Property in Cyberspace
Harold Smith Reeves†

An effective and efficient system of Internet¹ regulation requires a workable system of boundary definition and maintenance.² In the physical world, drawing and maintaining boundaries are frequently the subjects of litigation. It is likely that virtual boundary definition will similarly become a popular subject of litigation, and such definition will be no less legally problematic in the virtual world than it is in the physical world.

¹ The Internet, Cyberspace, and the Net are terms used throughout this Comment to refer to the collection of roughly 2.2 million computers now connected by interlinked computer networks.
² Although the courts have had only a handful of opportunities to address the legal issues raised by the use of this new medium, increased interest in the Internet by the legislative and executive branches, as well as by law enforcement agencies, suggests that the law will soon be called upon to resolve a variety of disputes on the information superhighway. Cases addressing Internet issues include United States v Morris, 928 F2d 504 (2d Cir 1991) (prosecution of the creator of the “Internet Worm”); Cubby, Inc. v CompuServe Inc., 776 F Supp 135 (S D NY 1991) (holding that a commercial computer bulletin board service is a distributor for purposes of libel); Sega Enterprises Ltd. v Maphia, 857 F Supp 679 (N D Cal 1994) (holding computer bulletin board service liable for copyright and trademark infringement); United States v LaMacchia, 871 F Supp 535 (D Mass 1994) (holding that person who distributed copyrighted software through a computer bulletin board service did not violate the wire fraud statute). For a discussion of legislative interest in Cyberspace, see, for example, David S. Bennahum, Mr. Gingrich’s Cyber-Revolution, NY Times A19 (Jan 17, 1995); Aaron Zitner, Minority leaders move to take off in cyberspace, Boston Globe 97 (Feb 19, 1995); Patrick J. Leahy, New Laws For New Technologies: Current Issues Facing the Subcommittee on Technology and the Law, 5 Harv J L & Tech 1 (Spring 1992). For a discussion of executive branch activity, see Peter H. Lewis, Gore Preaches, and Practices, the Techno-Gospel, NY Times D1 (Jan 17, 1994). For a discussion of law enforcement activity, see generally Mike Godwin, Virtual Community Standards: BBS Obscenity Case Raises New Legal Issues, Internet WWW page available at <http://www.eff.org/pub/legal/cases/AABBS_Thomases_Memphis/obscen_virtcom_stds_godwin.article> (version current on Jan 11, 1996) (on file with U Chi L Rev); John Perry Barlow, Crime and Puzzlement, Internet WWW page available at <http://www.eff.org/pub/Publications/John_Perry_Barlow/HTML/crime_and_puzzlement_1.html> (version current on Jan 11, 1996) (on file with U Chi L Rev); Steven Levy, The Cyberpunks vs. Uncle Sam: Battle of the Clipper Chip, NY Times Mag 44 (June 12, 1994) (discussing encryption and the National Security Agency’s interest in the Internet); John Schwartz, Chipping In to Curb Computer Crime: Federal Authorities Get High-Tech Help in Tracking Down Hacker, Wash Post A1 (Feb 19, 1995) (discussing law enforcement efforts to apprehend notorious computer hacker Kevin Mitnick).
This Comment provides legislatures, courts, and practitioners with models for drawing boundaries in Cyberspace. In so doing, it fills a pronounced gap in legal scholarship. To date, academic analysis of Internet regulation has relied exclusively on a conception of the Internet as a medium in constant motion. Scholars have proposed regulatory systems designed to govern the flow of virtual commerce by directly regulating the flow itself. Although this Comment addresses many of the same issues, it finds answers not in the swirl of flowing information, but in the relatively fixed boundaries that separate systems from systems, individuals from individuals, and communities from communities.

Section I of this Comment sets out three paradigmatic boundary models for the Internet, analyzes the unique features of each, and briefly describes the extent to which each model has gained acceptance in Cyberspace. Section II considers the extent to which each of these boundary models would further the particular purposes of Internet regulation and concludes that, given the variety of aims that virtual boundaries should further, there is no single model that satisfies all of the goals of Internet regulation. This Comment recommends a more principled approach to regulating Cyberspace, one that uses different boundary models in different regulatory contexts, depending on the dominant interest to be served in each context.

