if you are having trouble downloading -- click here to get the article in sections



# Foucault In Cyberspace:

## Surveillance, Sovereignty, and Hard-Wired Censors

**James Boyle[(1)] © 1997**

> *[T]he problems to which the theory of sovereignty were addressed were in effect confined to the general mechanisms of power, to the way in which its forms of existence at the higher level of society influenced its exercise at the lowest levels.. In effect, the mode in which power was exercised could be defined in its essentials in terms of the relationship sovereign-subject. But ..we have the .. emergence or rather the invention of a new mechanism of power possessed of a highly specific procedural techniques.. which is also, I believe, absolutely incompatible with the relations of sovereignty...It is a type of power which is constantly exercised by means of surveillance rather than in a discontinuous manner by means of a system of levies or obligations distributed over time....It presupposes a tightly knit grid of material coercions rather than the physical existence of a sovereign... This non-sovereign power, which lies outside the form of sovereignty, is disciplinary power...*[(2)]

This is an essay about law in cyberspace. I focus on three interdependent phenomena: a set of political and legal assumptions that I call the jurisprudence of digital libertarianism, a separate but related set of beliefs about the state's supposed inability to regulate the Internet, and a preference for technological solutions to hard legal issues on-line. I make the familiar criticism that digital libertarianism is inadequate because of its blindness towards the effects of private power, and the less familiar claim that digital libertarianism is also surprisingly blind to the state's own power in cyberspace. In fact, I argue that the conceptual structure and jurisprudential assumptions of digital libertarianism lead its practitioners to ignore the ways in which the state can often use privatized enforcement and state-backed technologies to evade some of the supposed practical (and constitutional) restraints on the exercise of legal power over the Net. Finally, I argue that technological solutions which provide the keys to the first two phenomena are neither as neutral nor as benign as they are currently perceived to be. Some of my illustrations will come from the current Administration proposals for Internet copyright regulation, others from the Communications Decency Act[(3)] and the cryptography debate. In the process, I make

opportunistic and unsystematic use of the late Michel Foucault's work to criticise some the jurisprudential orthodoxy of the Net.

---

# I

# The Internet Trinity

For a long time, the Internet's enthusiasts have believed that it would be largely immune from state regulation. It was not so much that nation states would not want to regulate the Net, it was that they would be unable to do so; forestalled by the *technology of the medium*, the *geographical distribution of its users* and the *nature of its content*. This tripartite immunity came to be a kind of Internet Holy Trinity, faith in it was a condition of acceptance into the community. Indeed the ideas I am about to discuss are so well known on the Net, that they have actually acquired the highest status that a culture can confer; they have become cliches.

## "The Net interprets censorship as damage and routes around it."

This quote from John Gilmore,[(4)] one of the Founders of the Electronic Frontier Foundation, has the twin advantages of being pithy and technologically accurate. The Internet was originally designed to survive a nuclear war; its distributed architecture and its technique of packet switching were built around the problem of getting messages delivered despite blockages, holes and malfunctions.[(5)] Imagine the poor censor faced with such a system. There is no central exchange to seize and hold; messages actively "seek out" alternative routes so that even if one path is blocked another may open up. Here was the civil libertarian's dream, a technology with *comparatively* low cost of entry to speakers and listeners alike, technologically resistant to censorship, yet politically and economically important enough that it cannot easily be ignored. The Net offers obvious advantages to the countries, research communities, cultures and companies that use it, but it is extemely hard to control the amount and type of information available; access is like a tap that only has two settings -- "off" and "full." For governments, this has been seen as one of the biggest problems posed by the Internet. For the Net's devotees, most of whom embrace some variety of libertarianism, the Net's structural resistance to censorship -- or any externally imposed selectivity -- is "not a bug but a feature."

## "In Cyberspace, the First Amendment is a local ordinance."[(6)]

To the technological obstacles the Net raises against externally imposed content filtration, one must add the geographic obstacles raised by its global extent; since a document can as easily be retrieved from a server 5,000 miles away as one five miles away, geographical proximity and content availability are

independent of each other. If the king's writ reaches only as far as the king's sword, then much of the content on the Net might be presumed to be free from the regulation of any *particular* sovereign.

The libertarian culture that dominates the Net at present posits that state intervention into private action is only necessary to prevent "harms." Seeing the Net as a "speech-dominated" realm of human activity in which harm would be comparatively hard to inflict, libertarians have been even more resistant to state regulation of the digital environment than of, the disdainfully named, "meatspace." "Sticks and stones can break my bones but bytes can never hurt me," or so goes their assumption. Thus, the postulate that a global Net cannot be regulated by national governments has been seen as an unequivocally positive thing.

John Perry Barlow's description of the First Amendment as a *local* ordinance, offers the sobering reminder that it is not merely "bad" state traditions, interventions and regulations that are enfeebled by cyberspace. There is a difference between speech being constitutionally protected and practically unregulable, indeed the latter situation may in some cases undermine the former protection.

## "Information Wants to be Free."

To a person interested in political theory, one of the most striking things about the Net is the instability of the political cartography. We divide our world up into contiguous and opposing territories -- public and private, property and sovereignty, regulation and laissez-faire -- "solving" problems by inquiring as to their placement on this map. In the everyday world these divisions seem comparatively solid and lumpish to most people, even if clever academic critics may harp on their *theoretical* indeterminacy. On the Net, things are different. Concepts and political forces seem to be up for grabs. Nothing illustrates this point better than the debate over intellectual property on-line. In the digital environment, is intellectual property just property, the precondition to an unregulated market, just another example of the rights that libertarians believe the state was specifically created to protect? Or is intellectual property actually *public regulation*, artificial rather than natural, an invented monopoly imposed by a sovereign state, a distorting and liberty-reducing intervention in an otherwise free domain?

While it would be hard to find anyone who believes entirely in either of these two stereotypes, recognisable versions of both do exist in the debate over intellectual property and -- more interestingly -- can be found across the political spectrum. George Gilder of the conservative Manhattan Institute, a fervent booster of capitalism and laissez faire, shows considerable skepticism about intellectual property [(7)] -- Peter Huber, from the same conservative think tank, pronounces it the very acme of liberty, privacy and natural right.[(8)] The Clinton Administration attempts to extend intellectual property rights on-line[(9)] and is roundly criticised by both civil liberties groups and right wing intellectuals.[(10)] This isn't just a disagreement as to tactics among people who might be said to share the same ideology: it is a fundamental set of disputes over the very social construction and normative significance of a particular phenomenon -- as if the Libertarian party couldn't agree on whether its motto was to be "Taxation is theft" or "Property is theft."

Stewart Brand's phrase "information wants to be free" has now penetrated the culture sufficiently deeply that it is now actually parodied in *advertisements*. Yet its ubiquitous nature may work to conceal the claims that it makes.

John Perry Barlow begins his famous essay "Selling Wine Without Bottles: The Economy of Mind on the Global Net" with this quote from Jefferson.

> If nature has made any one thing less susceptible than all others of exclusive property, it is the action of the thinking power called an idea, which an individual may exclusively possess as long as he keeps it to himself; but the moment it is divulged, it forces itself into the possession of everyone, and the receiver cannot dispossess himself of it. Its peculiar character, too, is that no one possesses the less, because every other possesses the whole of it. He who receives an idea from me, receives instruction himself without lessening mine; as he who lights his taper at mine, receives light without darkening me. That ideas should freely spread from one to another over the globe, for the moral and mutual instruction of man, and improvement of his condition, seems to have been peculiarly and benevolently designed by nature, when she made them, like fire, expansible over all space, without lessening their density at any point, and like the air in which we breathe, move, and have our physical being, incapable of confinement or exclusive appropriation. Inventions then cannot, in nature, be a subject of property.[(11)]

The quotation expresses perfectly the mixture of Enlightenment values and upbeat public goods theory that typifies Net analysis of information flows. Information *is* costless to copy, *should* be spread widely, and *cannot* be confined. Beyond the Jeffersonian credo lies a kind of Darwinian anthropomorphism. Information really does *want* to be free. John Perry Barlow credits Brand's phrase with

> recognizing both the natural desire of secrets to be told and the fact that they might be capable of possessing something like a "desire" in the first place. English biologist and philosopher Richard Dawkins proposed the idea of "memes," self-replicating, patterns of information which propagate themselves across the ecologies of mind, saying they were like life forms. I believe they are life forms in every respect but a basis in the carbon atom. They self-reproduce, they interact with their surroundings and adapt to them, they mutate, they persist. Like any other life form they evolve to fill the possibility spaces of their local environments, which are, in this case the surrounding belief systems and cultures of their hosts, namely, us. Indeed, the sociobiologists like Dawkins make a plausible case that carbon-based life forms are information as well, that, as the chicken is an egg's way of making another egg, the entire biological spectacle is just the DNA molecule's means of copying out more information strings exactly like itself.[(12)]

Viewed through this lens, the Net is the ultimate natural environment for information and trying to regulate the Net is like trying to prohibit evolution.

