Law Regulating Code Regulating Law

Citation

Lawrence Lessig, Law Regulating Code Regulating Law, 35 Loy. U. Chi. L. J. 1 (2003).

Published Version

http://lawecommons.luc.edu/luclj/vol35/iss1/2/

Permanent link

http://nrs.harvard.edu/urn-3:HUL.InstRepos:12912675

Terms of Use

Share Your Story

Law Regulating Code Regulating Law

Lawrence Lessig
Stanford Law School

Law Regulating Code Regulating Law

Lawrence Lessig*

Since lawyers have been thinking about cyberspace, there has been a debate about whether there is a law of cyberspace. Judge Frank Easterbrook famously said there was not. More accurately, he said legal academics should not speak as if there were, since the "best way to learn the law applicable to specialized endeavors is to study general rules."[1]

I have been a skeptic of Judge Easterbrook's skepticism.[2] Professor Orin Kerr has been a skeptic as well, though for different reasons. Professor Kerr believes there is something special about the law of cyberspace because there is a particularly difficult question of "perspective" in the law of cyberspace.[3] I agree, but I also believe there is a particularly difficult and general question that the law of cyberspace raises about how law and technology interact. Just as the law and economics movement taught lawyers that understanding the interaction between rules and economic incentives was essential if regulations were to have their intended effect, so too does cyberlaw teach that an understanding of the interaction between rules and technical structures is essential if regulations are to have their intended effect.

---

1. Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 209 (analyzing a statement made by the former Dean of the University of Chicago, Gerhard Casper, who said that his law school's curriculum encompassed the entire law).

2. Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 502 (1999).

3. Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357, 362–63 (2003) (explaining that the analysis of cyberlaw issues can produce very different results depending on whether one views them from the perspective of Internet users, who experience the Internet as a series of "virtual reality" abstractions that include activities such as chat, e-mail, and shopping, or from an external perspective, focusing on the physical makeup and hardware of the Internet and its place within the material world). "In a surprising number of situations, we arrive at one result when applying law from an internal perspective and a different result when applying law from an external perspective." *Id.* at 357.

The aim of this short essay is to continue that claim. I describe two types of cases where we can learn something about law in general from the interaction between law and technology in particular.

Not-Too-Much-But-Not-Too-Little Goods

Some say you cannot have too much of a good thing. That is not quite true. There are some things that are good things, which means we are better off with them than without them. But for some of these good things, more is not necessarily better. For these good things, there can be too much of a good thing.

Two examples of this kind of good are intellectual property and privacy.

Intellectual property is clearly a good. No modern society can flourish unless it accords at least some protection for creative work. No doubt, not all societies have done so. Our society, for example, did not protect foreign copyrights for the first 100 years of the Republic. But we, and most modern nations, are beyond that stage now. Most modern nations give creators some amount of exclusive protection for their creative work.

But as our tradition attests, and economists confirm, just because some intellectual property is good, it does not follow that more intellectual property is better. More precisely, just because some protection is good, it doesn't follow that increasing that protection is better. Too much intellectual property protection can stifle follow-on innovation. As Judge Richard Posner puts it:

> An expansion of copyright protection might . . . reduce the output of literature . . . by increasing the royalty expense of writers. The works of previous writers are inputs into current work, and these inputs get more expensive the more those earlier works are protected by copyright. . . . Thus writers themselves might as a group prefer less copyright protection in order to reduce the cost to them of writing their own works, even though it would mean forgoing some income from the sale of those works because they would be less fully protected against copying.[4]

The aim of policymakers therefore must be to strike a balance—to ensure that society secures to creators some protection for their creative work while also ensuring that that protection does not reach too far.

Privacy evinces the same need for balance. Every free society believes that there is some realm of individual life that should be free of

---

surveillance or invasion. The strong form of this view claims that this realm is beyond government regulation.[5] The weaker form would assert that this realm at least should be free presumptively from state control. In either view, privacy is a good because it insulates the individual from improper control.

But no one believes that individuals have an absolute right of privacy. A bank has a legitimate claim to know whether I have defrauded other lenders before. My dean has a legitimate claim to know whether I in fact graduated from law school. Fraud at a minimum limits the legitimate claims to privacy. And many believe that minimum is much thicker than just fraud.