I. BOUNDARY MODELS FOR THE INTERNET

Current judicial and legislative approaches to Cyberspace rely on a conception of bounded property developed to regulate the ownership of land. Under this conception, property "denotes not material things but certain rights." Arguably the most im-

---

3 Commentators do this by analogizing to existing regulatory schemes that regulate the flow of commerce or information in the physical world. See generally Henry H. Perritt, Jr., Access to the National Information Infrastructure, 30 Wake Forest L Rev 51, 62-67 (1995) (discussing statutory common carrier obligations imposed on communications networks). See also David R. Johnson and Kevin A. Marks, Mapping Electronic Data Communications Onto Existing Legal Metaphors: Should We Let Our Conscience (and Our Contracts) Be Our Guide?, 38 Vill L Rev 487, 498-506 (1993) (suggesting that the development of trucking industry regulation could provide a paradigm for Internet regulation).

4 For one example, see the discussion of the Computer Fraud and Abuse Act in text accompanying notes 52-61.

5 Morris R. Cohen, Law and the Social Order: Essays in Legal Philosophy 45 (Archon 1967) ("[A] property right is a relation not between an owner and a thing, but between the owner and other individuals in reference to things."). Cohen's observations are particularly applicable in the context of the Internet, where, as the things at issue become less
Property in Cyberspace

portant of these is the "right to exclude": the right to prevent access by others to one's land. But the right to exclude depends on the existence of adequately clear boundaries; the law must define that from which the property owner may exclude others.

Boundaries at the level of computer systems have gained widespread acceptance as the appropriate means of regulating the Internet. This Section, therefore, first examines how system-level boundaries currently operate in Cyberspace. It then discusses two alternative boundary models, with their respective advantages and disadvantages.

A. The System-Level Boundary Model

A computer system, as the term is used in this Comment, is a computer or an isolated network of computers that is connected to the Internet, provides Internet-related computer services to its users, and is governed by a system administrator. System administrators are individuals or groups of individuals charged with managing a local computer system. An administrator's tasks are, for the most part, limited to performing day-to-day maintenance and ensuring that computer connections within the system and with the Internet are functioning properly. Most importantly, it is the system administrator who allocates access to those wishing to enter the system.

The principal tool for excluding others from a local system is called a "firewall." An external firewall is a barrier between the local system and the Internet that allows only authorized individuals to enter the local system. An external firewall thus gives

well defined, the relational nature of property rights becomes more clear.

Id at 46 ("The essence of private property is always the right to exclude others."). See also Loretto v Teleprompter Manhattan CATV Corp, 458 US 419, 435 (1982) ("The power to exclude has traditionally been considered one of the most treasured strands in an owner's bundle of property rights.") (citations omitted). Other traditional property rights include the right to possess, the right to use, the right to manage, and the right to security. See A.M. Honore, Ownership, in A.G. Guest, ed, Oxford Essays in Jurisprudence: A Collaborative Work 107, 112-24 (Oxford 1981).

Examples of Internet-related computer services include electronic mail, the ability to transfer files to and from other locations on the Internet, and the ability to access the World Wide Web.

The system administrator distributes passwords to local system users and sets policy regarding when and to what those passwords may be changed. Frequently, a system administrator will grant access privileges to users of other "friendly" systems. The system administrator monitors these connections and the activities of such users on the local system. The system administrator, in short, not only builds the moat around the castle but also decides when and for whom the drawbridge will be lowered.

See William R. Cheswick and Steven M. Bellovin, Firewalls and Internet Security:
the system administrator the power to exclude others. Internal firewalls allow the system administrator to control authorized users' activities on the system by limiting their access to different parts of the system. Just as an external firewall prevents outside individuals from entering without authorization, internal firewalls exclude users from certain parts of that system. For example, a university system administrator might set up several internal firewalls—in addition to the external firewall between the university system and the Internet—to separate the student and administrative domains of the system.

This regime of system-level boundaries, under which both the right to exclude others and the right to regulate computer use accrue to the system administrator, is now predominant on the Internet. From its inception, the Internet has linked computer systems. In most cases, the system administrator initially determines if and how her system should be linked to the Internet. It is not surprising, therefore, that system administrators established these links in a way that largely preserved the integrity of the system-level boundaries protecting their domains.

Nevertheless, this historical accident need not dictate the future course of Internet regulation. The law remains free to recognize other boundary models where it would be efficient or appropriate to do so.