Taken together the three quotations assert that the technology of the medium, the geographical

distribution of its users and the nature of its content all make the Net it specially resistant to state regulation. The state is too big, too slow, too geographically and technically limited to regulate a global citizenry's fleeting interactions over a mercurial medium. Though I do not subscribe to the full-throated versions of any of these slogans, I have sympathy with each of them. It does excite me that the Net is highly resistant to externally imposed content filtration -- though I tend to worry about structural private filters as well as command-based public ones, and I recognise that speech and information can and will produce harm as well as good. I do think that the global nature of the Net is -- by and large -- a positive thing, though we need to pay more attention to things like the cost of the technology required to play the game, or the effects on workers of a networked economy in which companies can relocate around the world and find a new on-line workforce in an afternoon.[(13)] Finally, I am optimistic about the historical conjunction of technologies based on nearly costless copying and a political tradition that treats information in a more egalitarian way than other resources.[(14)] It is possible, of course, to conjure up a world in which rampant info-kleptocracy undermines scientific and artistic development. I have argued elsewhere that the main danger is not that information will be unduly free, but that intellectual property rights will become so extensive that they will actually stifle innovation, free speech and educational potential. In any event, I want to set aside my agreement or disagreement with the values behind the Net catechism, and focus instead on the factual and legal assumptions on which it relies. My argument is that info-libertarians should not be so quick to write off the state. In fact, I argue that the work of the distinctively non-digital philosopher, Michel Foucault, provides some suggestive insights into the ways in which power can be exercised on the Net and the reasons why much contemporary analysis is so dismissive of the power of law and the state.

---

# II

# Foucault & the Jurisprudence of Digital Libertarianism

When Netizens think of law, they tend to conjure up a positivist, even Austinian image;[(15)] law is a command backed by threats, issued by a sovereign who acknowledges no superior, directed to a geographically defined population which renders that sovereign habitual obedience.[(16)] Thus they think of the state's laws as blunt instruments incapable of imposing their will on the global subjects of the Net and their evanescent and geographically unsituated transactions. Indeed, if there was ever a model of law designed to fail at regulating the Net, it is the Austinian model. Fortunately or unfortunately for the Net, however, the Austinian model is both crude and inaccurate, and that is where the work of the late Michel Foucault comes in.

Michel Foucault was one of the most interesting of post war French philosophers and social theorists. His work was wide-ranging, sometimes obscure,[(17)] indeed deliberately so, and his historical generalisations would have been be insufferable if they were not so often provocatively useful.[(18)]

Above all, Foucault had the knack of posing problems in a new way -- re-orienting the inquiry in a way that was manifestly helpful for those who followed. This facility has been testified to by thinkers whose politics and methodology are very far from Foucault's own.[(19)]

From the point of view of this article, one of Foucault's most interesting contributions was to challenge a particular notion of power, power-as-sovereignty, and to juxtapose against it a vision of "surveillance" and of "discipline."[(20)] At the heart of this project was a belief that both our analyses of the operation of political power and our strategies for its restraint or limitation were inaccurate and misguided. In a series of essays and books, Foucault argued that, rather than the public and formal triangle of sovereign, citizen and right, we should focus on a series of subtler, private, informal and material forms of coercion organised around the concepts of "discipline" and "surveillance." The paradigm for the idea of surveillance was the Panopticon, Bentham's plan for a prison constructed in the shape of a wheel around the hub of an observing warden, who at any moment *might* have the prisoner under observation through a nineteenth century version of the closed circuit TV.[(21)] Unsure of when authority might in fact be watching, the prisoner would strive always to conform his behaviour to its presumed desires; Bentham had struck upon a behavioralist equivalent of the superego, formed from uncertainty about when one was being observed by the powers that be. The echo of contemporary laments about the 'privacy-free state' is striking. To this Foucault added the notion of discipline -- crudely put, the multitudinous "private" methods of regulation of individual behaviour ranging from workplace time-and-motion efficiency directives to psychiatric evaluation.[(22)]

Foucault pointed out the apparent conflict between a formal language of politics organised around relations between sovereign and citizen, expressed through rules backed by sanctions, and an actual experience of power being exercised through multitudinous non-state sources, often dependent on material or technological means of enforcement. Writing in a manner that managed to be simultaneously coy and sinister, Foucault suggested that there was something strange going on in the coexistence of these two systems.

> Impossible to describe in the terminology of the theory of sovereignty from which it differs so radically, this disciplinary power ought by rights to have led to the disappearance of the grand juridical edifice created by that theory. But in reality, the theory of sovereignty has continued to exist not only as an ideology of right, but also to provide the organising principle of the legal codes.... Why has the theory of sovereignty persisted in this fashion..? For two reasons, I believe. On the one hand, it has been.. a permanent instrument of criticism of the monarchy and all the obstacles that can thwart the development of a disciplinary society. But at the same time, the theory of sovereignty, and the organisation of a legal code centered upon it, have allowed a system of right to be superimposed upon the mechanism[] of discipline in such a way as to conceal its actual procedures ....[(23)]

Foucault was not writing about the Internet. He was not even writing about the twentieth century. But his words provide a good starting place from which to examine the catechism of Net inviolability. They

are a good starting point precisely because, when viewed within the discourse of sovereignty, of the promulgation and enforcement of Austinian "commands backed by threats" aimed at a defined territory and population, the Net does indeed look almost invulnerable. Things look rather different when viewed from the perspective of "a type of power which is constantly exercised by means of surveillance rather than in a discontinuous manner by means of a system of levies or obligations distributed over time [and which]... presupposes a tightly knit grid of material coercions rather than the physical existence of a sovereign." What's more, there is a sense in which the "system of right [is] superimposed upon the mechanism[] of discipline in such a way as to conceal its actual procedures"; the jurisprudence of digital libertarianism is not simply inaccurate, it may actually obscure our understanding of what is going on. Thus even the digerati may find the analysis that follows of interest; if only to see how far the Net can be made to treat censorship as a feature not a bug, how far local ordinances may reach in cyberspace, and how information's 'desire for freedom' may be curbed.

The examples I will give are drawn from different areas of regulation of communications technology. Some of them deal explicitly with the Internet: the Communications Decency Act, the proposed NII Copyright Protection Act, the regulation of cryptography. Others are directed towards technologies outside of the Net, at least for the present: the V-chip, the Clipper chip, digital telephony and digital audio recorders. All of them share one thing -- the state has worked actively to embed or hardwire the legal regime in the technology itself.[(24)] In most of them, the exercise of power is much more a matter of the quotidian shaping and surveillance of activity than of imposing sanctions after the fact. Yet these examples also present revealing differences -- illustrating a range of goals, tactics and results. Sometimes technology has been mandated by legislation, sometimes facilitated through state-sanctioned standard-setting bodies. Sometimes the legislation defines technological safe-harbours to sanctions that would otherwise apply and sometimes the state uses the power of the purse to create a *de facto* standard by refusing to purchase any equipment that does not conform to the desired technical/legal standards. I will begin with the Communications Decency Act, turn to the use of strict liability and digital fences in internet copyright policy and conclude with a sampler of hardwired regulation, drawn from a number of areas of communications technology.

---

## III

## Safe Harbours and Unintended Consequences

The Communications Decency act has been hailed as the nadir of Congressional regulation of communications technology. Badly drafted, inconsistently worded[(25)] and palpably unconstitutional, it appeared to most of the Internet community to be a case of technological ignorance run rampant. Here was a Congress regulating what it did not understand, and doing so in a way that would be practically futile because of the amount of content that came from beyond the jurisdiction of the United States. The reactions ranged from condescending amusement at the lack of Congress's technological knowledge to

proprietary anger that the law was overtly asserting its power over the electronic frontier. "Keep your laws off our Net" went the slogan.

When the CDA was struck down by two different three- judge panels[(26)] and then by a unanimous Supreme Court[(27)] the decisions were seen as an inevitable vindication of these libertarian views. The fact that the lower court opinions referred to the constitutional problems raised for the CDA by the fact that it could not reach much of the content on the Net merely sweetened the victory. Federal judges had come a long way towards recognising both the technological resistance of the Net to censorship and the fact that a global net could *never* be effectively regulated by a single national jurisdiction.[(28)] Two of the three parts of the Internet trinity had been acknowledged in the Federal Reporters. What's more they had actually been plugged into the framework of conventional First Amendment analysis. Given the fact that the CDA would be likely to be ineffective, could we possibly say that it passed strict First amendment scrutiny?[(29)] Wasn't this a case of substantially restricting "the freedom of speech" without effectively achieving the compelling state interest?

Seen through the lens provided by the jurisprudence of digital libertarianism, these reactions were entirely warranted. A command backed by threats uttered by a sovereign and directed towards a geographically defined population had met and been annihilated by a right held by citizens against intrusion by state power, in part because of the sovereign's inability to regulate those outside its borders. The Communications Decency Act vanishes as if it had never been -- an utter failure. Yet this analysis misses the developments surrounding the CDA: not the public criminal sanction but the shaping and development of privately deployed, materially based, technological methods of surveillance and censorship.

