics and literature departments--even win the Nobel Prize in economics, as Ronald Coase has done.

I regret to report that no one at this Symposium is going to win a Nobel Prize any time soon for advances in computer science. We are at risk of multidisciplinary dilettantism, or, as one of my mentors called it, the cross-sterilization of ideas. Put together two fields about which you know little and get the worst of both worlds. Well, let me be modest. I am at risk of dilettantism, and I suspect that I am not alone. Beliefs lawyers hold about computers, and predictions they make about new technology, are highly likely to be false. This should make us hesitate to prescribe legal adaptations for cyberspace. The blind are not good trailblazers.

Dean Casper's remark had a second meaning--that the best way to learn the law applicable to specialized endeavors is to study general rules. Lots of cases deal with sales of horses; others deal with people kicked by horses; still more deal with the licensing and racing of horses, or with the care veterinarians give to horses, or with prizes at horse shows. Any effort to collect these strands into a course on "The Law of the Horse" is doomed to be shallow and to miss unifying principles. Teaching 100 percent of the cases on people kicked by horses will not convey the law of torts very well. Far better for most students--better, even, for those who plan to go into the horse trade--to take courses in property, torts, commercial transactions, and the like, adding to the diet of horse cases a smattering of transactions in cucumbers, cats, coal, and cribs. Only by putting the law of the horse in the context of broader rules about commercial endeavors could one really understand the law about horses.

Now you can see the meaning of my title. When asked to talk about "Property in Cyberspace," my immediate reaction was, "Isn't this just the law of the horse?" I don't know much about cyberspace; what I do know will be outdated in five years (if not five months!); and my predictions about the direction of change are worthless, making any effort to tailor the law to the subject futile. And if I did know something about computer networks, all I could do in discussing "Property in Cyberspace" would be to isolate the subject from the rest of the law of intellectual property, making the assessment weaker.

This leads directly to my principal conclusion: Develop a sound law of intellectual property, then apply it to computer networks. Problem: we do not know whether many features of existing law are optimal. Why seventeen years for patents, a lifetime plus some for copyrights, and forever for trademarks? Should these rights be strengthened or weakened? Why does copyright have the particular form it does? What sense can one make of the fuzzball factors for fair use? How can one make these rights more precise, and therefore facilitate Coasean bargains? Until we have answers to these questions, we cannot issue prescriptions for applications to computer networks.

Cyberspace reduces the effective cost of copying. This continues a trend that began when Gutenberg invented movable type and gave rise to political demand for what has become copyright law. Yet how can we tackle the question whether copying has become too easy, and therefore should be met by countervailing changes, when we have not solved the problems posed by yesterday's technology? Consider the plain-paper photocopier. People can run off scholarly articles. To what extent may researchers copy articles from increasingly expensive journals to create a stockpile for their own future endeavors? This is a question about fair use; yet the fair-use criteria are so ambulatory that no one can give a general answer.

Just recently the Second Circuit held that copying for research within a for-profit corporation exceeded the bounds of fair use. The panel was divided; another circuit is to the contrary, and the Supreme Court split 4 to 4 when

*208*
reviewing that decision. n4 Both opinions leave the impression that a dime's worth of difference in the facts would alter the outcome. Lack of certainty in the property right makes protection of intellectual property all but impossible.

The Copyright Clearance Center barely raises enough money to cover the costs of its operations. When you copy something with a CCC slug line at the bottom, which directs you to remit 50<cents> per page to a particular account number, do you do it? No, you don't, because the extent of the fair-use privilege is so hard to grasp, and because remitting would be such a bother--do you tape two quarters to a post card and mail it?

When property rights are poorly specified, it is hard to transact about them, and correspondingly hard to promote the process of transaction that allocates resources to their highest valued uses. Instead we see second-best moves. Illustration: the price of academic journals has gone through the roof. Library subscriptions often exceed $500 per year; for some scientific or medical journals, the price exceeds $2,000. This high price is an advance fee for photocopying, and it may be that this way the authors (and publishers) get total revenues as high as they would collect if they could charge for reprints, or if they sold more journals at lower prices. n5 The high-price-journal, cheap-copy approach not only cuts the costs of transactions (no one has to collect or remit copy fees), but also cuts the marginal cost of using intellectual property. Because intellectual property can be used without being used up, the ideal pricing mechanism is a flat fee, with no marginal cost for use.

The blanket license for the right to play music approximates this ideal two-part price. But the blanket license works because [*210] the rights for public performance of music are very well specified. Not so for copying articles.

