INTRODUCTION

"I cannot remember a time," the novelist Robertson Davies wrote, "when I did not take it as understood that everybody has at least two, if not twenty-two, sides to him."¹ Davies' comment gives us a convenient point of departure to explore the relationship between law and cyberspace. Anyone who spends a significant amount of time on the Internet knows that the Net has at least two, if not twenty-two, sides to it. Auction sites, chat rooms, instant messaging, knowledge networks, and Net radio are but a few of the Internet's constantly expanding capabilities for communication, commerce, and social interaction. It seems remarkable, then, that at a time when we are seeking to understand and enhance a medium of such Protean character, so much of our thinking about the Internet has remained bound to—and bounded by—the same few metaphors that have dominated Internet culture over the past decade.

No metaphor has been more pervasive in this regard than the concept of cyberspace as the "Wild West." Early visionaries of the Internet characterized it as an "electronic frontier,"² comparing its

---

² See Mitchell Kapor and John Perry Barlow, Across the Electronic Frontier (July 10, 1990) <http://www.eff.org/pub/Misc/Publications/Mitch_Kapor/electronic_frontier.eff>. See also John Seabrook, Deeper 17, 272-73 (1997). The Electronic Frontier Foundation, which
explorers to the eighteenth- and nineteenth-century pioneers who settled the American West. Those comparisons have continued to the present day, both within the hacker community and in popular writing about the Internet. Some Internet visionaries have also used the Western metaphor as a rhetorical device to challenge the appropriateness of governmentally imposed law in cyberspace. More recently, government authorities, concerned about the spread of criminal activity involving the Internet, have invoked the Wild West metaphor to argue for the rule of law in cyberspace. Journalists and popular

Kapor and Barlow created, has continued to perpetuate the “electronic frontier” metaphor. See Electronic Frontier Foundation (visited November 25, 2000) <http://www.eff.org>.
4. For example, one hacker quoted in recent news accounts about computer crime prosecutions identifies himself only as “Bronc Buster.” See Lynn Burke, MostHateD to Plead Most Guilty, WIRED NEWS (March 29, 2000) <http://www.wired.com/news/print/0,1294,35264,00.html>.
6. David Johnson, for example, viewed legislative constraints on access to online personal data as little better than barbed wire fences in cyberspace, that would create “the prospect of a range war over ownership of data . . . .” David R. Johnson, Barbed Wire Fences in Cyberspace: The Threat Posed by Calls for Ownership of Transactional Information (Apr. 4, 1994) <http://www.eff.org/pub/Intellectual_property/cyber_barbwire_johnson.article>. John Perry Barlow offered an even harsher depiction of cyberspace-as-Wild-West, in which the rule of law had no legitimacy:

There is a cycle of frontier inhabitation which has usually gone like this: Misfits and dreamers, rejected by or rejecting society, are pushed out into the margins. There they set up camp and maintain what little order they want in it by unwritten codes, the honor of thieves, the Code of the West.

Despite their usual haplessness, they discover resources and start exploiting them. Burghers and boosters back in the civilized regions hear of these discoveries. Settlers, a milder sort, come in with their women and children and are repelled by the savagery and license of their predecessors, whether mountain men, prospectors or Indians. They send for troops, they elect representatives, they pass laws, and, pretty soon, they’ve created another civilized simulation of certainty.

Already we can find the usual Christian soldiers massing at the borders of Cyberspace . . . . [T]he government is preparing to place this new frontier under the rule of law. Whether the pioneers already there want it or not.


7. Recently, for example, at a conference between Internet industry representatives and senior political and law enforcement officials from the Group of Eight (Canada, France, Germany, Great Britain, Italy, Japan, Russia, and the United States), a senior representative of the Royal Canadian Mounted Police deemed the Internet “akin to the Wild, Wild West in its lawlessness.” John-Thor Dahlburg, G-8 Seeks Unity on Policing Internet, LOS ANGELES TIMES, May 18, 2000, at C3. For indications of the ubiquity of this view, see, e.g., John Makulowich, Wild West of the Information Age, WASHINGTON TECHNOLOGY (March 22, 1999) <http://www.wtonline.com/vol13no24/briefs/433-1.html> (quoting remarks of Attorney General Janet Reno that “[w]e cannot allow cyberspace to become the Wild West of the information age”);
writers have also tried to use the Wild West metaphor in writing about Internet crime, sometimes with results that range from the laborious to the unintentionally comic.

The reasons for the popularity of the cyberspace-as-Wild-West metaphor are easy to understand. The myths and legends of the Old West are so thoroughly infused in American history and culture that they readily come to mind whenever we begin to explore any new frontier, whether real or virtual. The myths and legends that come first to our minds, however, may depend largely upon the way we define ourselves in relation to the Internet.

Internet visionaries presumably found the Western metaphor appealing because their original notion of cyberspace accorded so well with the popular conception of the Old West. For them, the early Internet, like the Old West, "beckoned to the imagination as a place unregulated and uncivilized, whose inhabitants lived beyond the reach of law and the constraints of polite behavior." Their cyberspace, in

Interpol Urged to Stop Internet from Becoming "Wild West," WJIN NEWS (Nov. 8, 1999) http://www.wjin.net/html/news/3019.htm> (quoting Toshinori Kanemoto, President of Interpol, as saying that "We should not make the Internet a Wild West"); Polly Sprenger, U.K. Cyberspace Is No 'Wild West,' THE STANDARD (Sept. 23, 1999) <http://www.thestandard.com/article display/0,1151,6535,00.html> (quoting Patricia Hewitt, the United Kingdom’s Minister for e-commerce, as saying that "]w]e don’t accept that cyberspace is some Wild West frontier where law enforcement and the sheriff should keep out"); Elliot Zaret, FTC to Launch E-Commerce Division (Apr. 21, 1999) <http://www.zdnet.com/filters/printerfriendly/0,6061,2245064-2,00.html> (quoting Sheila Anthony, Commissioner of the Federal Trade Commission, as saying that the FTC would take “law enforcement actions to stop the Internet from turning into the ‘wild west’ of advertising and marketing.”). The title of the U.S. Department of Justice’s recent report on unlawful conduct on the Internet reflects this continuing reliance on the Western metaphor. See U.S. DEP’T OF JUSTICE, THE ELECTRONIC FRONTIER (2000).