The Communications Decency Act aimed to protect minors from indecent material; however, if it did so by substantially limiting the speech of adults it would be held unconstitutional as overbroad; "burning down the house to roast the pig" in the words of Justice Frankfurter.[(30)] The CDA's answer to this problem was to create safe harbours for indecent but constitutionally protected speech aimed at adults, provided that speech was kept from the eyes of minors.[(31)] The Act offered a number of methods to achieve this goal, such as "requiring [the] use of a verified credit card, debit account, adult access code, or adult personal identification number."[(32)] Given the technology and economics of the Net, however, the most important safe harbour for non-profit organisations was clearly going to be that provided by §223(e)(5)(A), offering immunity to those who had used "any method which is feasible under available technology."[(33)]

It is here that the irony begins. When the Communications Decency Act was first proposed, a number of computer scientists and software engineers decided that they would do something more than merely railing against its unconstitutionality. They were convinced that an answer to the perceived need for regulation could be met within the language of the Net itself.[(34)] I am not using the "language of the Net" as part of some deconstructive or Saussurean trope, the idea was literally to provide a filtering

system whose markers would be built into the language that makes the World Wide Web possible, Hyper Text Markup Language or HTML. Conceiving of technical solutions as intrinsically more desirable than the exercise of state power by a sovereign, as facilitators of private choice rather than threats of public sanction. they offered an alternative designed to show that the Communications Decency act was, above all, unnecessary. It is called the Platform for Internet Content Selection or 'PICS' and it allows tags rating a web page to be embedded within "meta-file" information provided by the page about itself.[(35)] The system can be adapted to provide both first party and third party content labelling and rating.[(36)] The system is touted as "value-neutral" because it *could* be used to promote any value-system. Sites could be rated for violence, for sexism, for adherence to some particular religious belief, for any set of criteria that was thought worthwhile. The third party filtering site could be the Christian Coalition, the National Organization for Women or the Society for Protecting the Manifest Truths of Zoroastrianism. Of course in practice, we might believe that the PICs technology would be disproportionately used to favour a particular set of ideas and values and exclude others, just as we might believe that *in practice* a Lochner regime of "free contract" would actually favour some groups and hurt others, despite the fact that each is -- on its face -- value neutral. But this kind of legal realist insistence on looking at actual effects and scrutinising actual, rather than formal power, is much less a part of our First Amendment discourse than of our private law discourse as Owen Fiss, Jack Balkin and Richard Delgado have each pointed out, though in very different contexts.[(37)]

While PICS and a variety of other systems offered a technical solution at the "speaker" end of the connection, other software programs also offered technical solutions at the listener end. These programs would not offer speakers a safe harbour from the reach of the Act. Rather they would "empower" computer users to protect their families from unwanted content through the use of software filters, thus raising in civil libertarians hearts the hope that the whole act was unnecessary. Programs such as SurfWatch, CyberPatrol, NetNanny and CyberSitter, would block access to unsuitable material and do so without the need for constant parental intervention.[(38)] Typically these programs maintained a list of forbidden sites as well as a text-search filter which would not load documents containing forbidden strings of words.

The irony that I mentioned is that these technical solutions were used by both sides in the dispute over the CDA. Those challenging the CDA argued that the availability of privately implemented technological fixes meant that the CDA failed First amendment scrutiny: clearly it was not the least restrictive means available to achieve the objective. "Listener-centered" blocking software would allow parents to control what their children saw while "Speaker-centered," or third party, rating systems such as PICS would offer a private solution to the problem of rating the content available on the Net.

The government took the opposite position, arguing that the availability of systems such as PICS meant that the CDA was not overbroad. Adult speakers would not be burdened by the law because such systems provided adequate methods for adult speakers to segregate their indecent but protected speech from the eyes of minors. Thus, in their eyes, the PICS scheme, developed to destroy the CDA, actually saved it.[(39)] The Supreme Court ultimately disagreed, though Justice O'Connor left open the possibility

that future technical developments might change that conclusion.[(40)] Before the decision was even handed down President Clinton was already signalling his political preference for a technical solution to the question of regulating speech on-line, talking vaguely of a "V-chip for the Net."[(41)] Bills have already been advanced in Congress which would require Internet Service Providers to provide filtering software to customers and aim at the development of an "E-chip."[(42)]

So where does the on-line speech stand after the Supreme Court's decision in Reno v. ACLU? From the perspective of the digital libertarian, the Net remains unregulated and the Internet trinity is undisturbed. From the perspective I have been developing here, things seem much more mixed. As the CDA was being constitutionally voided, the technological "solutions" were proceeding apace, some because of the CDA, some in spite of the CDA; In contrast to the extensive attention given to CDA, much of this process was effectively insulated from scrutiny because of the assumptions about law and state I have been exploring here.

PICS is wonderful tool for content selection, and if one assumes a world very much like the idealised version of the marketplace of ideas, in many ways an unthreatening and beneficial one. Yet its technological goal -- to facilitate third as well as first party rating and blocking of content -- helps to weaken the Net's supposed resistance to censorship at the same moment that it helps provide a filter for user-based selection. If national networks can be more easily run through a kind of PICS-filtered firewall, what happens to the notion that the of Internet tap can only be turned to "off" or "full"? One wonders how China or Singapore or Iran would choose to employ this "value-neutral" system. The technological component of the Internet faith does not fall but it is weakened. The state may not be able to deploy Austinian sanctions backed by threats over the Net but the technology provided by PICS gives it a different arsenal of methods to regulate content materially rather than juridically, by everyday softwired routing practices, rather than by threats of eventual sanction.

As for the listener based software filters, they present even more problems. Journalists studying these programs found that their list of selected sites was problematic and -- most importantly -- was actually hidden from the users.

A close look at the actual range of sites blocked by these apps shows they go far beyond just restricting "pornography." Indeed, some programs ban access to newsgroups discussing gay and lesbian issues or topics such as feminism. Entire *domains* are restricted, such as HotWired. Even a web site dedicated to the safe use of fireworks is blocked. All this might be reasonable, in a twisted sort of way, if parents were actually aware of what the programs banned. But here's the rub: Each company holds its database of blocked sites in the highest security. Companies fight for market share based on how well they upgrade and maintain that blocking database. All encrypt that list to protect it from prying eyes.[(43)]

The programs turned out to ban sites ranging from the National Rifle Association to the National Organization for Women and to do so in a way that is often undetectable by their purchasers. Nevertheless enthusiasm for these programs continues unabated. President Clinton promises that

government is working on an Internet V-Chip,[(44)] Boston city libraries are installing them on computers accessible to children[(45)] and Texas is considering mandating that Internet access companies make copies of these programs available to all their new customers.[(46)] Representative Markey introduced a Bill into this session of Congress which would require both the creation of an "E-chip" and the provision of free or "at cost" blocking software.[(47)] In constitutional terms this raises interesting questions of state action. One of the attractions of the technical solution is often that it allows the state to enlist private parties to accomplish that which it is forbidden to accomplish directly. But this state action problem is merely the constitutional incarnation of the political limitations of the jurisprudence of digital libertarianism -- its sole focus on state power, narrowly defined, its blindness towards the technical and economic shaping, rather than the legal sanctioning of the communications environment.

I do not want to overstate the effect of the mindset that I am describing. Not everyone in the digital world thinks this way. Libertarians too, have been worried by the dangers posed by technologically invisible filtering of communication -- indeed one of the most interesting thing about Internet politics is that they have forced libertarians to confront some of the tensions in their own ideas.[(48)] Finally other commentators have made the points I make here, though they also lamented the blindness imposed by an entirely libertarian focus.[(49)] Nevertheless, the result of the Supreme Court's decision in Reno v. ACLU will simply be to sharpen the turn to the kinds of filtering devices here and it is unlikely that this will leave the Net as free, or the state as powerless as the digerati seem to believe.

---

# IV

# Privatised Panopticons and Legalised Enclosures

I have argued elsewhere that the current government proposals for the "reform" of copyright on the Internet weigh only the costs of cheaper copying rather than its benefits, underestimate the importance of fair use to competition policy and free speech, fail to recognise the unique features of both intellectual property and networked environments, and apply bad economic analysis to an even worse depiction of current law.[(50)] Leaving aside the virtues or vices of these proposals aside for the moment, I will focus here on the methods by which they were to be implemented.

One of the key problems for any Internet copyright regime is enforcement. The Internet trinity I discussed earlier would seem to apply with particular strength to the problem of policing copyright on a global distributed network. The technology is resistant to control, the subject matter of the regime is intangible and trivially easy to circulate, and both the content and the people regulated by the regime are frequently beyond the jurisdiction of the sovereign in question. The combination of these circumstances

has produced a series of warnings that intellectual property law was doomed because neither its conceptual structure nor its enforcement mechanism could survive 'being digital.'[(51)] The best known of these warnings is also the best written.