Here too, then, policymakers must seek a balance. Their aim must be to guarantee enough privacy to ensure the flourishing of a free society. But they must also make sure that individuals don't have too much privacy, if the public benefits of information are not to be defeated. Again, as Judge Posner describes:

> The strongest defenders of privacy usually define the individual's right to privacy as the right to control the flow of information about him . . . .
>
> . . . .
>
> To the extent that personal information is concealed in order to mislead, the case for giving it legal protection is . . . weak. Protection would simply increase transaction costs, much as if we permitted fraud in the sale of goods.[6]

So how do policymakers achieve this balance? What factors should they consider?

From the traditional perspective of legal science, the only factors that get considered are those directly tied to regulation. We "balance" the protections for intellectual property by considering the sum of statutory and common-law protections. We evaluate the protections of privacy by considering those same protections, as well as the constitutional perspective. Policymaking from this perspective is simply the process

---

5. *See, e.g.*, Lawrence v. Texas, 123 S. Ct. 2472, 2475 (2003). Justice Kennedy wrote:
    Liberty protects the person from unwarranted government intrusions into a dwelling or other private places. In our tradition the State is not omnipresent in the home. And there are other spheres of our lives and existence, outside the home, where the State should not be a dominant presence. Freedom extends beyond spatial bounds. Liberty presumes an autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct.
Id.

6. Richard A. Posner, *An Economic Theory of Privacy*, REGULATION, May/June 1978, at 19, 20, 22.

of tuning legal code. And changes in policy, from this perspective, simply map changes in this legal code.

From the perspective of cyberlaw, however, policymaking cannot function focused on legal code alone. Policymaking instead requires a consideration of the interaction between this legal code and the architecture or technology within which this code functions. The protection of intellectual property is determined not just by the law that protects intellectual property but also by the technical infrastructure within which intellectual property exists.[7] Thus, before the spread of technologies to enable consumer peer-to-peer file sharing, the intellectual property on an audio CD was relatively well protected. After the rise of consumer peer-to-peer file sharing and peer-to-peer systems generally, that same intellectual property is protected relatively poorly. The change in protection is a change caused by changing technology. The law remains constant, but the effective policy protecting intellectual property is affected by a change in the technological context within which intellectual property exists.

The same point can be made about privacy. When the Internet was first deployed, its architecture produced relative anonymity for users of the Internet. The basic protocols did not identify who people were, where they came from, or what use they were making of the Internet. That information is not embedded in the basic Internet protocol, which means that the basic protocols protect the user from inadvertently revealing this information.

To those who valued the privacy effected by this initial architecture, this failure to provide data was a feature of the original Internet. But to some, this failure to provide data was a bug, not a feature. The inability to know who people were, or where they came from, made it impossible for the Internet to support certain kinds of transactions. It made it particularly hard for the government to monitor or track individual behavior.

---

7. *See, e.g.*, LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 122, 124 (1999) (discussing how changes in technology have affected the level of copy protection afforded to authors). As I've written before:

> Before the printing press . . . there was not much need to protect an author's copyright. Copying was so expensive that [the] nature itself protected that right. But as the cost of copying decreased, the threat to the author's control increased. As each generation has delivered a technology better than the last, the ability of the copyright holder to protect her intellectual property has been weakened.

Id.

The most obvious example of a transaction disabled by this early design of the network was basic Internet commerce. When the World Wide Web was first born, the basic protocol was "stateless." A server could not automatically keep track of who was accessing a web page. It couldn't know, for example, that I was the person who ordered 100 copies of Lessig's latest book when I moved from the order page to the check-out lane. Without a way to authenticate states, it would be impossible to keep track of purchases.

In 1995, the Netscape corporation fixed this. In version 2.0 of its browser, it released a protocol for the "cookies" technology. "Cookies" enable a web server to deposit a bit of code on a client's computer.[8] That code then identifies the browser to the server. Once identified, the server knows with whom it is dealing. And once it knows whom it is dealing with, it can serve that person according to the terms of any agreement.