9. One journalist, in writing about identity theft on the Internet, noted “that the United States in particular has become a Wild West for mischievous mouseslingers.” Tyler Hamilton, The Identity Thieves—Losing Face, TORONTO GLOBE AND MAIL (June 5, 1999) <http://www.infowar.com/class_1/99/class_1050699a_l.shtml>.

10. “Like the gunslinging sheriffs of old who introduced order to the West,” one journalist wrote, in a flurry of mixed metaphors, “federal agencies are increasingly wading into the digital landscape and throwing around their regulatory weight.” Doug Brown, Bulked-Up FTC: Let’s Get Busy, INTER@ACTIVE WEEK (Feb. 18, 2000) <http://www.zdnet.com/filters/printerfriendly/0,6061,2440841-35,00.html>.

11. TED MORGAN, A SHOVEL OF STARS 13 (1995). As Jane Tompkins has noted, the West functions as a symbol of freedom, and of the opportunity for conquest. It seems to offer escape from the conditions of life in modern industrial society: from a mechanized existence, economic dead ends, social entanglements, unhappy personal relations, political injustice. The desire to change places also signals a powerful need for
short, was most attractive because of its lawlessness; it was a place they saw as unbounded by stultifying legal restrictions.

Law enforcement officials, by contrast, typically find the Wild West metaphor disquieting. For them, it reflects the more malign form of lawlessness for which the Old West, in varying degrees, earned its reputation: an absence of generally accepted legal rules to protect the citizenry and lack of effective legal institutions to enforce those rules.\(^1\) In much of the Old West between 1865 and 1890, a respect for law and an acceptance of institutions drawn from Anglo-American law were slow to flourish. Government authorities today are probably mindful of that fact when they see in the electronic frontier a potential for the same kinds of disorder that affected the Western frontier.

We need to remember that when we use metaphor to describe or analyze a problem, metaphor inevitably has seductive qualities that can lead us seriously astray.\(^1\) While metaphor is pervasive in modern speech and writing, its main use is poetical rather than analytical.\(^1\) Metaphor swiftly reduces complex ideas by synthesizing two ideas or images "into a simple concrete equivalent."\(^1\) This power makes metaphor especially well-suited to poetic imagery and especially ill-suited to analytical description.\(^1\) More than other figures of speech, it tempts us to confuse similarity with identity and to define the problem we are studying in terms of the metaphor we have chosen. These seductive qualities are particularly strong with a metaphor as powerful and pervasive as the Western metaphor has been in American culture.

We must nonetheless resist the temptation to use Wild West metaphors when we examine the relationship between law and the Internet. Metaphors as laden with myth and popular belief as "the Old West" or "the Wild West" are unlikely to either illuminate particular concepts or express meanings more clearly than abstract language can.\(^1\) At a time when law and legal institutions are straining

---

self-transformation. The desert light and the desert space, the creak of saddle leather and the sun beating down, the horses' energy and force—these things promise a translation of the self into something purer and more authentic, more intense, more real.  


12. In some cowtowns known for their violence, a frontier marshal's tenure lasted, on the average, about two weeks. See DON WORCESTER, THE CHISHOLM TRAIL 130 (1980).  


15. READ, supra note 14, at 23.  

16. Id. at 23-24.  

17. See id. at 26.
to keep pace with the Internet's rapid growth and development,\(^\text{18}\) it is clear that such resistance will not be easy. The legal profession is already beginning to propose solutions to legal problems in cyberspace by insisting on the adoption of a single metaphor that frames the solutions in terms of false dichotomies.\(^\text{19}\) The fact remains that the more we insist on selecting any single metaphor or analogy—not merely the Wild West—as the correct one for framing complex cyberspace issues, the more likely we are to select rules that are inadequate, if not dangerously misleading.

At the same time, there can be considerable heuristic and analytical value in looking beyond the mythic dimensions of the Wild West metaphor. Metaphors that illuminate, rather than obscure, ideas and concepts may have considerable value in analyzing cyberspace issues. Certain empirically verifiable aspects of the Western experience\(^\text{20}\)—especially those with some relation to the growth of law in the American West—might offer metaphors more likely to illuminate ideas and expand both our insight into and understanding of cyberspace legal issues.

But which aspect of the real Western experience might serve that purpose? To serve as a point of comparison with the Internet, it should be some form of technology that was not only integral to the growth and settlement of the West, but also, as the Internet is likely to do in our time, something that ultimately transformed the West's law, culture, and character. The telegraph, the transcontinental railroad, and the six-shooter all were technologies integral to Western expansion. Yet none of them had a more decisive impact on the Old West's law and culture than a homely, but ultimately ubiquitous, piece of technology that cowboys sardonically termed "the devil's hatband":

barbed wire.\(^\text{22}\)

In this Article, I maintain that while there is an ongoing conflict of legal traditions over the desirability of fences in cyberspace, there are definite virtues in the creation of such fences, so long as we understand the physical, psychological, and moral dimensions of that proc-

---


19. See, e.g., Jonathan Wallace and Michael Green, Bridging the Analogy Gap: The Internet, the Printing Press, and Freedom of Speech, 20 SEATTLE U. L. REV. 711, 712 (1997) (advocating that the Supreme Court set forth "the operative metaphor for [Internet] freedom of speech and apply[y] the metaphor in conjunction with an appropriate analogy for the technology" (emphasis added)).


22. See DON WORCESTER, supra note 12, at xiv.
ess. Part I will present a brief survey of the history of barbed wire in the Old West, paying particular attention to the contending legal traditions that affected the manner and extent of that growth in the West. These contending legal traditions, which related to "fencing in" versus "fencing out" cattle, played a key role in the growth of barbed wire and ultimately in the growth and settlement of the Old West. Part II will then identify some of the similarities between that process and the continuing process of conflicting legal traditions in cyberspace. In particular, I will show that the concepts of "fencing in" and "fencing out" have continuing vitality and relevance in exploring the relationship of law and cyberspace. Finally, Part III will examine the extent to which those concepts have both historical and moral relevance in that exploration.