The riddle is this: if our property can be infinitely reproduced and instantaneously distributed all over the planet without cost, without our knowledge, without its even leaving our possession, how can we protect it? How are we going to get paid for the work we do with our minds? And, if we can't get paid, what will assure the continued creation and distribution of such work? Since we don't have a solution to what is a profoundly new kind of challenge, and are apparently unable to delay the galloping digitization of everything not obstinately physical, we are sailing into the future on a sinking ship. This vessel, the accumulated canon of copyright and patent law, was developed to convey forms and methods of expression entirely different from the vaporous cargo it is now being asked to carry. It is leaking as much from within as without. Legal efforts to keep the old boat floating are taking three forms: a frenzy of deck chair rearrangement, stern warnings to the passengers that if she goes down, they will face harsh criminal penalties, and serene, glassy-eyed denial.[(52)]

If one saw these technological transformations as mainly a threat to both the copyright owner and the enforcement power of the state, how would one respond, particularly if one took seriously the difficulties in policing that the Internet trinity points out? One would try to focus on building the regime into the architecture of transactions in the first place -- both technically and economically -- rather than policing the transactions after the fact. More concretely, one would want to escape from the practical and legal limitations of a sovereign-citizen relationship. Thus one might seek out private actors involved in providing Net services who are not quite as *mobile* as the flitting and frequently anonymous inhabitants of cyberspace. In this case, the parties chosen were the Internet Service Providers. One would pin liability on them and leave it up to them to prevent copyright infringement through technical surveillance, tagging and so on, and to spread the cost of the remaining copyright infringement over all the users of their service, rather than all the purchasers of the product in question.

By enlisting these nimbler, technologically savvy players as one's private police, one would also gain another advantage; freedom from some of the constitutional and other restraints that would burden the state were it to act directly. Intrusions into privacy, automatic scrutiny of e-mail, curtailing of fair use rights so as to make sure that no illicit content was being carried; all of these would occur in the private realm, far from the scrutiny of public law. There are advantages to privatising the Panopticon, it turns out.

Given all these "advantages" it is unsurprising to find that strict liability for on-line service providers became a central feature in the Clinton administration White Paper,[(53)] the Bills implementing its ideas [(54)] and the US's proposals for the WIPO treaties in Geneva.[(55)] The specifics of this proposal were relatively simple. On-line service providers were to be made strictly liable for copyright violations committed by their subscribers -- in part this was done by an expansive definition of fixation so that even holding a document in RAM memory as it was browsed, would constitute the creation of a copy.

(56) Clearly then, the relatively more stable versions held in a server's disk cache or stored temporarily in its computers would count as copies. The theory also depended on the notion that we should analogize the on-line service provider to an innocent but infringing photoshop and thus impose strict liability as a direct infringer, rather than analogizing the service provider to a business that rented Xerox machines by which material *could* be copied illegally, which would be liable only if it was guilty of contributory infringement.(57) Notably this theory was rejected by the only court to have faced it squarely.(58)

In one sense this strategy is very similar to the use of strict liability elsewhere in the legal system -- and of course it can be understood entirely without reference to the Foucauldian gloss. (Although one must note that the the conventional reasons for imposing strict liability are strikingly absent.(59)

With or without Foucault, however, thinking about the use of strict liability as an enforcement mechanism does illustrate the limitations of the Austinian view of the state's exercise of power. (Unsurprisingly perhaps, Austin argued againt strict liability and judges under the influence of Austinian reasoning actually declared that strict liability was not true law.)(60) My central point here is not the undesirability of strict liability for on-line service providers, though the rationale, legal basis and constitutionality of sucha system seem doubtful to me. Rather, I think that the possible impact of a strict liability system on actual privacy, speech and discourse indicates another limitation of the jurisprudence of digital libertarianism. Onee again, the focus on public, criminal and sanction-backed acts by states exercising their power directly, tends to obscure and thus to undervalue the efficacy of efforts that rely on privatised enforcement and surveillance, cost spreading and the use of "material coercion rather than the physical existence of a sovereign."

It is to the latter point that I now turn. One prong of the Administration's plan for copyright on the Net depended on enrolling private actors to act as enforcement agents in a way that sidestepped the rights, duties and privileges between citizen and sovereign. The other prong depended on coating technological anti-copying devices with the authority of the law in such a way as to change the relative powers of current copyright holders on the one hand and their customers and future competitors on the other. The two most important provisions are the "circumvention of copyright protection systems" section and the "integrity of copyright management information" section of the NII Copyright Protection Act of 1995. (61) Similar provisions were proposed by the United States during the WIPO conference.(62)

These two provisions seem on first sight to be entirely unobjectionable. The circumvention section imposes civil liability on importers, manufacturers and distributors of devices the primary purpose or effect of which is to circumvent a copyright protection system.(63) The management section imposes civil *and* criminal liability on someone who removes or tampers with copyright management information.(64) Obviously technological protections are going to be an important way by which digital intellectual property is safeguarded and these technological protections will include, among other things the kind of deeply embedded information that the management information section protects. Documents

will keep track of how many times they are read and may complain if they are read too much or by the wrong person. Pamela Samuelson calls these "texts that rat on you." Digital books sold to one person may be encoded so that they can't be read by someone else on another computer. Given the possibility of documents that have the copyright details bound into in every packet of data, and which also check themselves to be sure that no alterations have been made, quotation may be perceived as alteration. (Presumably internet service providers would also be encouraged to introduce some system of scanning which looked for altered or unauthorised packets of data.)

The point about all of this, is that there will be a continuing technological struggle between content providers, their customers, their competitors and future creators. Obviously it will sometimes be in the interest of content providers to make it as hard as possible for citizens to exercise their fair use rights. They will try to build technological and contractual fences around the material that they provide, not just to prevent it being stolen, but to prevent it from being used in ways that have not been paid for, even if those uses are privileged under current intellectual property law. They may want to stop their competitors from achieving "interoperability" or prevent their customers from selling second hand versions of their producs. The technical means to do this can be thought of digital fences. Sometimes those fences will be used to stop clear violations of existing rights. Sometimes they will be used to enclose the commons or the public domain. Thus by making it illegal or impractical for me to go around through or over the fence, the state adds its imprimatur to an act of digital enclosure. The Internet trinity tells us that information wants to be free and that the thick fingers of Leviathan are too clumsy to hold it back. The position is less clear if that information is guarded by digital fences which themselves are backed by a state power maintained through private systems of surveillance and control.

---

# V

# A Communications Sampler

The tendencies I have been describing here by no means end with the Communications Decency Act and the NII Copyright Protection Bill. In fact, the turn to privatised and technologically based enforcement to avoid practical and constitutional obstacles seems to be the rule rather than the exception.

Outside of the Net, the most obvious example of this is the V-Chip, a device to enable parents to restrict television programming through a "voluntary" rating system. While the rating system is voluntary, the device is mandated by section 551 of the Telecommunications Act of 1996.[(65)] The V-Chip decodes a set of ratings agreed to by private parties and suggested by a state-convened "private" board." It then blocks programming that is above a ratings threshold set by parents.[(66)] The attractiveness of this hardwired mix of public and private decisions can be judged by the spread of V-Chip analogies -- President Clinton's "V-Chip for the Net," Rep. Markey's "E-Chip." Why is this device so popular, not just as a device, but as a rhetorical trope? The answer, I think, is partly provided by the characteristics

outlined here. The V-chip seems to be merely a neutral facilitator of parental choice. The various acts of coercion involved -- the government making the television company insert the thing into the machine, the public-private board choosing which ratings criteria will be available for parents to use -- simply disappear into the background. Finally, the distributed privatised nature of the system promises that it might actually work -- though admittedly, state administration of the television system poses fewer headaches that state administration of the Net.

Another set of examples is provided by encryption policy. In the digital era, encryption is no longer merely the stuff of spy novels. It provides the walls, the boundaries, the ways of preventing unauthorized or unwanted entry. Faced with the development of a cryptography industry which would produce digital walls unbreakable by the state, the government responded by attempting to legislate its own backdoor The first proposal was that the encryption of all communications had to be through a government designed device -- known as the Clipper Chip. Your phone, fax or computer system would encrypt your communication using the algorithm hardwired into the Clipper Chip. The Clipper Chip utilizes a "key escrow" system under which the government maintains a "back door" key to decrypt all Clipper communications; a key that is supposed to be available only to law enforcement agencies who, most of the time, would have to get judicial approval of their actions. After considerable controversy, use of the Clipper Chip encryption system was declared "voluntary" for both the government and the private sector.

This might seem to be a partial vindication for the digital libertarian position. In fact, the government has, for the most part, adopted the Clipper Chip and has tried to use its considerable purchasing power to make it a de facto industry standard.[(67)] While the success of this method may have been undermined by later technical development, the strategy shows that hardwired legal regime can be implemented through market power as well as by fiat.

One of the arguments behind the Clipper Chip was that law enforcement agencies were merely striving to achieve the same level of physically permissible surveillance in a world of encoded transmissions as they currently possessed. With this as a baseline it was obvious that the material possibility for interception and decryption should be hardwired into the system itself. The same argument was made successfully over digital telephony. Realizing that new telephony technology, such as call forwarding, cellular telephones, and digital communications in general, present increasing challenges to wire tapping, Congress passed the Communications Assistance for Law Enforcement Act,[(68)] more commonly known as the "Digital Telephony Act." At its heart, the Digital Telephony Act requires that telecommunications companies make "tappability" a design criteria for the system. Everything recorded by the traditional "pen register" system, as well as a few new categories of information, must be digitally recorded. Under the Act, information regarding a subscriber's name, address, telephone toll billing records, telephone number, length of service and the types of services utilized are now available to the government.[(69)]

Technologically hardwired protections have also been implemented in order to protect intellectual property as in the Digital Audio Tape or (DAT) standard. Unlike compact disks, which until recently

were "read-only," digital audio tape technology allows users to make perfect copies of recordings. Fearing that this ability would lead to the development of an extensive market for copied tapes, the recording industry pushed for mandatory technological protection, which they received in the Audio Home Recording At of 1992.[(70)] This Act requires all DAT recorders to utilize the Serial Copy Management System, which allows a first copy to be made onto DAT but prevents all subsequent copies.