The high subscription fee for libraries does poorly at one of the critical ingredients of the blanket license: price discrimination. ASCAP and BMI charge by a radio station's revenues, or a licensee's gross receipts. The University of Chicago pays more for its ASCAP license than does Swarthmore College. But the Journal of Financial Economics demands the same $750 per year from Goldman Sachs, a business school, or a law school; it cannot discriminate as effectively as ASCAP does. So Goldman Sachs pays too little for the value received, and the University of Chicago Law School has just dropped its subscription. The pricing mechanism has not worked well, because of the difficulties in defining the property rights.

If we are so far behind in matching law to a well-understood technology such as photocopiers--if we have not even managed to create well-defined property rights so that people can adapt their own conduct to maximize total wealth--what chance do we have for a technology such as computers that is mutating faster than the virus in The Andromeda Strain?

Well, then, what can we do? By and large, nothing. If you don't know what is best, let people make their own arrangements.

Next after nothing is: keep doing what you have been doing. Most behavior in cyberspace is easy to classify under current property principles. What people freely make available is freely copyable. When people attach strings, they must be respected, and the tough question when someone copies commercial software will be whether the person making copies is a direct infringer or only a contributory infringer, and whether the remedy should be civil damages or time in prison. Lower costs of copying may make violations of the law more attractive, which suggests the allocation of additional prosecutorial resources, but movement along a cost continuum does not call for change in legal substance.

What else is there to do? I offer three themes.

1. Make rules clearer, to promote bargains. "We" don't know what is best, but in a Coasean world the affected parties will by their actions establish what is best.

The federal government's Working Group on Intellectual Property Rights recently issued a report called Intellectual Property and the National Information Infrastructure. In addition to the pompous title and the standard drumbeat of calls for more [*211] studies, this report contains a few concrete proposals. One, which I gather is controversial, is to amend the Copyright Act to beef up the distribution right. n6 The Working Group recommends that the law recognize that dissemination of copyrighted works via electronic transmission is one of the rights the copyright proprietor possesses.

One may say in response that this change gives too much to the copyright proprietor or restricts unduly the ability to disseminate works. Some people believe that copyright proprietors should be delighted to have a throng willing to transmit their works to consumers who will pay royalties for them (as a recipient clearly must do--for they get a copy whether or not a transmission is a "distribution" of the work). Perhaps so; but if this is so, the author or owner will
permit the transmission, just as song writers license the transmission of their works over the radio to people who may choose to turn on their tape recorders. An author could give this permission at large, while retaining the right to charge for the keeping of copies.

Simply put, it is awfully hard to know what the optimal compensation package for authors is, unless the property rights are clear. If something about the nature of cyberspace has made application of the distribution right cloudy, then by all means clear it up again, so that people may make their own arrangements. And on balance it is best to give these rights to authors. Why? Because if the best arrangement turns out to be free distribution, then private transactions may produce this result when the statute assigns the rights to authors; but if the best arrangement turns out to be some fee for distribution and a lower price for copying, it is extremely hard to reach this state of affairs if the statute cancels the distribution right. Private transactions could shift the right back to authors only if the parties have contractual relations (for example, patrons of the opera may agree not to tape the performances). We must bear in mind the high possibility of error in the original specification of entitlements--a risk especially high in a legislative world dominated by interest-group politics. (The copy law contains a special provision for agricultural fairs and exhibitions, still another allusion to the law of the horse!) The risk of error should lead to initial assignments that are easy to reverse, so that people may find their own way with the least interference. [*212]

2. Create property rights, where now there are none--again to make bargains possible.

Property rights in domain names is an example of what I have in mind. Until recently, domain names on the Internet were assigned by the government (rather, by a firm under contract to do the government's bidding). Allocation was first-come, first-served, with no effort to purge unused names. That led to people storing up domain names. Intellectual-property law rightly has been hostile to such maneuvers. Domain names have some of the attributes of trademarks; but one can't get a trademark by just filing. A firm must use a mark to obtain rights in it; must use the mark continuously; and once this occurs, latecomers stand behind it in line. Similarly, corporate names are registered with the states, and new arrivals cannot duplicate existing names.

The allocation of domain names is now in private hands, and the $50 annual fee will abate the snatch-and-grab incentive to a limited degree. But the allocation of names remains first-come, first-served, with the result that people lay claims to famous corporate and political names. Today you can point your browser to www.clinton96.org and find, not the home page for the Clinton reelection campaign, but a satire of that campaign, with a big picture of the President holding up one finger and a caption claiming that he has a single accomplishment--election. Dick Tuck has come to cyberspace. This is nonpartisan harassment: www.dole96.org also is a satire page.