I. THE "DEVIL'S HATBAND": A HISTORICAL SURVEY

In the growth and settlement of the Old West, boundary setting was a process that constituted "the very essence of frontier life."23 To define the physical territory that one owned, and in some respects, to define oneself and one's willingness to relate to others beyond that territory on the frontier,24 Western settlers needed some mechanism that would not only visibly delineate that territory for other settlers, but also would serve to control the movements of the increasingly vast herds of cattle.

If we pause for a moment to imagine a segment of barbed wire fence, we can see that barbed wire had a certain technological elegance that suited its purposes well. Barbed wire could be quickly produced in mass quantities and, once installed in the desired location, was both highly durable and highly effective in its intended uses. Because the wire presented such a small cross-section to wind and precipitation, it typically outlasted wood, which was hard to come by in cattle country.25 Its barbs—and the occasional intervention of "checkline riders" to keep cattle back from the fencing26—also made it efficient for restraining even large herds of cattle.

At the same time, the introduction of barbed wire in the West exacerbated a clash between two legal traditions, directly implicating the very nature of Western life and culture. In what had been New Spain and antebellum Texas and California, Spanish law "had tradi-

24. See id. 16, 18.
25. Id. at 309.
26. See TED MORGAN, supra note 11, at 267.
tionally held that the landowner must fence his land if he wished to protect his crops from cattle on the open range."27 This legal tradition led to the open-range system of cattle raising, in which multiple ranchers grazed cattle on unfenced public lands and cooperated with and helped one another, "particularly at roundup time."28 Consequently, "[t]he majority of cattlemen, especially in Texas, believed that farmers should fence their land to keep cattle out."29

On the other hand, as historian David Dery has explained,

English common law brought to America endorsed a "fence livestock in" concept, placing the burden of responsibility on the stock owner to control his livestock . . . . [A]s increasing numbers of settlers began pushing westward into cow country . . . more and more frequently, farmers turned to the law when cattle overran their fields. Both Kansas and Nebraska passed herd laws making it mandatory for cattlemen to restrain their herds from wandering at will over the prairies and plains . . . . The herd laws . . . reflected English common law . . . . Herd laws placed the responsibility on the cattlemen, even when cattle broke through fences or otherwise got loose.30

While cattlemen deplored the advent of the herd laws and tried (mostly in vain) to challenge them in courts,31 they had to find a means of restraining their cattle if they were to comply with those laws. At the time, the price of board fences in most places was prohibitive—between $500 and $1,000 a mile in mid-nineteenth century dollars—so cattlemen resorted to range riders and line riders, to patrol the boundaries of the ranches and drive back cattle that strayed too close to the unfenced line.32 This state of affairs left the range mostly open and the open-range culture relatively intact.

Barbed wire changed all that in the 1870s and 1880s. As settlers continued to pour into cattle country and cattlemen and farmers alike found this new technology substantially cheaper than board fencing,33 both groups began erecting barbed-wire fences. In addition, when a drought of epic proportions struck the West in 1883, water and grass for grazing became more precious than ever. Cattlemen who lacked

27. DERY, supra note 21, at 310.
28. Id. at 309.
29. Id. at 310.
30. Id. 308-10.
31. Id. at 309.
33. The cost of barbed wire fencing might range from $200 to $400 per mile. See DERY, supra note 21, at 315.
the foresight to acquire land and water rights fenced in land they did not own, including public lands and even "farms and small ranches belonging to other people in an effort to grab every possible acre of grassland for their cattle." 34 Other cattlemen induced their cowboys to file homestead claims on open range land and, for a price, to turn over their newly acquired land titles to the cattlemen. 35

The spread of laws requiring cattlemen to fence in land eventually became, as the United States Supreme Court described it with astringent understatement, "a subject of agitation." 36 The fencing of unfenced land soon took a destructive turn in many areas.

Fences blocked many public roads, cutting off schools and churches and interfering with the delivery of the mail. Men began to cut fences, and soon ranchers were hiring men to do the job. More than half of the counties in Texas reported the cutting and wrecking of fences and the burning of pasturelands by late 1883. . . . Perhaps half-a-dozen men were killed in battles between fence cutters and ranchers defending their property. By the fall of 1883 damage to fences in Texas was estimated at $20 million. 37

Decisive government action largely ended fence-cutting and the overfencing of land. A special session of the Texas legislature made fence cutting a felony with a maximum penalty of five years imprisonment; it also made the knowledgeable unpermitted fencing of public lands or lands belonging to others a misdemeanor. 38 Builders of such fences were required to remove them within six months. Those who built fences across public roads were ordered to place gates at 3 mile intervals and to keep them in good repair. 39 Illegal fencing of public lands continued elsewhere until 1885, when Congress "passed a law designed to speed prosecution of those who fenced public land" 40 and President Grover Cleveland issued an Executive Order for the removal of such fencing. 41

This survey of barbed wire's introduction into the Old West suggests at least two themes that directly apply to our consideration of the relationship between law and cyberspace. The first involves the conflict of traditions relating to the establishment of boundaries and

34. Id. at 320; White, supra note 32, at 264. See TED MORGAN, supra note 11, at 267.
35. DERY, supra note 21, at 320; White, supra note 32, at 263-64.
37. DERY, supra note 21, at 320-21.
38. Id.
39. Id. at 321.
40. Id. at 325.
41. White, supra note 32, at 265. See WORCESTER, supra note 12, at xvii.
the importance of the concepts of "fencing in" and "fencing out" in those traditions. The second involves the nature and impact of the mechanisms that people adopt to establish those boundaries and control certain items of value.