These examples give us a number of conclusions at odds to popular wisdom. On the one hand, they offer a cautionary note to the libertarian techno-optimists who believe that technology always grows out of governmental control and always in the direction of greater "liberty." Let us lay aside many of the assumptions behind that belief for a moment-- such as that governments are generally the greatest threat to daily "liberty" -- or conversely that liberty should be defined primarily around the absence of governmental restraint. Even with these qualifications the idea that the technological changes of the digital revolution are always outside the control of the state seems unproven,. In fact, the state is working very hard to design its commands into the very technologies that, collectively are supposed to spell its demise.

Another point needs to be made: As these examples indicate there are -- whether one likes them or not -- strong arguments that the "technologies of freedom" actually require an intensification of the mechanisms of surveillance, public and private, to which we are currently subjected. Cheap copying can be seen as primarily a threat to copyright, global communication as a source of child pornography and bomb recipes, encryption as a wall behind which the terrorist and the drug smuggler can hide. If the digital technologies enlarge our space for living, both conceptually and practically, the dangers posed by that expansion will prompt the demand -- often the very reasonable demand -- that the Panopticon be hardwired into the "technologies of freedom."[(71)]

---

## Conclusion

Looked at in a vaguely Foucauldian light, the examples I have given in this Article seem to point to two conclusions, conclusions which may seem paradoxical. On the one hand, the studies indicate that the assumption that the state will not be able to regulate cyberspace is definitionally blind to some of the most important ways that some states could, in fact, exert power. The jurisprudence of digital libertarianism could use a lot less John Austin and a lot more Michel Foucault. But one cannot simply limit the analysis to the available avenues of *state* power. *Discipline and Punish* was not a manual for state officials, but a challenge -- in some ways similar to the challenges posed by legal realism and feminism -- to the very categories of public and private and to the belief that power begins and ends with the state.

If the first conclusion of this study is that the state may actually have more power than the digerati

believe, the second conclusion is that the attractiveness of technical solutions stems not simply from the fact that they work, but that they apparently elide the question of power -- both private *and* public -- in the first place. The technology appears to be "just the way things are"; its origins are concealed, whether those origins lie in state-sponsored scheme or market-structured order, and its effects are obscured because it is hard to imagine the alternative. Above all, technical solutions are less contentious;[(72)] we think of a legal regime as coercing, and a technological regime as merely shaping -- or even actively facilitating -- our choices. In the Lochner era a strikingly similar contrast was drawn between the coercive nature of public law and the free private world of a market that was merely shaped by neutral, facilitative rules of contract and property. The legal realists did a remarkably good job of pointing out the shortcomings of that picture of the market. If we are to have some alternatives to the jurisprudence of digital libertarianism we will have to offer a richer picture of Internet politics than that of the coercive (but impotent) state and the neutral and facilitative technology.

---

---

# Endnotes

1. Professor of Law, Washington College of Law, American University. My remarks at the conference dealt more specifically with the law and policy of proposed changes to copyright on the Internet. However, I have already outlined some of those views in print, and at some length. *See* James Boyle, Shamans, Software and Spleens: Law and the Construction of the Information Society at 136-39, 192-200 (Harvard University Press 1996), *Intellectual Property Policy On-Line: A Young Person's Guide*, 10 Harv. J.L. & Tech. 47 (1996), *Sold Out*, N.Y. Times, March 31st 1996, at E15, *Overregulating the Internet?*, Insight, January 15th, 1996, at 24, *A Politics of Intellectual Property: Environmentalism for the Net*, Duke L.J. (forthcoming). The editors of the Cincinnati Law Review were kind enough to allow me to address myself in this article to a slightly different issue, though one of profound importance to the symposium as a whole -- the extent to which state regulation of the Net is possible at all, and the costs and benefits of "technical solutions." In the course of that discussion, I use a number of examples drawn from the recent proposals on Internet copyright.

2. Michel Foucault, Two Lectures, *in* Michael Foucault, Power/Knowledge: Selected Interviews and Other Writings, 1972-1977, 78, 104 (Colin Gordon ed. & Colin Gordon et al. trans., 1980).

3. The Telecommunications Act of 1996, Pub. L. No. 104-104, tit. V, §§ 501- 61, 110 Stat. 56 (1996).

4. There are a variety of versions of the claim but the content is pretty consistent. *See, e.g.*, John Perry Barlow, Passing the Buck on Porn (visited June 24, 1996) <http://www.eff.org/pub/Publications/John_Perry_Barlow/HTML/porn_and_responsibility.html> "The Internet, in the words of ... John Gilmore, 'deals with censorship as though it were a malfunction and routes around it.'" Judith Lewis, *Why Johnny Can't Surf*, LA Weekly, Feb. 21, 1997, at 43. "[I]t's not easy to push standards of decency

on a network that, as ... John Gilmore put it (though even he can't remember where), treats censorship as damage and routes around it."

5. *See generally*, Todd Flaming, *An Introduction to the Internet*, 83 Ill. B.J., 311, (1995); Joshua Eddings, How the Internet Works 13 (1994); Bruce Sterling, Short History of the Internet (Feb. 1993), (available at <gopher:// gopher.isoc.org:70/00/Internet/history/short.history.of.Internet>).For background information on Internet legal issues, *see generally* Lawrence Lessig, *The Zones Of Cyberspace*, 48 Stan. L. Rev. 1403 (May 1996),*The Path Of Cyberlaw* 104 Yale L.J. 1743 (May 1995), David R. Johnson & David Post, *Law And Borders--the Rise Of Law In Cyberspace* 48 Stan. L. Rev. 1367 (May 1996). For a recent article dealing with some of the issues discussed here and arguing that individual network systems often can and should become the regulators, see David R. Johnson & David G. Post, And How Shall the Net Be Governed? A Meditation on the Relative Virtues of Decentralized, Emergent Law (visited June 24, 1997) <http://www.cli.org/emdraft.html>

6. John Perry Barlow, Leaving the Physical World (visited June 24, 1997) <http://www.eff.org/pub/Publications/John_Perry_Barlow/HTML/leaving_the_physical_world.html>(discussing the inapplicability of physical-world standards in Cyberspace).

7. One of the strongest statements of his position comes in the manifesto he co-authored with a number of other prominent members of the digerati. "Unlike the mass knowledge of the Second Wave -- public good knowledge that was useful to everyone because most people's information needs were standardized -- Third Wave customized knowledge is by nature a private good. If this analysis is correct, *copyright and patent protection of knowledge (or at least many forms of it) may no longer be necessary*. In fact, the marketplace may already be creating vehicles to compensate creators of customized knowledge outside the cumbersome copyright/ patent process, as suggested by John Perry Barlow." George Gilder, Esther Dyson, Jay Keyworth, Alvin Toffler, *A Magna Carta for the Knowledge Age*, 11 New Perspectives Quarterly 26 (1994) (emphasis added).

8. Huber, in fact, has taken a direct shot at the notion that "information wants to be free." *See* Peter Huber, *Tangled Wires: The Intellectual Confusion and Hypocrisy of the Wired Crowd*, Slate, Oct. 18, 1996 at <http://www.slate.com/Features/TangledWires/TangledWires.asp>. Huber labels the intellectual property rights skeptics as hypocrites whose real attitude is merely a desire for liberal redistribution of everyone else's stuff. His views are frankly dismissive; he is criticising a group of people, some of whom have argued in favour of maintaining the existing intellectual property rules in cyberspace and others of whom have argued that reliance on rules rather than technological innovation would actually inhibit the operation of capitalism online. Yet his description of this "Wired Crowd," many of whom make Ayn Rand sound like Vladimir Ilyich, is that their position is that of a hypocritical New Dealer -- "My property is mine; yours is for sharing." *Id.* Wired, we are supposed to believe, is the Economic and Philosophical Manuscripts in cyberspace. (Would that it were true! In fact, Wired's ideal of scathing social commentary is to claim that someone's computer is out of date.) Huber seeks to restore normative appeal to intellectual property by arguing that it "is just a commercial form of privacy law. Indeed for some, it's the only kind of privacy they still own." This powerful argument suffers a little from the

example that follows. "Madonna can no longer stop you from gazing at her breasts. Copyright at least makes you pay for the pleasure." *Id.* Our sympathies are with her.. (and with him if this is the best illustration that comes to mind.) Stopping the world from gazing at her breasts has never seemed to be particularly high on Madonna's list of priorities -- at least as a matter of "privacy." True, Madonna might prefer a legal regime which would allow her to wring the maximum commercial advantage in every market for images of her and references to her -- for example by making people like Huber pay if they wished to use her as an example, restricting the fair use privilege, limiting news reporting and biography to authorized images and so on. Yet it is not clear why this desire, in itself, makes the notion of such a regime normatively compelling as a matter of social policy. There is also a danger in labelling critics of extensive intellectual property rights "anti-privacy." If there is a "privacy" interest consisting solely in the extraction of the maximum rent for one's intellectual property, then was the Justice Department's investigation of Microsoft's allegedly anti-competitive practices an attempt to cut down on Bill Gates' "privacy" interest in Windows 95? Or are we referring simply to spin-off effects in a particular case? Are Federal automobile emissions standards "anti-privacy"if they make it harder for me to leave the paparazzi in the dust? Intellectual property *can* be used to preserve privacy and I have used a stout and WASP-y pair of wingtips to hammer in a nail; this does not mean that the manufacturers of Birkenstock sandals are "anti-carpentry." There are indeed profound and interesting linkages and tensions between property and privacy, and this point has been made for some time. *Compare* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 113 (1890). *with* Michael Madow, *Private Ownership of Public Image: Popular Culture and Publicity Rights*, 81 Cal. L. Rev. 127 (Jan. 1993). Yet, as these articles both show, intellectual property most definitely is not "*just* a commercial form of privacy law."