Property rights need to be better specified than that. Appropriation of names and trademarks would not be tolerated in the rest of the commercial or political world; why so for Internet addresses? In other words, we need to bring the Internet into the world of property law. I grant that, with search facilities, you can find the American Broadcasting Corporation even if someone else has www.abc.com. Nodes are in the end numbers, and conversion to letters is arbitrary. But the search process is costly and can be avoided by correct allocation in the first place.

By "correct" allocation I certainly do not mean allocation according to some government formula. We have tried that approach with broadcast licenses, and it has failed. Indeed, even in the world of over-the-air communications, the Federal Communications Commission has moved in the direction Ronald Coase and Leo Herzel pointed in the 1950s: sell frequencies at auctions. n7 So [*213] it can be with domain names. Let people bid for symbols, then sell them in a developed aftermarket. Perhaps initial allocations could be made by corporate names or product trademarks. Details are far less important than the principle that it is important to establish property rights, without which welfare-increasing bargains cannot occur.

That the Internet spans the world means some difficulty in defining property rights in names; many jurisdictions may have different ideas about optimal allocations. But the telephone system spans many legal regimes without duplication of numbers. International disagreements about patent or copyright laws are much more complex than those necessary to establish domain names.

Some other nations are jittery about the fact that no one owns or runs the Internet; it is a web of little, autonomous nets. But no one can regulate the whole process of information exchange, and even those who hate the idea of free communication have little choice but to join on the terms the participants are willing to accept. China must follow the international consensus if it wants access to other nodes.

3. Create bargaining institutions.
Computers offer many opportunities to do, at next to no cost, the sort of thing the Copyright Clearance Center has tried and failed to do for photocopies. Consider, for example, the question whether a publisher of content on the Internet wants to authorize the making of copies and, if so, the making of copies that can be recopied, or a single copy for use on a local computer. Or does the publisher only want to authorize viewing on screen? All are logical possibilities, each rational for some authors, or for any given author at different times. How is it possible to specify which is which, and to collect payment?--especially in a world where Netscape Navigator is making cache copies behind everyone's back and turning all of you into persistent infringers!

The answer, it seems to me, is a convention--a protocol under which each file contains its own instructions on this question, and programs know how to interpret them. You are familiar with such conventions. When your modem calls a remote modem, the two devices engage in elaborate interrogation to discover what speed to use and what compression and error-correction algorithms are in place. An international standards-setting organization agreed on the language; private firms all over the world [*214] have decided whether, and to what extent, to use this agreed language for communications. Some firms have come up with their own extensions, outside the organization's framework. Encryption technology is similar. You may notice that when Netscape enters a particular corner of the web, a solid key appears in the lower left of the screen; this shows that the client and the server have agreed on an encryption protocol, securing the session.

There are several available protocols. n8 So can it be with copying. A standards-setting organization could prescribe, say, twenty different copying rules--sets of permission and payment terms. There could be competing organizations, with their own standards. Each Internet server and client would understand these terms and carry out the negotiation automatically, remitting any payment to an agreed depository by secure methods.

In raising this possibility, I have in mind still a third meaning of the Law of the Horse. Gerhard Casper did not originate that phrase. It comes from Karl Llewellyn. When he was beginning the project that led to the Uniform Commercial Code, he contrasted the rules for trade between merchants with the rules for idiosyncratic transactions between amateurs, which he called the law of the horse. n9 Why hitch professionals to a wagon designed for amateurs? Llewellyn's idea, realized in the UCC, was to give merchants a menu of options from which they could choose at low cost. One option would be the presumptive rule, applied unless the merchants said otherwise.

The Working Group expresses some concern that courts would balk at enforcing such "contracts of adhesion," n10 but recent cases show that the concern is unjustified. n11 There is no reason to distinguish contract terms from any other aspect of a product's composition. A buyer of a computer does not control the quality of the circuits; the seller arranges both product attributes and contract terms. Just as no one would think of saying that the buyer of a computer with a 500 MB disk really is "entitled" to a [*215] 750 MB disk, or a faster disk, on the ground that disk size and speed is a "contract of adhesion," so it is foolish to complain about contract terms. These all are mediated by price. "Better" terms (as buyers see things) support higher prices, and sellers have as much reason to offer the terms consumers prefer (that is, the terms that consumers find cost-justified) as to offer any other ingredient of their products. It is essential to enforce these terms if markets are to work.