As cookies became more prevalent, however, they had a more general effect on the Internet. Now it was easier for information about users of the Internet to become known. And this in turn meant it was easier to track who did what on the Internet.

Thus, as the ability to track increased, this meant that privacy on the Internet decreased. This decrease came not from law. This decrease came from a change in technology.

In both cases, my point so far is simply descriptive. The effective protection for intellectual property and privacy depends upon the sum of the protections from both law and technology. And likewise, the changes in protection for intellectual property and privacy depend upon both the changes in law and the changes in technology.

Yet this fairly obvious point seems lost on policymakers, at least policymakers keen on maintaining balance. Or alternatively, if the point is not lost on policymakers, then recent policy is a good sign that in neither context are policymakers interested in maintaining balance.

Consider the battles about intellectual property that currently rage among policymakers. We're currently in the middle of a copyright war, as the recording industry and Hollywood battle the Internet. This battle was engendered by the emergence of a digital network that, by consequence of its design, allowed the distribution of perfect copies of

---

8. *See generally* NETSCAPE, PERSISTENT CLIENT STATE HTTP COOKIES, *at* http://wp.netscape.com/newsref/std/cookie_spec.html (last visited Oct. 16, 2003) (describing how cookies work); *Netscape Navigator, in* WIKIPEDIA, *at* http://www.wikipedia.org/wiki/Netscape_Navigator (last modified Sept. 8, 2003) (explaining the development of Netscape).

digital content for free. That meant that it was increasingly difficult for content owners to control the distribution of their content. This in turn has inspired a reaction by content owners to reassert control, and hence, protection, of their content.

The reaction has been on two fronts—both legal and technical. First, the content industry pushed for changes in the law protecting copyright. These changes increased the legal protections securing content and extended the term under which content was protected. But in addition to these legal changes, technologists have been working on technical changes designed to correct, or counterbalance, the effect of the Internet's design.

These technical changes include an array of technologies designed to enable "trusted systems" for content. Trusted systems would facilitate the controlled distribution of protected content, counteracting the lack of control produced by the Internet. Examples of these technologies are many: encryption technologies to control the copying of CDs, digital-wrapper technologies to lock up content unless the user has the right key, etc. No single standard has yet to emerge, but the support for a strong system of trust is being deployed by Microsoft and others.

From a policy perspective, the question should be whether this change in technology, in response to a change in technology, reestablishes balance between protection of intellectual property and access to intellectual property. One way to answer that question is to ask whether the change preserves traditional limits on intellectual property. For example, will "fair use" continue in a world governed by "trusted systems," or will "fair use" be coded away by technologies that regulate access to copyrighted material?[9]

It is clear at least that technologies can be coded to remove traditional freedoms of fair use. An eBook reader, for example, can disable the ability to print a short selection from a book, even though printing a short selection from the book would plainly be considered fair use. Or

---

9. Eldred v. Ashcroft, 123 S. Ct. 769, 788–89 (2003). The Supreme Court said:

   In addition to spurring the creation and publication of new expression, copyright law contains built-in First Amendment accommodations.

   ... [T]he "fair use" defense allows the public to use not only facts and ideas contained in a copyrighted work, but also expression itself in certain circumstances. Codified at 17 U.S.C. § 107, the defense provides: "The fair use of a copyrighted work, including such use by reproduction in copies ... for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright." The fair use defense affords considerable "latitude for scholarship and comment," and even for parody.

   Id. (citations omitted).

the technology could be designed to disable the capacity to cut and paste from one document to another, as a way to control the ability to quote.

These controls come from the code, not from the law. Indeed, in most cases, they are controls that exceed any control that the law would otherwise allow. You couldn't claim a violation of the copyright if a user of your book Xeroxed three pages of your novel. But you could use these controls built into an eBook reader to effect exactly that kind of control. The code could thus remove a kind of access that the law would otherwise protect.

If balance were the objective of the policymakers tuning copyright law, then this ability to code away fair use should suggest a policy response to reinforce fair use. This response could either mandate that this code protect traditional fair use, or more generally, it could limit control beyond the control that the law otherwise imposes. Or the law could recognize affirmatively the right of users to "hack" code that interferes with access protected by the traditional limits of copyright law.