9. *See generally* Information Infrastructure Task Force, Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights (Sept. 1995)

10. *See* James Boyle, *Intellectual Property Policy On-Line: A Young Person's Guide*, 10 Harv. J.L. & Tech. 47, 52 (1996)

11. John Perry Barlow, *Selling Wine Without Bottles: The Economy of Mind on the Global Net*, Wired 2.03 (1993) at 86 (visited Jun. 24, 1997)

<http://www.eff.org/pub/Publications/John_Perry_Barlow/HTML/idea_economy_article.html> (quoting 13 The Writings of Thomas Jefferson 333-34 (Albert E. Bergh ed., 1907) (letter from Jefferson to Isaac McPherson, Aug. 13, 1813)).

12. John Perry Barlow, *Selling Wine Without Bottles: The Economy of Mind on the Global Net*, (visited Jun. 24, 1997)

<http://www.eff.org/pub/Publications/John_Perry_Barlow/HTML/idea_economy_article.html>

13. Global, lightspeed mobility of *labour* is not something that Adam Smith had contemplated; is it a quantitative or a qualitative distinction?

14. *See* James Boyle, Shamans, Software and Spleens: Law and the Construction of the Information Society at 182-83 (Harvard University Press 1996) "To someone like me, who believes a lot of our social ills come from the restriction of egalitarian norms, [the] fact [that our current ideas about information have strong egalitarian underpinnings] has an optimistic ring." *See also* Eugene Volokh, *Cheap Speech and What It Will Do*, 104 Yale L.J. 1805, 1847 (May 1995) "[T]he Supreme Court has based its jurisprudence on an idealized view of the world, a view that doesn't quite correspond to the world in which we live.... [T]his idealized world ... is much closer to the electronic media world of the future than it is to the print and broadcast media world of the present. If my predictions are right, the new technologies will make it much easier for all ideas, whether backed by the rich or the poor, to participate in the marketplace. ... [D]uring the print age, the Supreme Court created a First Amendment for the electronic age. The fictions the Court found necessary to embrace are turning, at least in part, into fact."

15. John Austin, The Province Of Jurisprudence Determined (H.L.A. Hart ed. 1954) *See also* James Boyle, *Thomas Hobbes and the Invented Tradition of Positivism: Reflections on Language, Power, and Essentialism*, 135 U. Pa. L. Rev. 383 (Jan. 1987).

16. One of the reasons for this may be the overwhelmingly libertarian cast to Internet politics in the United States. Libertarians tend to concentrate on state power rather than private power, they tend to focus on the obvious restraints on freedom imposed by criminal law's impact against the citizen, rather than the subtler restraints imposed by the rules constituting and structuring market and other relationships. Both ideas 'fit' the Austinian image. By making a criminal statute the paradigm of the *exercise* of state power, and the citizen's right against the government the paradigm of its *limitation*, the libertarian codes his normative ideas about political problems and solutions into the very image of law itself.

17. "You will recall my work here, such as it has been ... None of it does more than mark time. Repetitive and disconnected, it advances nowhere. Since indeed it never ceases to say the same thing, it perhaps says nothing. It is tangled up into an indecipherable, disorganised muddle. In a nutshell, it is inconclusive. Still, I could claim that after all these were only trails to be followed, it mattered little where they led; indeed, it was important that they did not have a predetermined starting point and destination. They were merely lines laid down for you to pursue or to divert elsewhere, or re-design as the case might be. They are, in the final analysis, just fragments, and it is up to you or me to see what we can make of them. For my part, it has struck me that I might have seemed a bit like a whale that leaps to the surface of the water disturbing it momentarily with a tiny jet of spray and lets it be believed, or pretends to believe, or wants to believe, or himself does in fact believe, that down in the depths where no one sees him any more, where he is no longer witnessed nor controlled by anyone, he follows a more profound, coherent and reasoned trajectory. Well, anyway, that was more or less how I at least conceived the situation; it could be that you perceived it differently." Michel Foucault, Two Lectures, *in* Michael Foucault, Power/Knowledge: Selected Interviews and Other Writings, 1972-1977, 78-79 (Colin

Gordon ed. & Colin Gordon et al. trans., 1980).

18. *What Is an Author?*, in Textual Strategies: Perspectives In Post-Structuralist Criticism 141 (Josue V. Harari ed., 1979), Discipline and Punish: The Birth of the Prison (Alan Sheridan ed. & trans., 1979)

19. *See, e.g.*, Richard Posner, Sex and Reason at 23, 182 (Harv. Univ. Press 1992) (describing Foucault's writings on sexuality as "remarkable" and "eloquent").

20. Michel Foucault, Discipline and Punish: The Birth of the Prison (Alan Sheridan ed. & trans., 1979)

21. Janet Semple, Bentham's Prison: A Study of the Panopticon Penitentiary (1993); The two writers to have used Foucault's ideas most notably in the legal privacy and cyberspace context are J.M. Balkin, *What is a Postmodern Constitutionalism?* 90 Mich. L. Rev. 1966, 1987 (1992) and Larry Lessig, *Reading the Constitution in Cyberspace*, 45 Emory L. J. 869, 895 (Summer 1996) (citing Michel Foucault, Discipline and Punish: The Birth of the Prison at 139-40 (Alan Sheridan ed. & trans., 1979)).

22. In many ways, Foucault himself was most interested in a portion of this analysis that I shall pursue here only episodically. In a series of works on the treatment of insanity and on penology he argued that the emergence of the academic and intellectual "disciplines" as we know them now is reciprocally linked in important ways to this minute and quotidian regulation of behaviour. At the same time, retrofitting some of his earlier work on the human sciences into this new theoretical mold, he suggested that our conception of "an individual" was not some naturally occurring fact of nature from which analyses could begin, but instead, in part, a result of the concatenation of discipline and surveillance. Elsewhere I have explored the connections between power and knowledge (James Boyle, *The Politics of Reason: Critical Legal Theory and Local Social Thought*, 133 U. Pa. L. Rev. 685 (April 1995)), and the effects of the construction of subjectivity (James Boyle, *Is Subjectivity Possible? The Postmodern Subject in Legal Theory*, 62 U. Co. L. Rev. 489 (1991)). While there are interesting things to be said about the construction of subjectivity in cyberspace, my goal here is more mundane.

23. Michel Foucault, Two Lectures, *in* Michael Foucault, Power/Knowledge: Selected Interviews and Other Writings, 1972-1977, 78, 105 (Colin Gordon ed. & Colin Gordon et al. trans., 1980).

24. The best, and often the only, chronicler of the role of hard and softwired regimes is Lawrence Lessig. "I don't take issue with the values inherent in any one particular system of code. My criticism is directed against those who think about cyber regulation solely in terms of "law." Laws affect the pace of technologicalchange, but the strictures of software can do even more to curtail freedom. In the long run, the shackles built by programmers may well constrain us most." Cyber Rights Now: Tyranny in the Infrastructure Wired 5:07 (June 1997) http://wwww.wired.com/wired/5.07/crn/index.html *See also* Lawrence Lessig, The Zones of Cyberspace 48 Stan. L. Rev. 1403, 1408. " In the well implemented system, there is no civil disobedience. Law as code is a start to the perfect technology of justice."

25. Compare 47 U.S.C. §223(a)(1)(A)(ii) "obscene, lewd, lascivious, filthy, or indecent" with §223(a)(1)

(B)(ii) "obscene or indecent" and §223(d)(1)(B) "in terms patently offensive as measured by contemporary community standards." None of these terms are defined and it is not clear that they are intended to be distinct from each other. The Telecommunications Act of 1996, Pub. L. No. 104-104, tit. V, §§ 501- 61, 110 Stat. 56 (1996). With some reservations the lower courts treated both phrases as equivalent to "indecency" as defined in Pacifica (FCC v. Pacifica Foundation, 438 U.S. 726 (1978)). The Supreme Court was less willing to waive away the statute's internal inconsistencies. "Regardless of whether the CDA is so vague that it violates the Fifth Amendment, the many ambiguities concerning the scope of its coverage render it problematic for purposes of the First Amendment. For instance, each of the two parts of the CDA uses a different linguistic form. The first uses the word "indecent," 47 U. S. C. A. §223(a) (Supp. 1997), while the second speaks of material that "in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs," §223(d). Given the absence of a definition of either term, this difference in language will provoke uncertainty among speakers about how the two standards relate to each other and just what they mean." Reno v. ACLU, No. 96-511, WL 348012 (U.S. June 26, 1997). Perhaps in desperation, the government's strategy in the case was to argue that the Act was intended to regulate only "commercial pornography" - a phrase that appears nowhere within it. This argument was rejected both in the three judge panel below, ACLU v. Reno, 929 F. Supp. 824, 854-55 (E.D. Pa. 1996), and in the Supreme Court; Reno v. ACLU at __.