Repeated transactions in thick markets. That's what copying is on computer networks. Just as computers lower the cost of copying, so they expand the size and thickness of the market, and lower the cost of transacting in intellectual property, for both negotiation and payment can be done automatically once authors and users decide what terms they will accept. People tend to emphasize the effect on copying costs and disregard the effects on the size of the market and the costs of transactions; yet just as lower costs of copying pose a challenge to authors, the lower costs of transacting may represent the solution. Computers now match all trades on the London Stock Exchange; they can match trades in a virtual intellectual-property auction place. Work is under way to revise Article 2 of the UCC to supply more standard, off-the-rack rules for computer software. n12 I trust that the authors will resist the temptation to limit the range of allowable choices, rather than to write a menu containing the most popular morsels. The plan can be extended to intellectual property, either by listing options in the statute or through a private standards-setting effort.

To make this work, the author's instructions about dissemination and payment must remain with the copy. The Working Group recommends a new statute to prevent tampering with copyright protection and management systems. n13 This proposal may or may not be right in the details, but it is not clear to me that any change is necessary. Excising any part of the intellectual property likely creates a derivative work, which itself is a subject of control under current law. This is not the time or place to get into details, however.

A quick summary: Error in legislation is common, and never more so than when the technology is galloping forward. Let us not struggle to match an imperfect legal system to an evolving world that we understand poorly. Let us
instead do what is essential to permit the participants in this evolving world to make their own decisions. That means three things: make rules clear; create property rights where now there are none; and facilitate the formation of bargaining institutions. Then let the world of cyberspace evolve as it will, and enjoy the benefits.

FOOTNOTES:

n1 "One finds more than a few courses in law schools entitled 'Law and ' in which the blank is indeed intellectually blank." Michael Tonry and Norval Morris, Retirement of Sheldon Messinger, 80 Cal L Rev 310 (1992).


n4 Williams & Wilkins Co. v United States, 487 F2d 1345 (Ct Cl 1973), aff'd by an equally divided Court, 420 US 376 (1975).


n8 The process can be automatic and secure. Netscape's security methods are simple compared with those used at MIT, which, despite the greatest concentration of bright hackers on the planet, has never had a security breach. See Jeffrey I. Schiller, Secure Distributed Computing, 271 Scientific American 66 (Nov 1994).

n9 Karl N. Llewellyn, Across Sales on Horseback, 52 Harv L Rev 725, 735, 737 (1939); Karl N. Llewellyn, The First Struggle to Unhorse Sales, 52 Harv L Rev 873 (1939).

n10 See, for example, Working Group Report at 49-50 (cited in note 6).


n12 See Working Group Report at 53 (cited in note 6).

n13 Id at 212-213 (analysis), App I 5-12 (draft legislation).
In the spring of 1996, at an annual conference organized under the name “Computers, Freedom, and Privacy” (CFP), two science-fiction writers told stories about cyberspace’s future. Vernor Vinge spoke about “ubiquitous law enforcement,” made possible by “fine-grained distributed systems”; through computer chips linked by the Net to every part of social life, a portion would be dedicated to the government’s use. This architecture was already being built—it was the Internet—and technologists were already describing its extensions. As this network of control became woven into every part of social life, it would be just a matter of time, Vinge threatened, before government claimed its fair share of control. Each new generation of code would increase this power of government. The future would be a world of perfect regulation, and the architecture of distributed computing—the Internet and its attachments—would make that possible.

Tom Maddox followed Vinge. His vision was very similar, though the source of control, different. The government’s power would not come just from chips. The real source of power, Maddox argued, was an alliance between government and commerce. Commerce, like government, fares better in a better regulated world. Property is more secure, data are more easily captured, and disruption is less of a risk. The future would be a pact between these two forces of social order.

Code and commerce.

When these two authors spoke, the future they described was not yet present. Cyberspace was increasingly everywhere, but it was hard to imagine it tamed to serve the ends of government. And commerce was certainly interested, though credit card companies were still warning customers to stay far away from the Net. The Net was an exploding social space of something. But it was hard to see it as an exploding space of social control.

I didn’t see either speech. I listened to them through my computer, three years after they spoke. Their words had been recorded; they now sit archived on a server at MIT. It takes a second to tune in and launch the replay of their speeches about a perfectly ordered network of control. The very act of listening to these lectures given several years before—served on a reliable and indexed platform that no doubt recorded the fact that I had listened, across high-speed, commercial Internet lines that feed my apartment both the Net and ABC News—confirmed something of
their account. One can hear in the audience’s reaction a recognition both that these authors were talking fiction—they were science-fiction writers, after all—and that the fiction they spoke terrified.

Three years later it is no longer fiction. It is not hard to understand how the Net could become the perfect space of regulation or how commerce would play a role in that regulation. The current battle over MP3—a technology for compressing audio files for simple distribution across the Net—is a perfect example. Last year MP3 was quite the rage: CDs were copied and e-mailed, and web sites were built with thousands of songs archived and ready for anyone to take. “Free music” joined the list of free stuff that the Internet would serve.