B. The Open-System Model

The computer networks that preceded the Internet were designed to achieve two goals. The first was to allow researchers at different locations to share access to the limited number of supercomputing facilities then available. The second was to

Repelling the Wily Hacker 9, 53 (Addison-Wesley 1994) (distinguishing the "traditional" external firewall from the more unusual internal firewall). Cheswick and Bellovin describe a firewall as a “collection of components placed between two networks” that has the following properties: (1) “[a]ll traffic from inside to outside, and vice-versa, must pass through the firewall”; (2) “[o]nly authorized traffic, as defined by the local security policy, will be allowed to pass”; and (3) “[t]he firewall itself is immune to penetration.” Id at 9.

Id at 53-54.

10 The Internet descended, albeit indirectly, from Arpanet (Advanced Research Project Agency Network), which came online in 1969. The basic technology of the Internet was developed and tested on Arpanet. For example, the most popular feature of the Internet, electronic mail, or “e-mail,” was first tested on Arpanet in 1971. For a discussion of Arpanet and the circumstances surrounding its birth, see Aaron Zitner, A quiet leap forward in cyberspace: 25 years ago, the internet was born—and not many people noticed, Boston Globe A85, A96 (Sept 11, 1994).

11 Id at A96.
facilitate the communication of ideas among members of these geographically scattered research communities.\(^\text{13}\)

Initial efforts to develop cost-effective computer networks had little success. Transmitting a message from beginning to end over a single telephone line was both time consuming and prohibitively expensive. Researchers needed a system that would permit nearly instantaneous transmission of large amounts of information at low cost. Interconnected computer networks, incorporating packet switching, provided the solution.\(^\text{14}\)

The Internet has exceeded expectations as a cost-effective means for rapid communication between large numbers of people. It is estimated, for example, that thirty million messages are sent over the Internet via e-mail every day.\(^\text{15}\) The Internet brings together many people who would never meet under normal circumstances, and facilitates regular communication between people who would otherwise be isolated from each other.\(^\text{16}\)

In addition to facilitating personal communication between individuals, the Internet permits rapid dissemination of information to large audiences. Information placed on the Internet spreads quickly from one local network to another. Within days, a single piece of information might be replicated and disseminated to hundreds of different locations.\(^\text{17}\) The original desire to

\(^\text{13}\) Id.

\(^\text{14}\) Packet switching involves breaking down a message into smaller pieces, then sending each piece down a separate path over the network to its destination. The computers that make up the network are interconnected in a web-like lattice in which each location is linked to several others. This interconnection effectively results in an infinite number of possible routes to a destination. See Steven J. Vaughan-Nichols, *Inside the Internet: Millions Use It, But Few Understand How It Works*, Computer Shopper 602, 602-03 (Sept 1994). For further discussion of packet switching and the switching protocols used on the Internet, see Paul Merenbloom, *A Guided Tour of the TCP/IP Protocol and Its Related Tools*, Info World 61 (Aug 15, 1994). For more information about the Internet's interlinked networks, see generally Hearing on Internet Access before the Subcommittee on Science of the Committee on Science, Space, and Technology, 103d Cong, 2d Sess 125-39 (Oct 4, 1994) (testimony of Jim Williams, Executive Director, Farnet, Inc.).

\(^\text{15}\) Mike Toner, *Surfing on the Internet*, Atlanta J-Const F1, F1 (July 24, 1994).

\(^\text{16}\) See, for example, Mike Godwin, *The Electronic Frontier Foundation and Virtual Communities*, Internet WWW page available at <http://198.93.154.10/~tex/innkeeping> (version current on Jan 11, 1996) (on file with U Chi L Rev) (The cofounders of the Electronic Frontier Foundation, an organization dedicated to promoting Internet accessibility, used the Internet as a complement to their face-to-face contact. "In effect, they [became] next-door neighbors, although [one founder] lived in Pinedale, Wyoming, and the other in Brookline, Massachusetts.").

\(^\text{17}\) The case of the Internet Worm is illustrative. See text accompanying notes 45-62. The worm reached roughly 10 percent of the sixty thousand computers linked to the Internet within approximately three hours of being released.
provide a means for sharing information has, in fact, evolved into what could be termed a communal ethic on the Internet.\footnote{See Hearings on Internet Security before the Subcommittee on Science of the House Committee on Science, Space, and Technology, 103d Cong, 2d Sess 42, 49 (1994) (testimony of Dr. Vinton G. Cerf, President, Internet Society) ("The general spirit of openness was and continues to be instrumental in fostering rapid evolution of the Internet. . . . The Internet is filled with an endless variety of freely available information, largely organized and made available on a voluntary basis by users eager to share what they have learned or created.")} 