II. CONFLICTING TRADITIONS IN CYBERSPACE: THE RELEVANCE OF "FENCING IN" AND "FENCING OUT"

The conflict of traditions in the Old West, as I have described it, involved ostensibly contradictory legal rules that two sovereigns had devised in different periods. One rule adjured farmers to fence out cattle, the other required cattlemen to fence in cattle. Clearly, neither rule standing alone could claim logical or moral superiority over the other. Choosing one or the other, nonetheless, had two distinct virtues. First, it provided a settled rule that uniformly applied to all similarly situated parties. Second, it recognized implicitly that the potentially conflicting activities of farmers and cattlemen required the adoption of a rule to address the reciprocal harms that each could cause to the other's interests. In Coasian terms, society benefited from the selection of a rule that avoided what that society perceived to be the more serious harm. Both rules also addressed a critical aspect of harm avoidance or reduction that Coase himself did not address: deciding whether society would derive a greater benefit by requiring one party to restrain that harm (that is, fencing it in), the other party to exclude it (that is, fencing it out), or some combination thereof.

Likewise, the Internet is experiencing a conflict of traditions that affects its culture and development. This conflict could be broadly characterized as legal, in the sense that legal norms and values are implicated. A more precise characterization would be that the conflict is between a legal and a nonlegal tradition, rather than two competing legal traditions as in the Old West.

42. Bernhard Grossfeld has cited the "fencing in"/"fencing out" conflict in the Old West as an example of "geography [being] more powerful than legal culture or history." BERNHARD GROSSFELD, THE STRENGTH AND WEAKNESS OF COMPARATIVE LAW 83 (Tony Weir trans. 1990). From the historical evidence cited above, it appears that a combination of technology, economics, politics, and climate were more decisive than geography in the ultimate selection of the "fence cattle in" rule.

43. See Ronald A. Coase, The Problem of Social Cost, 3 J.L. & ECON. 1, 2 (1960). Coase is a professor of economics, now retired from the University of Chicago, who won the Nobel Prize in Economics for his seminal work in the field of law and economics. See Anne Swanson, Nobel Prize in Economics Goes to Univ. of Chicago Professor, WASH. POST, Oct. 16, 1991, at F1. What makes his 1960 article on social cost especially pertinent to the present discussion is that, to examine the problem of reciprocal harm and social cost, Coase chose "the case of straying cattle which destroy crops growing on neighboring land." Ronald Coase, supra, at 2.

The legal tradition in this case embodies a set of norms, long established in various legal systems, that support the making of, and foster obedience to, legal rules for the creation and enforcement of boundaries in physical space. This tradition derives its support from the majority of the public, who have relatively little familiarity with computing and Internet technology, but who are generally familiar with laws establishing boundaries and are accustomed to accepting the utility of boundaries and rules in everyday life.

In contrast, the nonlegal tradition embodies a loosely connected patchwork of norms, generally libertarian in character, that tend to disfavor legal rules for cyberspace as much as cowboys did barbed wire. This tradition derives its support from a comparatively small minority, who are, on average, far more familiar with the technology but who question the need for and desirability of fences in cyberspace. A minuscule segment of this latter group goes still further, opposing fences in cyberspace (whether for personal or commercial purposes) when they disagree with the reasons for creating those fences. These individuals are also willing to take action to assist others in circumventing cyberspace fences that they oppose for personal, commercial, or ideological reasons. In short, the conflict between these two traditions focuses not on whether fencing in or fencing out is more appropriate for some aspect of cyberspace, but whether there should be fences at all in cyberspace and, in some cases, whether anyone has a right to erect them.

This general antipathy to the notion of fences in cyberspace is unfortunate for two reasons. First, it tends to polarize discussion about the regulation of cyberspace, turning it into an “us versus them” confrontation. Second, by keeping the debate focused on whether there should be fences or not, thoughtful consideration of the issue is

45. For example, for several years one computer consultant has been “reverse-engineering” blocking and filtering programs intended to protect children from sexually oriented on-line content and publishing the sites disclosed through his reverse-engineering. The consultant’s professed intent is to show that many sites blocked by such programs are neither pornographic nor offensive. See Patricia Jacobus, Free Speech Advocate Raises Ire of Filtering Firms, CNET.COM (March 8, 2000) <http://news.cnet.com/news/0-1005-202-1567022.html>.

The effects of publishing blocked sites extends beyond merely demonstrating to the general public that certain blocking programs are overinclusive. Such publication also can enable the operators of the blocked sites to change their Internet Protocol addresses or Uniform Resource Locators to escape the blocking effects of the programs. Publications also can assist minors—at least those with a modicum of computer expertise and the desire to use it—to circumvent the programs and gain access to sexual content that their parents presumably would have wanted to keep from them. In the latter two circumstances, the reverse engineers’ actions necessarily interfere in some measure with a parent’s wishes to control his or her child’s access to sexual content—in effect, cutting the cyberspace fences that the parent installed to fence out undesirable content.
forced into an overly narrow frame of reference. It is too late to say that there should not be fences of some kind in cyberspace. People need fences online for much the same reasons they do offline: to protect children, to shield personal data from criminal or unauthorized use, or to simply maintain a comfortable level of personal privacy in everyday activity.

It is in this regard that the concept of "fencing in" and "fencing out" can be useful in exploring the relationship of law and cyberspace. When applied to certain Internet related problems, it can help us to understand those problems more clearly and to think through how cyberspace law could and does allocate responsibility for implementing solutions to those problems.

Take, for example, the availability of sexually oriented content on the Net. Society in general, and parents in particular, have an undeniable right to protect minor children from harmful materials of a sexual nature. Indeed, the Supreme Court has consistently recognized "the principle that 'the parents' claim of authority in their own household to direct the rearing of their children is basic in the structure of our society." Curiously, the debate about controlling minors' access to sexually oriented Internet content has focused exclusively on one approach: how parents and schools can effectively block and filter such content to keep it from children. Perhaps because the parents' claim of authority over their minor children is so strong and compelling, the debate apparently assumes that as a matter of public policy, parents and school officials should have the primary responsibility for "fencing out" the harmful content, and that the purveyors of the content have no responsibility for "fencing it in."