Yet the response of policymakers has been precisely the opposite. In 1998, Congress passed the Digital Millennium Copyright Act ("DMCA"),[10] which not only failed to recognize any affirmative right to gain access consistent with traditional limits of fair use, but affirmatively proscribed any effort to circumvent code protecting content.[11] The DMCA thus not only fails to balance the imbalance caused by changes in code; the DMCA plainly exacerbates it.

This failure of policymaking is either a product of the failure to account for both technology and law together, or it manifests a decision by policymakers (encouraged by content owners) to change the tradition of balance in copyright. Congress says it is not changing the balance of copyright law in the DMCA at least. The DMCA explicitly states "[n]othing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title."[12] But whatever it means to do, its effect is to weaken the balance

---

10. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 U.S.C, 28 U.S.C, and 35 U.S.C.).

11. 17 U.S.C. § 1201 (2000 & West Supp. 2003).

12. *Id.* § 1201(c)(1); *see also* H.R. REP. NO. 105-551, pt. 2 (1998) (discussing the DMCA and fair use considerations). The House Report states:

> The Committee considers it particularly important to ensure that the concept of fair use remains firmly established in the law. . . . H.R. 2281, as reported by the Committee on Commerce, fully respects and extends into the digital environment the bedrock

of copyright law. Rather than tuning a "not too much, not too little" value, the effect is to skew the protection toward the extreme.

The same dynamic exists in the context of privacy. As I described, the Internet initially secured a strong degree of privacy. When tied with encryption technologies, the privacy enabled was extraordinarily strong. This led the government initially to try to control encryption technologies. The government banned the export of strong encryption technologies and tried to push as a standard an encryption technology that would preserve a back door that government could use.[13]

These efforts at controlling encryption were flawed, but the government's motivation is understandable given the "not too much, not too little" character of privacy. The concern of the government was that privacy would be too strong; the response was to regulate technologies to remedy that concern. That particular response failed (fortunately). But regulating encryption was not the only way the government could alter the balance protecting privacy. While the government failed to restrict the means to encrypt, in fact the general encryption of content has not yet become common. Thus, the government could induce, or benefit from, other changes in technology designed to increase the identifiability of behavior in cyberspace. Some of these changes are the simple by-product of changes driven by commerce; others have a more direct connection to government policy.

The first of these changes I have already described—cookies technology. But cookies are not the end of the effective modifications of the original privacy of the Internet. Instead, there has been an explosion of technologies designed to identify who people are, where they come from, and what activity they are engaged in.

These changes, like the changes protecting copyrighted material, are also affected by the law. The requirement of jurisdiction-specific regulations has pushed the demand for technologies that map the physical location of a user with a specific jurisdiction. This, in turn,

---

principle of "balance" in American intellectual property law for the benefit of both copyright owners and users.

H.R. REP. NO. 105-551, pt. 2, at 26.

13. *See* Paul E. Proctor & Christian Byrnes, *The Politics of Cryptography*, PERFORMANCE COMPUTING, Oct. 1, 1999, at 25; John Schwartz, *Disputes on Electronic Message Encryption Take on New Urgency*, N.Y. TIMES, Sept. 25, 2001, at C1, *available at* LEXIS, News Library, The New York Times File; *Encryption: The Story So Far*, WASHINGTONPOST.COM, *at* http://www.washingtonpost.com/wp-srv/tech/analysis/encryption/background.htm (last updated Sept. 17, 1997); *see also* ELEC. PRIVACY INFO. CTR., CRYPTOGRAPHY POLICY, *at* http://www.epic.org/crypto (last visited Oct. 3, 2003) (providing information on encryption law proposals).

enables effective local zoning of content on the Internet according to local rules.[14]

A much more dramatic example is offered by the Patriot Act.[15] Under that Act, the government's authority to survey Internet activity has dramatically increased. The government may monitor surfing behavior of anyone upon a showing to a judge that the monitoring is "relevant" to an ongoing criminal investigation. So too the standard required of American intelligence agencies has been lowered. Those agencies have been granted new powers to engage in roving surveillance domestically as well.[16]

This increase in authority to monitor behavior takes advantage of the character of the Internet, which is to enable a vast amount of data gathering in a manner wholly invisible to the target of the monitoring. This shift in the technical architecture, tied to the shift in legal authority, makes the Internet a far more pervasive surveillance medium than any other in social life.