But this year the story has changed. The recording industry is pushing a standard that would make it easier to control the distribution of these files; Congress has passed a statute that makes it a felony to produce software that evades this control; and one company that produces Sony Walkman-like machines to play MP3 files has already announced plans to enable its machine to comply with these standards of control. Control will be coded, by commerce, with the backing of the government.

Vinge and Maddox were first-generation theorists of cyberspace. They could tell their stories about perfect control because they lived in a world that couldn’t be controlled. They could connect with their audience because it too wanted to resist the future they described. Envisioning this impossible world was sport.

Now the impossible has been made real. Much of the control in Vinge’s and Maddox’s stories that struck many of their listeners as Orwellian now seems quite reasonable. It is possible to imagine the system of perfect regulation that Vinge described, and many even like what they see. It is inevitable that an increasingly large part of the Internet will be fed by commerce, and most don’t see anything wrong with that either. Indeed, we live in a time (again) when it is commonplace to say: let business take care of things. Let business self-regulate the Net. Net commerce is now the hero.

This book continues Vinge’s and Maddox’s stories. I share their view of the Net’s future; much of this book is about the expanding architecture of regulation that the Internet will become. But I don’t share the complacency of the self-congratulatory cheers
echoing in the background of that 1996 recording. It was obvious in 1996 who “the enemy” was; now nothing is obvious.

The future is Vinge’s and Maddox’s accounts together, not either alone. If we were only in for the dystopia described by Vinge, we as a culture would have an obvious and powerful response: Orwell gave us the tools, and Stalin gave us the resolve, to resist the totalitarian state. A spying and invasive Net controlled by Washington is not our future. 1984 is in our past.

And if we were only in for the future that Maddox described, many of our citizens would believe this utopia, not science fiction. A world where “the market” runs free and the evil we call government, defeated, would, for them, be a world of perfect freedom.

But neither story alone describes what the Internet will be. Not Vinge alone, not Maddox alone, but Vinge and Maddox together: a future of control in large part exercised by technologies of commerce, backed by the rule of law.

The challenge of our generation is to reconcile these two forces. How do we protect liberty when the architectures of control are managed as much by the government as by the private sector? How do we assure privacy when the ether perpetually spies? How do we guarantee free thought when the push is to propertize every idea? How do we guarantee self-determination when the architectures of control are perpetually determined elsewhere? How, in other words, do we build a world of liberty when the threats are as Vinge and Maddox together described them?

The answer is not in the knee-jerk antigovernment rhetoric of our past. Reality is harder than fiction; governments are necessary to protect liberty, even if also sufficient to destroy it. But neither does the answer lie in a return to Roosevelt’s New Deal. Statism has failed. Liberty is not to be found in some new D.C. alphabet soup (WPA, FCC, FDA, etc.) of bureaucracy.

A second generation takes the ideals of the first and works them out against a different background. It knows the old debates; it has mapped the dead-end arguments of the preceding thirty years. The objective of a second generation is to ask questions that avoid dead-ends and move beyond them.

There is great work out there from both generations. Esther Dyson and John Perry Barlow still inspire, and still move on (Dyson is now the temporary chair of an organization some think will become the government of the Internet; Barlow now
spends time at Harvard.) And in the second generation, the work of Andrew Shapiro, David Shenk, and Steven Johnson is becoming well known and is compelling.

My aim is this second generation. As fits my profession (I’m a lawyer), my contribution is more long-winded, more obscure, more technical, and more obtuse than the best of either generation. As fits my profession, I’ll offer it anyway. In the debates that rage right now, what I have to say will not please anyone very much. And as I peck these last words before e-mailing the manuscript off to the publisher, I can already hear the reactions: “Can’t you tell the difference between the power of the sheriff and the power of Walt Disney?” “Do you really think we need a government agency regulating software code?” And from the other side: “How can you argue for an architecture of cyberspace (open source software) that disables government’s ability to do good?”

But I am also a teacher. If my writing produces angry reactions, then it might as well affect a more balanced reflection. These are hard times to get it right, but the easy answers to yesterday’s debate won’t get it right.
CHAPTER 17: WHAT DECLAN DOESN’T GET

Declan M. McCullagh is a writer who works for Wired News. He also runs a “listserve” that feeds to subscribers the bulletins that he has decided to forward and facilitates a discussion among these members. The list was originally called “Fight Censorship,” and it initially attracted a large number of subscribers who were eager to organize to resist the government’s efforts to “censor” the Net.