26. *See* ACLU, 929 F. Supp. 824 (E.D. Pa. 1996). In striking down the CDA, the District Court held that "[j]ust as the strength of the Internet is chaos, so the strength of our liberty depends upon the chaos and cacophony of the unfettered speech the First Amendment protects. For these reasons, I without hesitation hold that the CDA is unconstitutional on its face." *Id.* at 883 (Dalzel, J., concurring).

27. Reno v. ACLU, No. 96-511, WL 348012 (U.S. June 26, 1997).

28. ACLU v. Reno, 929 F.Supp. 824, 832 (E.D. Pa. 1996).. (discussing findings of fact) "There is no centralized storage location, control point, or communications channel for the Internet, and it would not be technically feasible for a single entity to control all of the information conveyed on the Internet."

*But cf.* Chief Justice Rehnquist's question during oral arguments (visited Jun. 24, 1997) <http://www.aclu.org/issues/cyber/trial/sctran.html>"But if 70 percent [of indecent speech on the Internet] is shielded and 30 percent isn't, what kind of an argument is that against the constitutionality of the statute?"

29. Charles Nesson & David Marglin, *The Day the Internet Met the First Amendment: Time and the Communications Decency Act*, 10 Harv. J.L. & Tech. 113, 115 (Fall 1996).

30. Butler v. Michigan, 352 U.S. 380, 383 (1957), *quoted in* Sable Communications v. FCC, 492 U.S. 115, 127.

31. The Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996) (to be codified at 47 U.S.C. §223(e)(5)(A)).

32. The Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996) (to be codified at 47 U.S.C. §223(e)(5)(B)).

33. The Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996) (to be codified at 47 U.S.C. §223(e)(5)(A)).

**(5)** It is a defense to a prosecution under subsection (a)(1)(B) or (d) of this section, or under subsection (a)(2) of this section with respect to the use of a facility for an activity under subsection (a)(1)(B) of this section that a person--

**(A)** has taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to a communication specified in such subsections, which may involve any appropriate measures to restrict minors from such communications, including any method which is feasible under available technology;

34. *See* Paul Resnick and Jim Miller, *The CDA's Silver Lining*, Wired (1996) vol. 4(8) at 109.

35. *See generally* Albert Vezza, *Platform for Internet Content Selection: What Does It Do?* (visited Jun. 24, 1997) <http://www.w3.org/PICS/951030/AV/StartHere.html> For a critique of PICS see Lessig *Cyber Rights Now: Tyranny in the Infrastructure supra* note 24.

36. First party rating is rating provided by the person posting the information. Third party rating is rating provided by some other entity. World Wide Web Consortium, *PICS Statement of Principles* (visited Jun. 24, 1997) <http://www.w3.org/PICS/principles.html>

37. See Owen M. Fiss, *Free Speech and Social Structure*, 71 Iowa L. Rev. 1405, 1424-25, ("Today abolition of the fairness doctrine can be passed off as just one more instance of 'deregulation.' It seems to me, however, that there is much to regret in this stance of the Court and the [First Amendment] Tradition upon which it rests. The received Tradition presupposes a world that no longer exists and that is beyond our capacity to recall--a world in which the principal political forum is the street corner."), Liberalism Divided (Westview Press 1996), J.M. Balkin, *Some Realism About Pluralism: Legal Realist Approaches to the First Amendment*, 1990 Duke L.J. 375 (1990) ("In assessing what constitutes substantial overbreadth or vagueness, I do not think it inappropriate to employ common sense judgments about the way the world works. Although the distinction between public power and private power is significant, even more significant for me are what power relations (public or private) exist in the standard case in which the statute operates."), Richard Delgado, *First Amendment Formalism Is Giving Way to First Amendment Legal Realism*, 29 Harv. C.R.-C.L. L. Rev. 169 (Winter 1994) ("The transition to the new [legal realist] paradigm is, however, far from complete."). *But cf.* Steven G. Gey, *The Case Against Postmodern Censorship Theory*, 145 U. Pa. L. Rev. 193, 195-97 (Dec. 1996) ("The theoretical advances celebrated by Delgado and other progressive critics of the First Amendment are not really advances at all. They are simply refurbished versions of arguments used since the beginning of modern

First Amendment jurisprudence to justify government authority to control the speech (and thought) of citizens. ... Moreover, despite the different objectives of the new censors, their reasons for supporting government control over speech are not significantly different from those of their reactionary predecessors. ... The postmodern censorship theory offered by this new generation of politically progressive legal scholars is neither progressive nor, for that matter, even "postmodern." In the end, it is just censorship.")

38. *See generally* Kathryn Munro, *Filtering Utilities*, PC Magazine, Vol. 16, No. 7 (Apr. 8, 1997) at 235 (describing and reviewing various filtering software products).

39. For a fuller version of this argument, *see* James Boyle et al., *Before the Supreme Un-Court of the United States* (visited Jun. 24, 1997)

<http://www.wcl.american.edu/pub/faculty/boyle/unreno.htm> (Justice Un-Scalia, dissenting)

40. "Despite this progress, the transformation of cyberspace is not complete. Although gateway technology has been available on the World Wide Web for some time now, id., at 845; Shea v. Reno, 930 F. Supp. 916, 933-934 (SDNY 1996), it is not available to all Web speakers, 929 F. Supp., at 845-846, and is just now becoming technologically feasible for chat rooms and USENETnewsgroups, Brief for Federal Parties 37-38. Gateway technology is not ubiquitous in cyberspace, and because without it "there is no means of age verification," cyberspace still remains largely unzoned--and unzoneable. 929 F. Supp., at 846; Shea, supra, at 934. User based zoning is also in its infancy. For it to be effective, (i) an agreed upon code (or "tag") would have to exist; (ii) screening software or browsers with screening capabilities would have to be able to recognize the "tag"; and (iii) those programs would have to be widely available--and widely used--by Internet users. At present, none of these conditions is true. Screening software "is not in wide use today" and "only a handful of browsers have screening capabilities." Shea, supra, at 945-946. There is, moreover, no agreed upon "tag" for those programs to recognize. 929 F. Supp., at 848; Shea, supra, at 945." Reno v. ACLU, No. 96-511, WL 348012 at 24 (U. S. June 26, 1997) (O'Connor, J., concurring in part and dissenting in part).

41. Remarks by President Clinton at Town Hall meeting in Bridgeport, W. Va. (May 22, 1997) "[I]t may be that what we have to do is to try to develop something like the equivalent of what we are developing for you for television, like the V-chip ... It's technically more difficult with the Internet. ... But I think that is the answer; something like the V-chip for televisions, and we are working on it."

42. *See, e.g.*, Ed Markey, Empowerment Act (Fed. Doc. Clearing House 1997) (press release June 19, 1997).

43. Declan McCullagh and Brock Meeks, *Keys to the Kingdom* (visited Jun. 24, 1997) <http://www.eff.org/pub/Publications/Declan_McCullagh/cwd.keys.to.the.kingdom.0796.article>

44. See supra note

45. Geeta Anand, *Library OK's limits on 'Net access; Compromise calls for filter software only on computers used by children*, Boston Globe, Mar. 22, 1997, at A1.

46. Marc Ferranti, *Site-filtering issue goes to state level*, InfoWorld, Apr. 21, 1997, at 60.

47. Ed Markey, Empowerment Act (Fed. Doc. Clearing House 1997) (press release June 19, 1997).

48. With a cavalier disregard for the problems that this raises for my thesis, some of the best investigative reporting on, and discussion of, the politics of private technological censorship has been done by the cyber journalist Declan McCullagh and his "Fight Censorship" discussion list. (*See* Meeks & McCullagh, *Keys to the Kingdom,* supra note __.) In one sense, this raises the issue that I discussed earlier -- the politics of the Net are up for grabs and the conventional categories of political ideology and theory are much more mutable there.

49. "Although many people were surprised at [the revelations in the McCullagh and Meeks article], it was in fact completely predictable from a historical perspective. Too much discussion of the future of unfettered electronic communications takes place in a social vacuum, from an extremely simplistic viewpoint (I refer to this the "net.libertarian" mindset). Because of a perspective that might be rendered "government action bad, private action good" there's great unwillingness to think about complicated social systems, of private parties acting as as agents of censorship." Seth Finkelstein, *Internet Blocking Programs and Privatized Censorship*, The Ethical Spectacle, August 1996 <http://www.spectacle.org/896/finkel.html>

50. *See* James Boyle, *Intellectual Property Online: A Young Person's Guide*, 10 Harv. J. L. & Tech. 47 (1996); James Boyle, Shamans, Software, and Spleens 18-20, 51-61, 162-63 (1996); James Boyle, *Q: Is Congress turning the Internet into an information toll road? Yes: The Senate would whack away at 'fair use' of electronic documents needed for news and education*, Insight, Jan. 15, 1996; James Boyle, *Sold Out* N.Y. Times, March 31, 1996, § 2, at 2.