The point in both contexts is that policymakers must account for both law and technology in securing a balance for "not too much, and not too little" goods. That account must therefore rely upon a relatively subtle appreciation of technical architectures. The government seems attuned to this need in the context of surveillance; content holders are attuned to this need in the context of copyright. The only perspective that seems to have missed this need is the perspective defending a public domain.

These two extremes have converged in the latest battle in the copyright war. The Recording Industry Association of America

---

14. Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653, 688 (2003). Zittrain writes:

> The Internet's brilliant methodology of data routing—a flexible set of intermediaries functioning in tandem yet with little central coordination—offers multiple opportunities for control that are only now coming into focus for regulators. Such control cannot be accepted, even if initiated for substantively good intentions, without the most exacting of processes to avoid abuse, including a comprehensive framework where sovereigns' actions to block material are thoroughly documented and open to challenge. If carefully implemented and circumscribed, however, government mandated destination-based filtering stands the greatest chance of approximating the legal and practical frameworks by which sovereigns currently sanction illegal content apart from the Internet.

Id.

15. USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified in scattered sections of U.S.C.).

16. *See* ELEC. FRONTIER FOUND., EFF ANALYSIS OF THE PROVISIONS OF THE USA PATRIOT ACT THAT RELATE TO ONLINE ACTIVITIES, *at* http://www.eff.org/Privacy/ Surveillance/Terrorism//20011031_eff_usa_patriot_analysis.php (Oct. 31, 2001).

("RIAA") has recently launched a series of lawsuits against individuals who share content.[17] Yet these suits depend upon the increasing ability of Internet Service Providers ("ISPs") to identify users of different services. Thus, Verizon and other ISPs have been forced by subpoena to reveal the identity of customers whom the RIAA says use file-sharing networks.

Thus, a reality is slowly dawning upon many Internet users. There is no anonymity in cyberspace. Indeed, the legal system has driven commercial entities to a place where the behavior and use of the Internet is perpetually and effectively monitored. That may be good for some and bad for others. But it is a level of surveillance we have never before seen. Music fans of every generation since the cassette tape have shared music with each other. This is the first generation when that sharing has become punishable and traceable.

Some-Regulation-Better-Than-None Examples

A second class of cases in which the interaction between legal policy and technology matters we could call the "some regulation is better than no regulation" cases. In these cases, the failure to regulate has perverse consequences, even for the values thought to be served by the regulatory forbearance.

Two examples are pornography and spam. Both are examples of speech that many would like to filter, but that are not themselves illegal. When both began to become common on the Internet, there was a strong push to find ways to facilitate filtering.

In the context of pornography, the push initially manifested itself in the form of legislation. In 1996, Congress enacted the Communications Decency Act ("CDA"),[18] designed to ban the distribution of "indecent" material to minors.[19] That statute was obviously unconstitutional as

---

17. *See* Frank Ahrens, *Record Industry Sues 4 Students Running File-Sharing Networks*, WASHINGTONPOST.COM, *at* http://www.washingtonpost.com/wp-dyn/articles/A22370-2003 Apr3.html (Apr. 3, 2003); Jane Black, *Big Music: Win Some, Lose a Lot More?*, BUS. WK. ONLINE, *at* http://www.businessweek.com/technology/content/may2003/tc2003055_8073 _tc078.htm (May 5, 2003); *see also* Zack Rosen, $97,800,000,000, *at* http://www.ews.uiuc.edu/ ~zrosen/ (last visited Oct. 16, 2003) (providing information relating to the RIAA's 2003 suit against the four college students).

18. Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 133 (codified as amended in scattered sections of 18 and 47 U.S.C.).