But Declan uses the list now for more than a discussion of censorship. He feeds to the list other news that he imagines his subscribers will enjoy. So in addition to news about efforts to eliminate porn from the Net, Declan includes reports on FBI wiretaps, or efforts to protect privacy, or the government’s efforts to enforce the nation’s antitrust laws. I’m a subscriber; I enjoy the posts.

Declan’s politics are clear. He’s a smart, if young, libertarian whose first reaction to any suggestion that involves government is scorn. In one recent message, he cited a story about a British provider violating fax spam laws; this, he argued, showed that laws regulating e-mail spam are useless. There is one unifying theme to Declan’s posts: let the Net alone. And with a sometimes self-righteous sneer, he ridicules those who question this simple, if powerful, idea.

I’ve watched Declan’s list for some time. For a brief time I watched the discussion part of the list as well. But the most striking feature about this list to me is the slow emergence of a new topic of concern—one that now gets more posts than “censorship.”

This topic is Y2K—the “year 2000 problem” that threatens to disrupt much in our social and economic life as computers discover that the new millennium does not compute. As clearly as Declan’s libertarianism comes through, so too does his obsession with Y2K. He is either terrified or perversely amused by what the new millennium will bring.

From the perspective of this book, these twin concerns—with regulation by the state and regulation by code—are quite consistent. Just as we should worry about the bad regulations of law, so too should we worry about the bad regulations of code. And from the perspective of this book, Y2K is our first real crisis in code. It is the first time that the culture as a whole will have to confront the environmental damage done by shortsighted coders. Like shortsighted lawmakers, they have created a crisis whose proportions we cannot yet see.
But from the perspective of Declan’s libertarianism, these twin concerns are harder to reconcile. Y2K is the product of a certain kind of libertarianism. It is the product of not thinking through the regulation of code, and of law not properly holding coders responsible for their code. Thousands of coders went about their work thinking their actions were simply their own. The culture and the legal system essentially treated those actions as those of individuals acting alone. Now, years after the first bad code was compiled, we are faced with a kind of environmental disaster: we are surrounded by code that in critical and unpredictable ways will misfire—at a minimum causing the economy millions of dollars, and under some doomsday scenarios causing much worse damage.

It is a lack of a certain kind of regulation that produced the Y2K problem, not too much regulation. An overemphasis on the private got us here, not an overly statist federal government. Were the tort system better at holding producers responsible for the harms they create, code writers and their employers would have been more concerned with the harm their code would create. Were contract law not so eager to allow liability in economic transactions to be waived, the licenses that absolved the code writers of any potential liability from bad code would not have induced an even greater laxity in what these code writers were producing. And were the intellectual property system more concerned with capturing and preserving knowledge than with allowing private actors to capture and preserve profit, we might have had a copyright system that required the lodging of source code with the government before the protection of copyright was granted, thus creating an incentive to preserve source code and hence create a resource that does not now exist but that we might have turned to in undoing the consequences of this bad code. If in all these ways government had been different, the problems of Y2K would have been different as well.

Y2K is just one example of a more general point that has been at the core of this book. We’ve had technology in our lives forever, and people have written about the consequences of technology for society since there has been technology. But this continuity should not blind us to an important disconnect we are about to see. Code may be only a difference in degree, but a difference in degree at some point becomes a difference in kind. The unintended consequence of private coding behavior is a time-bomb set to explode over the next year or so. The Y2K problem
should awaken us to other time-bombs in our lives—that is, to the general effect that code will have on our lives.

For here is a reality that all this “code talk” obscures. By speaking as I have about the code in cyberspace, by describing how government might regulate that code, by making it seem as if the worlds I am describing were in some sense elsewhere, I have obscured an obvious and critical point that the Y2K crisis makes real: code is not elsewhere, and we are not elsewhere when we feel its effects. As Andrew Shapiro puts it: “Seeing cyberspace as elsewhere misconstrues its legal significance. It keeps us from seeing the way that regulatory forces like code, which some say are ‘there,’ are actually affecting us here.”

We live life in real space, subject to the effects of code. We live ordinary lives, subject to the effects of code. We live social and political lives, subject to the effects of code. Code regulates all these aspects of our lives, more pervasively over time than any other regulator in our life. Should we remain passive about this regulator? Should we let it affect us without doing anything in return?

And thus again the odd juxtaposition of Declan’s two obsessions. Governments should intervene, at a minimum, when private action has public consequences; when shortsighted actions threaten to cause long-term harm; when failure to intervene undermines significant constitutional values and important individual rights; and when a form of life emerges that may threaten values we believe to be fundamental.