A leading commentator on cyberspace law, Lawrence Lessig, provides one example of this mode of thinking. To deal with the problem of online sexual content, Lessig suggests the creation of a Web browser that disables the collection of personal information about a user, but signals that the user is a minor. Servers with adult material could identify the client as a kid, and thus deny access. Setting aside the distinct possibility that an adolescent boy with moderate knowledge of the Internet can quickly download another browser without a "kids' mode" and visit adult sites with ease, Lessig's proposal tacitly imposes on parents the primary responsibility to acquire the browser software necessary to allow their child to surf safely. The

---

47. Id. at 865, quoting Ginsberg v. New York, 390 U.S. 629, 639 (1968).
fence, in other words, is made more flexible, but the parents are the only parties who bear the responsibility for putting it up and keeping it in good repair.

It is necessary to ask whether this exclusive focus on the parents and "fencing in" is the only way to look at the problem. Consider the operations of adult bookstores in physical space. Society would vigorously oppose an adult bookstore owner who proposed to conduct his business from an open-air tent, where sexually oriented materials would be visible from any direction of approach and no physical constraints would impede minors from coming within viewing distance. Law and public policy routinely impose on adult bookstores the primary responsibility for "fencing in" sexual content that could be harmful to minors. They do so by requiring the store owners to maintain physical barriers in their stores and to verify the ages of patrons, so that minors who might enter the store are nonetheless prevented from viewing sexual materials. The bookstore owners, in effect, bear the primary responsibility for "fencing in" the harmful content, and "fencing out" the class of individuals who should not have contact with that content. In that situation, society has weighed the relative harms—the diminution of commerce in sexually oriented material versus damage to "the physical and psychological well-being of minors"—and made its decision about which harm more urgently needs to be avoided.

A similar analysis with respect to online sexual content would help to foster a new perspective on the problem. In this analysis, we need to weigh the relative potential harms to adult content merchants and minors in light of our ability to control and direct the architectures we create for cyberspace. We must then consider whether the allocation of responsibility can be shifted, consistent with constitutional values, in two ways: first, by explicitly choosing who should bear primary responsibility for "fencing in" or "fencing out" to avoid the greater harm, and second, by requiring the adoption of mechanisms, such as software or legal standards, to accomplish that purpose.

50. See, e.g., Lessig, supra note 48, at 506.
51. One recent media report notes that various "adult sites," including sites that facilitate alcohol sales, gambling, and pornography, are referring users to adult verification systems. Some of these systems "purportedly accept birth certificates or other documents as proof." Lynn Voedisch, You Must Be 18 to Enter, CNN.COM (Jan. 17, 2000) <http://cnn.com/2000/TECH/computing/01/17/are.you.18.idg/index.html>. Some critics charge that such systems are no more than "scams," where sites do nothing more than ask the person seeking to enter the site whether they are at least 18 and seek no independent verification of the person's response. See id. In any event, the existence of sites that accept physical documentation of age indicates that it
Another type of Internet conduct where the "fencing" concept is applicable is crime that involves continued interaction between a criminal and a victim. Fraud and cyberstalking\textsuperscript{52} are types of crime in which the victim often (though not always) has had some voluntary contact with the criminal at the outset, even if the victim does not realize the criminal's true purpose until later.\textsuperscript{53} In other words, the fraudulent content that the criminal directs at the victim does not have characteristics that most observers would readily identify as offensive or harmful, unlike sexual content, which does have readily identifiable harmful or offensive characteristics. It is therefore difficult, if not impossible, for an individual to "fence out" fraudulent content through the use of software unless he or his Internet service provider (ISP) blocks or filters all "spam"\textsuperscript{54} and he avoids visiting chat rooms and message boards altogether.

Moreover, the nature of the relationship between a criminal and a victim is wholly different from the relatively arm's-length relationship that exists between a commercial content provider and a prospective consumer. Unlike the commercial provider, there is no legitimate harm to the criminal that law and public policy must take into account. The law's only concern in determining who should be responsible for "fencing in" or "fencing out" fraudulent content, is the victim's economic and related loss.\textsuperscript{55} The law therefore appropriately places the responsibility solely on the criminal, imposing criminal sanctions on anyone who disseminates content on the Internet with the

\textsuperscript{52} Cyberstalking, for purposes of this discussion, can be defined as any effort to use the Internet to carry out the types of activities that stalkers conduct in physical space, such as direct contact with the victim or surveillance of the victim's activities. See U.S. DEP'T OF JUSTICE, CYBERSTALKING (1999).

\textsuperscript{53} In many cases, Internet fraud and cyberstalking can be conducted without any prior contact between criminal and victim. Some forms of Internet fraud, such as credit card fraud, may involve hacking into insecure e-commerce Web sites and downloading credit card numbers for later use at other sites. Similarly, cyberstalking can involve the purchase of personal data, such as Social Security numbers, from commercial Web sites without the knowledge or consent of the person to whom that number is assigned. See, e.g., Net Stalking Victims Tell Their Tales, MSNBC (March 28, 2000) <http://www.msnbc.com/news/388008.asp>.

\textsuperscript{54} "Spam" is a verb defined as sending "copies of the same message to large numbers of newsgroups or users on the Internet. People spam the Internet to advertise products as well as to broadcast some political or social commentary." TECH ENCYCLOPEDIA (visited Dec. 1, 2000) <http://www.techweb.com/encyclopedia>.

\textsuperscript{55} It has become clear to law enforcement authorities in recent years that the impact of white-collar crime often extends well beyond the victim's direct economic losses. Fraud victims have reported other significant effects, including depression and loss of trust in others. See, e.g., UNITED STATES-CANADA WORKING GROUP ON TELEMARKETING FRAUD, REPORT (1997).
intent to defraud. In effect, the law requires that all online individuals "fence in" any content that has a fraudulent purpose.