51. *See* Nicholas Negropronte, Being Digital (1995).

52. *See* John Perry Barlow, *Selling Wine Without Bottles: The Economy of Mind on the Global Net*,

<http://www.eff.org/pub/Publications/John_Perry_Barlow/HTML/idea_economy_ article.html>

53. United States Department of Commerce, Information Infrastructure Task Force, Intellectual Property and the National Information Infrastructure: the Report of the Working Group on Intellectual Property Rights at 114-24 (Sept 1995) ("White Paper"); James Boyle, *Intellectual Property Online: A Young Person's Guide*, 10 Harv. J. L. & Tech. 47, 58-111 (1996); Niva Elkin-Koren, *Copyright Law and Social Dialogue on the Information Superhighway: The Case Against Copyright Liability of Bulletin Board Operators*, 13 Cardozo Arts & Ent. L. J. 345 (1995); *Cf., Religious Technology Center v. Netcom*, 907 F.

Supp. 1361, 1377 (N.D. Calif. 1995) (stating that strict liability for ISPs "would chill the use of the Internet because every access provider or user would be subject to liability when a user posts an infringing work to a Usenet newsgroup." *Id.* at 1377).

54. *See* NII Copyright Protection Act of 1995, S. 1284, 104th Cong. (1995), H.R. 2441, 104th Cong. (1995).

55. *See* WIPO Copyright Treaty, Dec. 23, 1996, CRNR/DC/94 (visited June 26, 1997) <http://www.wipo.org/eng/diplconf/distrib/94dc.htm>; *See also, News from WIPO* (visited June 26, 1997) <http://www.hrrc.org/wiponews.html> (detailing course of deliberations during the Diplomatic Conference).

56. *See* James Boyle, *Intellectual Property Online: A Young Person's Guide,* 10 Harv. J. L. & Tech. 47, 830194 (1996) (discussing MAI Systems Corp. v. Peak Computer, Inc., 991 F.2d 511 (9th Cir.1993)).

57. *Id.* at 103-04.

58. *See* Religious Technology Center v. Netcom, 907 F. Supp. 1361 (N.D. Calif. 1995); *See also,* Playboy Enterprises, Inc. v. Chuckleberry Publications, Inc., 939 F. Supp. 1032 (1996); Sega Enterprises, Ltd. v. Maphia, 948 F. Supp. 923 (1996);

59. We impose strict liability on manufacturers on products for a number of reasons -- one of which is that we believe the state could not possibly inspect every product and every design in the market-place. Simply by forcing manufacturers to internalise the costs of injuries caused by their products, we produce a strong, private set of incentives that in turn encourage internal mechanisms of review and product redesign. *See* Guido Calabresi, The Cost of Accidents: A Legal and Economic Analysis (1970); *See also,* Guido Calabresi, *First Party, Third Party, and Product Liability Systems: Can Economic Analysis of Law Tell Us Anything About Them?*, 69 Iowa L. Rev. 833 (1984); A. Mitchell Polinsky, An Introduction to Law and Economics at 97-106 (2d ed. 1989). Plaintiffs become private attorneys-general. There are however, also some striking differences between the familiar example of the use of strict liability in the tort setting and the imposition of strict liability on internet service providers. In product liability, the conventional range of reasons for imposing strict liability on the manufacturers includes the claims that:

They are generally the cheapest cost-avoiders -- in other words, they are best able to respond to liability for damage by making changes that could prevent the damage

They are generally the best loss spreaders -- in other words, they are best able to pass the cost of unavoidable or cost-justified damage on to the appropriate group, consumers of the good in question.

They are generally in an advantageous position in terms of knowledge and effective power -- at least as compared to the relatively powerless individual consumer. *See* Escola v. Coca Cola Bottling Co., 150 P.2d 436, 440-43 (1944) (Traynor, J., concurring).

In the online setting, none of these claims is obviously correct. In some cases service providers may be able to prevent illicit copying relatively cheaply without imposing large social costs. On many other occasions however, it seems that the costs of their enforcement may outweigh the benefits -- in the form of transaction costs required to ensure compliance, for example, or draconian restrictions of the fair use privileges of their subscribers so as to be sure that illicit copying is not being carried on. (Since ISP's would pay for all detected copyright infringements, but would not be forced to internalise the cost to their customers of restricting fair use, the incentives would be asymmetrically anti-consumer.) Leaving aside the efficiency costs of enforcement by service providers, there is also the question of whether they are the cheapest cost-avoider. In many cases, the party best situated to avoid the cost of copyright infringement will be the owner of the copyright. Whether by developing technical solutions or by fine-tuning their business plan so as to minimise the incentives to violate copyright in the first place, copyright owners might well be the cheapest cost-avoiders. If that is true, it would actually be inefficient to allow them to rely on another party for enforcement of their rights.

Beyond the question of the cheapest cost-avoider is the question of best loss spreader and here too it is hard to be confident that the ISP's are the appropriate parties. The economic analysts' mantra is "activities should internalise their full costs." If the costs of a good or activity are not passed on to those who use the good or engage in the activity, then those individuals will make inefficient choices. Thus, for example, if the price of gasoline does not reflect the environmental damage done by gasoline, that damage becomes a negative externality, and gasoline is inefficiently priced relative to its "true" costs. Over what group then, should the costs -- i.e. the copyright owner's forgone profit -- of illicit copying be imposed? The inquiry is a fascinating one, with more layers than I can fully explore here. It is complicated by the fact that the "costs" imposed by the illicit copying of an information good are economically different in some ways from the costs imposed by theft of material goods. As a content provider, I can make a rational economic decision to sell my good across some cheap but "leaky" medium, which lowers my costs of advertising and distribution and increases the number of unauthorised copies circulating. I may even believe that some of the unauthorised copies provide a *benefit* to me -- making my word processing program a de facto standard in the industry or establishing my band as the best known, thus increasing the market for future products. But let us leave aside the joys of pointing out that economic analysis depends on questions of interpretation that cannot themselves be decided according to economic criteria. There is at the very least, strong reason to doubt that users of on-line services, rather than purchasers of the good in question, are the appropriate group over whom the costs of illicit copying should be spread. This would, in fact, actively undermine the competitive incentives to companies to develop their own anti-copying methods.

Finally, the asymmetry of power and knowledge that occurs when Mrs. McPherson confronts the Buick Motor Company, is by no means as clear when Microsoft wants Netcom to do its enforcement work. For all of these reasons, the imposition of strict liability on ISP's does look rather different than its imposition on manufacturers of defective products. If there is an advantage to this scheme, that advantage redounds mainly to the content providers; such a plan would shift enforcement costs from owners and allow them to reap the benefits of the Net without fully bearing its costs.

60. *See* 2 John Austin, Lectures on Jurisprudence 136 (5th ed. 1885)

61. *See infra* note ___.

62. *See* WIPO Copyright Treaty, Dec. 23, 1996, CRNR/DC/94 (visited June 26, 1997) <http://www.wipo.org/eng/diplconf/distrib/94dc.htm>; *See also, News from WIPO* (visited June 26, 1997) <http://www.hrrc.org/wiponews.html> (detailing course of deliberations during the Diplomatic Conference).

63. *See supra* note 52 at § 1201.

64. *See supra* note 52 at § 1204.

65. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996).

66. See, Kristin S. Burns, *Protecting the Child: The V-Chip Provisions of the Telecommunications Act of 1996*, 7 Depaul-Lca J. Arts & Ent. L. 143 (1996); David V. Scott, *The V-Chip Debate: Blocking Television Sex, Violence, and the First Amendment*, 16 Loy. L.A. Ent. L. J. 741 (1996).

67. *See* Howard S. Dakoff, *The Clipper Chip Proposal: Deciphering the Unfounded Fears that are Wrongfully Derailing its Implementation*, 29 J. Marshiall L. Rev. 475, 482-84 (1996) (discussing the use of the government's purchasing power to create a de facto encryption system); *See also*, Richard L. Field, *1996: Survey of the Year's Developments in Electronic Cash Law and the Laws Affecting Electronic Banking in the United States*, 46 Am. U. L. Rev. 967, 993 (1997); Ira S. Rubenstein, *Export Controls on Encryption Software* 748 PLI/Comm 309 (1996); A. Michael Froomkin, *The Metaphor is the Key, Cryptograpy, the Clipper Chip, and the Constitution,* 143 U. Pa. L. Rev. 709 (1995).

68. Pub. L. No. 103 - 414, 108 Stat. 4279 (1994) (codified at 47 U.S.C.A. s 1001 -10 (Supp. 1995)

69. 18 U.S.C. s 2703(c)(1)(C) (1994). See Susan Friewald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act,* 69 S. CAL. L. REV. 949 (1996).

70. 17 U.S.C. §§ 1001-1010 (1994).

71. Ithièl de Sola Pool, Technologies of Freedom (Harv. Univ. Press 1983).

72. See Lessig, *Cyber Rights Now: Tyranny in the Infrastructure supra* note 24.