Yet so pervasive is our sense of the failure of government that a writer as intelligent as Declan cannot see the implications of these two great evils that he does so much to report. If we believe that government cannot do anything good, then Declan’s plea—that it do nothing—makes sense. And if government can do nothing, then it follows that we should treat these man-made disasters as natural. Just as we speak of the disaster of the West Coast sliding into the Pacific, so too should we speak of a disaster of code sliding us into another dark age. Neither can we do anything about, yet both are great topics for growing audiences.

I’ve advocated a different response. We need to think collectively and sensibly about how this emerging reality will affect our lives. Do-nothingism is not an answer; something can and should be done.
I've argued this, but not with much hope. So central are the Declans in our political culture today that I confess I cannot see a way around them. I have sketched small steps; they seem very small. I've described a different ideal; it seems quite alien. I've promised that something different could be done, but not by any institution of government that I know. I've spoken as if there could be hope. But Hope, it turns out, was just a television commercial.

The truth, I suspect, is that the Declans will win—at least for now. We will treat code-based environmental disasters—like Y2K, like the loss of privacy, like the censorship of filters, like the disappearance of an intellectual commons—as if they were produced by gods, not by Man. We will watch as important aspects of privacy and free speech are erased by the emerging architecture of the panopticon, and we will speak, like modern Jeffersons, about nature making it so—forgetting that here, we are nature. We will in many domains of our social life come to see the Net as the product of something alien—something we cannot direct because we cannot direct anything. Something instead that we must simply accept, as it invades and transforms our lives.

Some say this is an exciting time. But it is the excitement of a teenager playing chicken, his car barreling down the highway, hands held far from the steering wheel. There are choices we could make, but we pretend that there is nothing we can do. We choose to pretend; we shut our eyes. We build this nature, then are constrained by this nature we have built.

It is the age of the ostrich. We are excited by what we cannot know. We are proud to leave things to the invisible hand. We make the hand invisible simply by looking the other way.

But it is not a great time, culturally, to come across revolutionary technologies. We are no more ready for this revolution than the Soviets were ready for theirs a decade ago. We, like the Soviets, have been caught by a revolution. But we, unlike they, have something to lose.
How Shall the Net Be Governed?

David G. Post
The American Lawyer, "Plugging In," October 1996

There is no more fundamental question facing those who think about the legal regime for the developing electronic world than this: How will cyberspace be governed, and by whom? How will baseline rules of conduct that facilitate reliable communications and trustworthy commerce be established? Who will define, punish and prevent wrongful actions that trash the electronic commons or impose harm unjustifiably on others?

We take for granted a world in which geographical borders lines separating physical spaces are of primary importance in determining the rules that define legal rights and responsibilities: Law-making sovereignty itself is defined, at bottom, by control over a physical territory, and we look, essentially, to whether the persons residing in that territory have a voice in the exercise of that law-making power to assess whether or not the assertion of that power is legitimate. To be sure, this core assumption has been under strain in recent years as expansions in global trade and the ease of global transport and communication have increased the number and scope of interactions across physical boundaries, and global law-making institutions have been slowly adjusting to this gradual weakening of the significance of physical location. Multi-lateral action -- the GATT Treaty being perhaps the most noteworthy -- has been spurred by a recognition that an increased degree of harmonization of national intellectual property regimes is required in a world where goods and services can so easily cross national boundaries. Choice-of-law doctrine, too, has slowly adjusted; we no longer strictly apply the law of "the place" where an event or transaction takes place -- remember lex locus delicti and lex locus contractu? -- but look increasingly to where the effects of those events are felt for the source of applicable law.

But cyberspace does not merely weaken the significance of physical location, it demolishes it. It has no territorially based boundaries at all, because the cost and speed of message transmission on the Net is entirely independent of physical location: messages can be transmitted from any physical location to any other location without any distance-based degradation, decay, or delay, and without any physical cues or barriers that might otherwise keep certain geographically remote places and people separate from one another. The Net enables simultaneous transactions between large numbers of people who do not know, and in many cases cannot know, the physical location of the other party. One can logically and meaningfully talk of the "location" of events and transactions in cyberspace only in reference to a virtual space consisting of the "addresses" of the machines between which messages and information are routed; the system is entirely indifferent to the physical location of those machines.

And just as events in cyberspace thus take place "nowhere," they also can be characterized as taking place everywhere at once, in the sense that the effects of online activities are felt simultaneously in every corner of the global network. A World Wide Web page located on a machine in, say, Berlin can be accessed just as easily by users in Frankfurt, Germany; all jurisdictions simultaneously feel the effects of the information posted there, and thus all would appear to have equal claims to make the law governing the content of this site, surely a recipe for international chaos.