The concept of fencing does not necessarily mean that the government is required to regulate by specifying or developing the type of fencing. Take, for example, the recent spate of distributed denial of service (DDoS) attacks against a number of e-commerce sites. One tell-tale sign of a DDoS attack is the sending of "spoofed packets," which are comprised of digital data that contains legitimate destination addresses but appear to originate from an illegitimate source within a particular network. Networks and ISPs that want to reduce the risk of receiving spoofed packets are using filtering technology that stops spoofed packets from making their way onto the Internet.

One organization has already developed and made available at no cost to the public an antispoofer test tool, which allows users to test whether their filters are working properly. This action, along with recent efforts by private-sector organizations to combine their efforts with regard to Internet security, show that the private sector can accomplish things through collective action, without government intervention or direction. Indeed, we might even say that this type of collective action is in the tradition of the Old West, as it is reminiscent of the cooperative and mutually supportive actions of open-range cattlemen.

We need to pause here, though, to clarify what we mean when we refer to fences in cyberspace. Although one might think that the only kind of fence we can create in cyberspace consists of bits and bytes, such a belief is premised on certain assumptions about the nature of cyberspace itself. These assumptions must be examined with care if we are to explore the relationship between law and cyberspace more completely. Part III will provide the outlines of that examination.

56. A DDoS attack consists of the coordinated launch of a large number of messages from multiple computers to a particular network or computer. The purpose of this attack is to overwhelm the network or computer with so many messages that it slows or completely interrupts service at that network or computer. See "denial of service attack," TECHENCYCLOPEDIA (visited Sept. 8, 2000) <http://www.techweb.com/encyclopedia>. In February 2000, a spate of DDoS attacks felled a number of leading e-commerce websites, such as Amazon.com, Dell, eBay, and Yahoo! Ultimately, Canadian authorities arrested and charged a 15-year-old boy, who is suspected of having used at least 54 computers to launch the coordinated attacks. See Canada Broadens Its Case Against Suspected Hacker, N.Y. TIMES.COM (Aug. 4, 2000) <http://www.search1.nytimes.com/search/daily/b...+cyber-lib+cyber-lib+8725+0+wAAA+Mafiaboy> (visited Sept. 8, 2000).

57. See <http://www.icsa.net>.

58. See id.
III. Cyberspace, Physical Space, and Moral Choices

One critical aspect of the conflict between legal and nonlegal traditions in cyberspace is that defenders of the nonlegal tradition, as well as supporters of the legal tradition, routinely treat the concept of cyberspace as reality, not metaphor. In their view, cyberspace is truly a place different from the world we knew before the creation of the Internet. Several of the leading scholars in cyberspace law have lent support to this view by asserting that cyberspace is literally a separate "place" or "space,"59 or referring to cyberspace as a "new space" distinct from "real space" or from "a space that we have inhabited."60

The cyberspace-as-new-space metaphor is an integral element in some of the prevailing legal interpretations of cyberspace. In essence, it provides the foundation—particularly an explicit major premise and an implied minor premise—of a syllogism that those interpretations appear to have adopted. That syllogism is as follows:

(1) Cyberspace is a space or place different from real space (the explicit major premise);

(2) Laws that regulate conduct in real space cannot effectively regulate conduct in cyberspace (the inarticulate minor premise); and

(3) Therefore, we must either refrain from applying these ineffective real-space laws to cyberspace, or devise new laws or modes of regulation that can effectively regulate cyberspace.

Acceptance of the so-called "separateness" of cyberspace also encourages an inference that the character of cyberspace law must differ from the character of law governing real space.61

---


60. Lawrence Lessig, The Path of Cyberlaw, 104 YALE L.J. 1743, 1744 (1995). See also, e.g., Lawrence Lessig, Constitution and Code, 27 CUMB. L. Rev. 1, 2, 3, 13 (1997). While Lessig disagrees strongly with Johnson's and Post's notion that cyberspace constitutes a place separate from real space and beyond the reach of real-space government, his writings have sometimes failed to make clear whether he considers the regulatory forces of cyberspace to be elsewhere than real space. See Andrew L. Shapiro, The Disappearance of Cyberspace and the Rise of Code, SETON HALL CONST. L.J. 703, 717-18 (1998). More recently, Lessig definitively stated that "cyberspace is not a place," then immediately went on to describe it in spatial terms as "many places." LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 63 (1999). A fuller consideration of Lessig's views, which richly deserve such consideration, is beyond the scope of this Article.

61. See David R. Johnson and David Post, supra note 59, at 1379, 1381.
Several features of these interpretations are troublesome. First, the notion of cyberspace's "separateness" from physical space involves an assumption about physical reality for which its proponents offer no empirical support. This notion can have a profound consequence for legal analysis.\(^\text{62}\) If it is assumed that the nature of cyberspace is truly distinct from that of physical space, then we literally could not count on principles we are accustomed to applying in the real world, such as physics—or law. We would have to treat even the most basic activities in cyberspace as though we had no experience with them and develop new legal concepts to address cyberspace issues without reference to real-world legal concepts.

The perception of cyberspace as separate from real space also tends to encourage a belief that cyberspace is an actual jurisdiction separate from the polities that exist in real space and, therefore, should be governed in ways that traditional political processes cannot be trusted to handle.\(^\text{63}\) Finally, it should not be surprising that if we accept the notion that there is a clear difference between physical space and cyberspace, we may be more inclined to believe that mechanisms that function in the physical world, such as fences, cannot have effective counterparts in the cyberspace world.

The lack of empirical evidence of cyberspace's "separateness" from physical space suggests that we need to make our own observations of cyberspace and collect empirical evidence. Gathering this kind of evidence about the nature and operation of cyberspace serves to improve our understanding of it, as well as our ability to make law relating to it. Because computers increasingly blur the distinction between physics and psychology,\(^\text{64}\) these two fields may be the most appropriate to inform and guide our observations.