19. *Id.* § 502 (codified at 47 U.S.C. § 223(a) (2000), *amended by* PROTECT Act, Pub. L. No. 108-21, § 603 (1)(B), 117 Stat. 687 (2003)).

     Whoever—

     . . . .

enacted, and the Supreme Court quickly struck the law down.[20] Congress then enacted the Child Online Protection Act ("COPA") in 1998, which tried to achieve the same end through more constitutional means.[21]

These legislative efforts to facilitate the blocking of pornography have been resisted by many. To many, these efforts smack of censorship. The government is taking steps to make possible the blocking of certain content, even if the government itself is not blocking the content. Those steps, many believe, are improper for a government constrained by the First Amendment.

Yet this view obscures an obvious point that becomes clear when considering the interaction between the technical infrastructure and the legal rules.

The objective of many who resist regulation to channel or zone pornography is to preserve free speech values. The regulation is seen to infringe those values; for this reason, the regulation is resisted.

But the absence of legal regulation to respond to the problem of pornography is not the same as the absence of regulation. Instead, the absence of legal regulation can simply increase the demand for technical regulation—for code designed to respond to pornography. This technical regulation has taken a number of forms, from software that blocks particular websites, to labeling standards used to rate

---

... makes, creates, or solicits ... any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age ... ;

. . . .

. . . .

. . . .

... shall be fined under title 18 [United States Code], or imprisoned not more than two years, or both.

Id.

20. Reno v. ACLU, 521 U.S. 844, 874 (1997) (holding the Communications Decency Act of 1996 unconstitutional because it "presents a great[] threat of censoring speech that, in fact, falls outside the statute's scope").

Given the vague contours of the coverage of the statute, it unquestionably silences some speakers whose messages would be entitled to constitutional protection. That danger provides further reason for insisting that the statute not be overly broad. The CDA's burden on protected speech cannot be justified if it could be avoided by a more carefully drafted statute.

Id.

21. Child Online Protection Act, Pub. L. No. 105-277, 112 Stat. 2681-736 (1998) (codified at 47 U.S.C. §§ 230–231 (2000)).

websites. But whatever its form, the technology has been criticized fairly strongly.[22]

The particular criticism that I want to focus on, however, is the over-inclusiveness of this filtering software. The technologies that have been developed in response to the problem of pornography don't limit themselves to pornography. Instead, these technologies enable a wide range of filtering, from pornography, to violence, to sites that criticize filtering.[23] Thus, the scope of the filtering from these private, technology-based solutions is often wider than the scope of filtering aimed at by the initial drive to block pornography.

Yet these private solutions are demanded because there is no effective public solution targeting the core concern—pornography. Thus, one consequence of the absence of an effective public solution is a private response that goes beyond the scope of any constitutional objectives of the law. The kind of filtering that is enabled by these private technologies is more extensive than the kind of filtering that the law could, consistent with the First Amendment, require.

My point is not that private filtering is bad, or that individuals should not be allowed to filter beyond the scope of what Congress can filter. It is instead a simpler point: that the unintended consequence of a failure

---

22. *See* ACLU, FAHRENHEIT 451.2: IS CYBERSPACE BURNING? (1997), *available at* http://archive.aclu.org/issues/cyber/burning.html (last visited Oct. 3, 2003); Richard J. Peltz, *Use "The Filter You Were Born With": The Unconstitutionality of Mandatory Internet Filtering for the Adult Patrons of Public Libraries*, 77 WASH. L. REV. 397, 410 (2002); Adam Goldstein, Note, *Like a Sieve: The Child Internet Protection Act and Ineffective Filters in Libraries*, 12 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1187, 1189–97 (2002); Junichi P. Semitsu, Note, *Burning Cyberbooks in Public Libraries: Internet Filtering Software vs. the First Amendment*, 52 STAN. L. REV. 509 *passim* (2000).