Any discussion of law in cyberspace must address this truly radical transformation of the law-making landscape. Want to control the transmission of pornographic material over the global net? Think you have the answer to the question of the proper scope of copyright in electronic information? Convinced that new rules regarding electronic contracts are required? In these and all other cases regarding activity in cyberspace, one must at some point stop and ask: Who will implement these rules, and by what means? If material placed on the net is equally accessible across the globe regardless of the geographical location from which it originates, can, say, the U.S. Congress determine whether or not the material is pornographic, or infringing of an author's copyright? If it does so, how can it enforce its determination when the source of the information is not within its borders? And if it relies on the within-border effects of online actions to justify its assertion of jurisdiction over, say, a World Wide Web server in Germany, or Mexico, or Brazil, what is to prevent the Germans, or Mexicans, or Brazilians from asserting their jurisdiction over Web servers in Des Moines or Dallas?

The difficulties that existing territorial sovereigns will experience if they seek to extend their jurisdiction to govern all
actions on the net that have substantial effects on their own citizenry does not mean that the net is inherently ungovernable. Anarchy, after all, has its costs; random results -- systematic misrouting of messages, say -- don't encourage trade or continuing interactions among people or entities. Large numbers of users will not visit online spaces if they encounter systematic fraud or vandalism or other activities they view as harmful or antisocial. The basic problem of social life -- how can people order their collective affairs to achieve results that they cannot accomplish on their own -- has not disappeared in cyberspace, and one would expect that if one model of governance is inadequate for the task others will be tried. Existing sovereigns could enter into international agreements to establish new and uniform rules specifically applicable to conduct on the net. Alternatively, we can envision, perhaps, creation of a new international organization (along the lines of the World Trade Organization) to establish new rules -- and new means of enforcing such rules and of holding those who make the rules accountable to appropriate constituencies. But what is perhaps most interesting about the rise of cyberspace is the glimpse it gives us of a fourth possibility, what might be called "decentralized, emergent law."

Consider how the Internet arose in the first place: the Internet exists only because a very large number of individual computer networks voluntarily adopted a new language -- the "Internet Protocols," consisting of a series of technical rules governing the way that messages are to be formatted and routed from one machine to another -- that allows those networks to communicate with one another. No sovereign authority with the power to compel obedience among its subjects promulgated those rules, no treaty decreed that a specific set of such standards must be used in order to link each of the diverse individual networks together into a single global web. Instead, under the banner of "rough consensus and working code," groups like the Internet Engineering Task Force and the World Wide Web consortium -- unofficial, unsanctioned, collections of interested volunteers -- published proposed communication standards that became the "law of the net" only because large numbers of individual system administrators voluntarily adopted the proposed rules. Each individual network remains free to impose its own technical standards on its users -- the Microsoft Network uses different communications principles for intra-network communication than does America Online, or Counsel Connect, or the Georgetown University LAN -- subject to the overriding mandate that if it wants to enable communication with other similarly-situated networks, it must adopt the basic communication protocols that those other networks have adopted.

If one thinks about it in this way, the net is hardly a "lawless" place at all; it is, indeed, a remarkable triumph of international coordination and cooperation, a complex adaptive system that produces a type of order that does not rely on top down, hierarchical control. Can this decentralized governance model, of local diversity within voluntarily-adopted constitutive rules, be made to work outside of the narrow technical domain in which it has heretofore operated, i.e., can this process work to set rules governing human social behavior? Of course, we know that this model can work in some contexts -- it's called federalism, and we have witnessed its success in our own constitutional system and elsewhere. Electronic federalism looks very different than what we have become accustomed to, because here individual network systems, rather than territorially-based sovereigns, are the essential governance unit. The law of the net, in other words, can emerge from the voluntary adherence of large numbers of network administrators to basic rules of law (and dispute resolution systems to adjudicate the inevitable inter-network disputes), with individual users "voting with their electrons" to join the particular systems they find most congenial. Or perhaps we should think of this as the law of the nets, for one possible (or even likely) consequence of this evolutionary development is the emergence of multiple network confederations, each with their own "constitutional" principles -- some permitting and some prohibiting, say, anonymous communications, some imposing strict rules regarding redistribution of information and others allowing freer movement -- enforced by means of electronic fences prohibiting the movement of information across confederation boundaries.

This governance model does not, of course, "solve" all problems (any more than the existing system of international law perfectly administers and enforces rules in the non-virtual world), and these governance issues will not be resolved overnight. Nor will they be resolved without a struggle; existing sovereigns are not about to blithely relinquish their law-making prerogatives and go quietly into that "Twilight of Sovereignty" that Walter Wriston presciently foresaw several years ago. But the Internet itself is testament to the enormous power of this rule-making model that may, in the end, prove to be irresistible.