1. Physics

It takes no great knowledge of physics to understand that every component of computers and the Internet—right down to the silicon,


\(^{63}\) At a "Junior Summit" conducted at MIT in 1998, for example, 94 teenaged delegates from around the world endorsed the concept of "Nation1," a so-called "cybercountry" stemming from a Website oriented toward teenagers. Participants discussed principles for building a "cybernation" separate from individual physical nations: as one delegate put it, "We need to populate the country before we can change the world.... It takes more than a week to build a country. We've only just begun." "Junior Summit" Endorses New Nation (Nov. 24, 1998) <http://www.zdnet.com/zdnn/stories/news/0,4586,2168911,00.html>. For a classic statement of the belief that cyberspace constitutes an area beyond the authority of government in real physical space, see John Perry Barlow, The Declaration (Feb. 8, 1996), reprinted in SALON <http://www.salonmagazine.com/08/features/declaration.html>.

copper, and plastic in our home computers—consists of the same
physical elements as everything else on Earth. Every e-mail we send
or receive, every Web page we access, works because the electrons or
photons at work on the Internet are exactly the same as those we find
in every other aspect of the physical world. Furthermore, the sym-
metry of physical laws that quantum physics has helped to establish
operates exactly the same way for cyberspace as it does for the rest of
the physical world.

One can see whether the symmetry of physical laws applies to
cyberspace by conducting a "thought experiment" that involves an
imaginary computer with a wireless connection to the Internet. There
are four symmetry operations in physics that are relevant at this scale:

(a) Translation in Time. Translation in time involves a proc-
ess whereby one builds the computer and starts it, and
then builds the same computer three days later and starts it
at the same time in exactly the same condition; holding all
other features of the environment the same, the two com-
puters will go through the same actions in exactly the same
way. Common experience with computers shows that
there would be no change in this computer's operation in
relation to the Internet. Whether one built it today or
three days from now, it would work exactly the same.

(b) Translation in Space. Translation in space involves a proc-
ess whereby, if one starts an apparatus at certain coordi-
nates in space and translates it to new coordinates, the laws
of physics do not change. Here, too, the computer and
its Internet connection will function exactly the same,
whether one moves it side to side, up and down, in a circle,
or upside down.

(c) Uniform Velocity in a Straight Line. Uniform velocity in a
straight line involves a process whereby, if one has an
apparatus working a certain way and then moves it and all
relevant surroundings at a uniform velocity in a straight
line, the laws of physics will not change. As many of us
may have seen on airplane or train travel while we or

65. Quantum physicists define "symmetry" as a property of matter if it can be subjected to
a certain operation and appears exactly the same after the operation as before. See Richard P.
Feynman, Six Not-So-Easy Pieces 1 (1997).
66. See id. at 25.
67. See id. at 5.
68. See id. at 25-26.
others were using laptops, this operation also holds true for computers and Internet use.

(d) Rotation in Space. Rotation in space involves a process whereby, if one turns a thing in space at an angle and turns everything else that is relevant along with it, the laws of physics will be unchanged.\(^69\) Here, too, the physical laws would stay the same for the computer while connected to the Internet, regardless of the direction or dimension of rotation.

This thought experiment is meant to suggest a proposition that physicists and engineers would think obvious but that some cyberlaw scholars might think heretical: that at all points of its existence and operation, cyberspace is part of physical space and it functions in perfect accordance with the laws of physics that govern the real world.

2. Psychology

When we turn to the field of psychology, we also find that people behave in cyberspace in accordance with the same principles of psychology that govern their offline behavior. For example, as I have described in a paper on the social engineering of Internet fraud,\(^70\) people who become victims of online fraud schemes are susceptible to the same modes of psychological influence that criminals have employed for many years in traditional fraud schemes—such as authority, consistency, scarcity, and social proof.\(^71\)

Admittedly, the technology of the Internet makes it possible to depict events in ways that make it more difficult to distinguish between fact and fiction.\(^72\) It also has fostered the development of new modes of online social interaction (such as chat rooms) that criminals can exploit in ways different from their customary methods. However, the tools of social influence and deception that criminals use, and the types of vulnerabilities that they seek in their victims, remain the same in both the online and offline contexts.

These conclusions—that cyberspace is not separate from physical space and that our online behavior accords with the psychological

\(^69\) See id. at 9, 25.

\(^70\) See Jonathan J. Rusch, The "Social Engineering" of Internet Fraud, Paper at the Internet Society Conference, San Jose, California (June 24, 1999) reprinted at <http://www.isoc.org/inet99/proceedings/3g/3g2.htm>.


principles governing offline behavior—have two interesting implications for our examination of law and cyberspace. For one thing, they vitiate the argument that rules in cyberspace must necessarily differ from those in the physical world because cyberspace is different, or new space. In certain respects, they suggest that there should be a presumption against crafting different rules for cyberspace conduct, absent a compelling justification. Secondly, they suggest that as we devise new types of fences in cyberspace to protect personal privacy, we may not realize that in the process, we are implicitly making choices that have moral and psychological ramifications.

For example, in response to the swell of public concern about protecting personal privacy, several companies are now offering anonymizing programs that purport to make the user’s path untraceable as he wends his way through the Internet. Some of these programs even offer users a function that enables them to adopt one or more separate online identities. Individuals clearly ought to have mechanisms enabling them to retain control over identifying data or other personal data that others may seek to acquire from them online. It is understandable that some people may wish to be anonymous if they are behaving lawfully as passive observers of certain Web content and they wish simply to avoid leaving traces of who they are or where they have been.

The debate on this issue, however, tends to define the problem solely in terms of the right to anonymity, as though there were a single, unqualified, absolute right. We need to be precise about the terms we use to describe and categorize online conduct. When the debate turns, in part, on a person’s claim that he has a right to use programs that facilitate the creation of online identities other than his real identity, we must accept that we are now speaking of a right to pseudonymity, and to the creation of a morally problematic type of cyberspace fence. When we choose to adopt false names and identities in order to interact with others online, we are—whether we are prepared to accept it or not—making moral choices.

Barbed wire fences do not purport to be anything other than what they appear to be. Selection of false identities, on the other hand, clearly involves holding oneself out to be someone and something that one is not. When we do so with the intention to mislead or deceive someone else, Sissela Bok has cogently argued, we cannot evade the fact that we are lying.