23. PEACEFIRE, ABOUT PEACEFIRE.ORG, *at* http://www.peacefire.org/info/about-peacefire.shtml (last visited Oct. 3, 2003). The website states:

> Peacefire.org was created in August 1996 to represent the interests of people under 18 in the debate over freedom of speech on the Internet.
>
> . . . .
>
> . . . .
>
> In October 1998, we added pages to Peacefire.org about how to disable the different censorware programs.
>
> . . . .
>
> Peacefire first received attention in December 1996 when CYBERsitter added it to their list of "pornographic" Web sites and sent a letter to our ISP threatening to block all of their hosted sites if Peacefire were not closed down. . . . The only content on Peacefire.org at that time that had anything to do with CYBERsitter was our original CYBERsitter page, which listed some of the Web sites that the program blocked, including N.O.W., Mother Jones and the International Gay and Lesbian Human Rights Commission.

Id.

to regulate properly is often a greater burden on the spread of speech than an effective regulation would achieve. And, as a corollary, if there were effective regulation to deal with pornography, much of the demand for private blocking would evaporate. The absence of public regulation thus induces more private regulation; and the presence of public regulation can reduce the demand for expansive (and speech-burdening) private regulation.[24]

A similar pattern exists with spam regulation. Unsolicited commercial e-mail has become an increasingly burdensome part of e-mail. The obvious reason for this burden is the favorable economics that the Internet offers e-mail advertisers. Users pay for the transportation cost of e-mail; advertisers thus get to free ride off of users. The consequence is that almost forty percent of e-mail is now spam.

When this problem initially emerged, there were many who resisted the idea of regulation to deal with spam. Again, regulation was seen as a kind of censorship, because it was government regulation effecting a restriction on speech.

Yet as with pornography, the consequence of failing to regulate has not been the absence of regulation. Instead, there has been an explosion of private technologies designed to facilitate the filtering of unsolicited commercial e-mail. These private technologies, as with the filtering of pornography, are both under- and over-inclusive. They are under-inclusive, because spammers can be counted on to seek ways to escape the filters. They are over-inclusive because they block a great deal of speech that is not spam.

The failure of this technology has led many to adopt a white-list approach to e-mail—only accepting mail from people whom they know. And to the extent this response becomes common, a general and valuable feature of the original design of the Internet is inverted: a medium that facilitated the broad spread of content at low cost becomes a medium that requires a reservation before your message gets delivered.

The lesson again is that the demand for private regulation increases in this context when public regulation fails. This is of course not a lesson new to the Internet: vigilantism may be necessary in some contexts, but it is not preferable to an effective government. But the regulatory power of code is much greater and more plastic in cyberspace, so this

---

24. *See* LESSIG, *supra* note 7, at 181 (describing effective private regulation).

commonplace point becomes more salient. Here too, effective public regulation could reduce the demand for inefficient private regulation.

In both contexts, the integration of a legal and technological perspective yields an initially counter-intuitive result. Some regulation may in fact advance free speech interests more than no regulation, even if that public regulation is a form of speech restriction.

Resistance

These examples are meant to mark two kinds of cases. If these are in fact *kinds*, then there will be other examples as well. But the lessons from these particular examples have been resisted to date. And about these particular instances of resistance, I make some general observations.

The two examples of good requiring balance rather than extremes—intellectual property and privacy—increasingly push to the extreme as our legal system loses a capacity to articulate balance. A powerful rent-seeking drives the extreme in intellectual property. A powerful terror allows the extreme about privacy to be achieved almost without notice. Understanding the dynamic between law and technology is not likely to remedy the problem in either case. More powerful passions control.

But the dynamic between law and technology could matter to the second class of cases—the "some-regulation-better-than-none" cases. Here an ideology against regulation limits the willingness to regulate, but the consequence of this ideology defeats the very values that are being defended. Recognizing the dynamic could therefore help advance the protection of values important here and elsewhere. But recognizing this dynamic requires incorporating a perspective that cyberlaw teaches.

American law has traditionally been very good at including outside perspectives as a way to understand the legal domain. The law and economics movement was just a maturation of the realist movement. Both progressed by testing legal claims against the knowledge produced by other disciplines.

That same openness is necessary now. As many are beginning to recognize, the single most salient feature of cyberspace is its ability to embed controls that resist or reinforce values that we bring to cyberspace. We must understand the manner in which these values are resisted or reinforced if we are to continue the experiment of self-government, where self-conscious choice determines the law we live life subject to.