74. See SISSELLA BOK, LYING 6, 7 (1978) [hereinafter BOK, LYING]. Bok, a distinguished
We all can imagine circumstances in which we might consider lying about ourselves or our personal identities to someone we encounter online. We might, for example, consider giving an online news site false names and false background information if we want access to the resources of that site but are annoyed by the intrusiveness of the site's demands for our personal information. The problem is that under any circumstances, when we lie—when, that is, we make statements with the intent to mislead or deceive—we are arrogating to ourselves a certain power at the expense of the power of the person we are deceiving. We enable ourselves to misinform that person, to obscure our true objective, or to eliminate or withdraw alternatives that that person might want to preserve in weighing the costs and benefits of some course of action.

Moreover, when we lie, we also lay claim to a free-rider status with respect to the rest of society. We choose to lie to others, but do not want to be deceived ourselves. We therefore insist that others be honest with us, even as we are dishonest with them. The problem is that as each of us individually decides to follow this approach, we begin to create a tragedy of the commons in cyberspace. As Bok put it, "If enough persons adopt the free-rider strategy for lying, the time will come when all will feel pressed to survive."

Furthermore, we need to consider not only the liar's perspective, but also the perspective of the deceived. Should that person learn that she has been deceived, she is likely to feel betrayed, resentful, manipulated, suspicious of others who would deal with her in future, and mistrustful of the environment in which the deception occurred. She may not perceive, or will be less inclined to assume, that others might want to deal honestly with her in that environment in the future. In addition, if the deception limits or distorts the choices that the deceived makes for other people, those people feel the adverse effects of the lie and come to share the deceived's perspective even if they are never direct recipients of the lie.

philosopher and author, has written several books that explore the moral and ethical dimensions of various features of modern society. See, e.g., SISSELA BOK, MAYHEM (1999); SISSELA BOK, SECRECY (1982). See also Randy Cohen, The Gift That Keeps On Giving, N.Y. TIMES MAGAZINE, June 4, 2000, at 37.

75. See BOK, LYING, supra note 74, at 14.
76. See id. at 20.
77. See id. at 20-21.
78. See id. at 24.
80. SISSELA BOK, supra note 74, at 25 n.*.
81. See id. at 21-22.
82. See id. at 22-23.
Finally, those who are inclined to defend systematic lying to
others in cyberspace do not take account of the fact that liars
usually weigh only the immediate harm to others from the lie
against the benefits they want to achieve. The flaw in such an
outlook is that it ignores or underestimates two additional kinds
of harm—the harm that lying does to the liars themselves and
the harm done to the general level of trust and social coopera-
tion. Both are cumulative; both are hard to reverse.83

For these reasons, in both "real space" and cyberspace interac-
tions, we need to adopt a presumption against lying, and to favor
truthful statements over lies, in the absence of special consider-
ations. When a situation arises where lying is a possible choice, we need first
to seek truthful alternatives, and "only where a lie is a last resort can
one even begin to consider whether it is morally justified."84

The importance of extending the presumption against lying to
cyberspace should be self-evident once we recognize that cyberspace is
part of the real world. When we blindly encourage the creation and
spread of fences in cyberspace that are premised on the deception of
others, we inadvertently make choices about what kind of cyberspace
we want for ourselves, our children, our friends, and our colleagues.
In the very short term, of course, our options for protecting our per-
sonal privacy may be more limited. We are given the choice between
feeling confident about surfing the Net by adopting a false identity, or
worrying that wrongdoers may try to acquire our personal data and
turn it to their own malign purposes if we surf with truthful identifying data. Considering the risks, many people do not hesitate to opt for
what they consider to be an excusable or white lie.

We can, however, try to encourage the development of other
mechanisms—other types of fences—that will allow us to retain con-
trol of truthful personal data, no matter where we venture on the Net,
without having to deceive others. One model for this approach is a
recently publicized browser plug-in that discriminates between "first-
party cookies" (that is, cookies that come from the site one is visiting
at that moment) and "third-party cookies" (that is, cookies coming
from other servers that one has not visited). This tool reportedly
allows the user to choose different levels of security for his personal
data by blocking no cookies, third-party cookies, or all cookies.85 The
virtue of this concept is that it does not require us to lie to move in

83. Id. at 25.
84. Id. at 32-33 (emphasis in original).
cyberspace; it allows us not only to “fence in” our personal data but also to alter the size of the fence to fit different circumstances and needs. We need to encourage the development of other types of cyberspace fences with similar concepts, so that lying does not have to become a routine part of our social interactions on the Internet.

CONCLUSION

As we move into the next century, we need to reorient our thinking about cyberspace law. First of all, we need to accept that, for the foreseeable future, our thinking about law and its relation to the Internet must be tentative, provisional, and constantly shifting—much like the Internet itself. The headlong pace of advances in Net related technologies, and the likelihood that the Net before long will have more than “twenty-two sides” to it, will make it difficult to do otherwise.

We also need to remember, as a Tom Stoppard character put it, that “language is as capable of obscuring the truth as of revealing it.” It is necessary to identify the metaphors that have become commonplace in Internet culture and subject them to critical examination in order to fortify the rigor of our thinking about cyberspace and cyber-space law. A more comprehensive examination of these metaphors deserves inclusion on a cyberspace law research agenda.

Finally, we need to recognize that one of the major challenges for cyberspace law will be to foster greater acceptance of the concept that fences in cyberspace are not invariably “the devil’s hatband.” If “the Internet is for everyone,” as Vinton Cerf stated, we must continue to provide more robust mechanisms for “fencing in” or “fencing out,” as appropriate, so that the growing online population can be confident that what it considers valuable will be protected and that which can cause harm if left unrestrained will be restrained. Our ability to provide those mechanisms, through software and through law and legal institutions, will be one measure of how well we are making sense of cyberspace and making sensible law for cyberspace.

86. Tom Stoppard, Professional Foul sc. 5, in EVERY GOOD BOY DESERVES FAVOR AND PROFESSIONAL FOUL 75 (1978).