Unfortunately, this ability to spread information rapidly carries with it a great potential for harm. The Internet also facilitates the spread of computer viruses and the infringement of copyrights, to name but two examples.\footnote{See Johnson and Marks, 36 Vill L Rev at 513 (cited in note 3).} Actions taken on one system will often have consequences for users of other systems. For example, censorship of certain types of messages on a single system will not only prevent users of that system from receiving those messages but will also prevent users of the Internet from receiving those messages from that particular system. The latter effect may not be substantial in the particular instance. However, if widespread, system-level censorship will have a considerable effect on the life of the Internet as a whole. Sound Internet regulation, therefore, must consider the ability of actions to have consequences in Cyberspace that are both unpredictable and difficult to measure.

Accordingly, anyone crafting legal rules for Cyberspace must be careful to consider the impact that those rules will have in a world where consequences can follow quickly and unexpectedly. Given the difficulty, at the system level, of gauging the scope of an action's ramifications for the whole Internet, a legal approach that considered the network as a whole might be the best way to regulate behavior.

This type of Internet-wide approach to the regulation of Cyberspace is what this Comment terms an "open-system" conception of Internet regulation. Under this conception, the law would look to the actions taken in Cyberspace—considering their consequences and apparent motivations—rather than the boundaries crossed in the course of performing those actions. As will become clear below,\footnote{See Section II.B.} this approach has the advantages of considering the full extent of the world it hopes to regulate and of providing clear rules to govern individual conduct. However, the breadth of this approach increases the risk that the courts will
hesitate to craft rules of general applicability and will, instead, bog down in the particulars of each case. The result would be a legal regime characterized by inconsistent decisions and providing little guidance to those who must enforce and those who must obey the law.

The open-system conception has been proposed almost exclusively by those who think and write about the Internet. As I have noted, those who govern the Internet are, on the whole, adherents to the system-level conception of boundary definition.

C. The Individual-Level Boundary Model

In lieu of either system-level boundaries or an open regime with no boundaries at all, the law might define and enforce property rights in Cyberspace with reference to the individual user. Under this individual-level boundary model, the law would respect the boundaries established by individuals; the key feature would be the individual user’s choice to exclude others. In contrast to the open-system model, which would respect no boundaries at all, the individual-level model would respect a multiplicity of boundaries. But unlike the system-level model, under the individual-level model, system-level boundaries would be, from a legal perspective, permeable.

The level of exclusion under an individual-level regime would vary. For example, a user might choose to demarcate her entire account as inaccessible to others. If her need to exclude were more limited, she could allow access only to files or directories. Likewise, the pool of individuals granted access could be expanded or contracted as the user saw fit. The law would serve only to enforce the individual’s decisions.

II. ANALYZING VIRTUAL BOUNDARIES

This Section proposes legal rules for defining and governing boundaries on the Internet. Section A argues that the system-level boundary model is appropriate either where system administrators are best able to protect the interests furthered by legal regulation or where the users of a computer system share the relevant interests in common. Section B argues that the law should employ the open-system model, which conceives of the Internet as an amorphous and undefined collection of actors, whenever interests that are common to all users of the Internet would best be served by the application of universal rules. Finally, Section C advocates the individual-level boundary model for
those cases where either an individual interest has been recognized as worthy of protection (for example, where an individual’s privacy interest is at stake) or where an individual possesses unique knowledge of the potential value of a piece of information to others (for example, where an author is deciding how widely to disseminate her work).

The practical relevance of this Section is apparent. The law’s role in protecting individual privacy, encouraging commerce, and preventing theft or destruction of property has long been recognized. Other interests, although more theoretical, are no less important: promoting collective action, encouraging the internalization of external costs, and lowering monitoring costs. Although the law does not often seek to further these interests explicitly, a well constructed system of regulation should take them into account.

Some might question the practicality of such an ad hoc approach. One might argue, for example, that no workable legal standard could allow violations of system-level boundaries in commercial contexts but not in the context of corporate espionage. Courts may not have the resources or expertise to determine, on a case-by-case basis, whether a line has been crossed by a malicious trespasser or by an overzealous consumer. However, the facial similarity of the two situations requires rules that, rather than establishing hard and fast standards of general applicability, recognize the true nature of the suspect behavior. For example, crossing over a system-level boundary is not always malicious. In a world where hackers are but a small fraction of all Internet users, laws that make every violation of system-level boundaries a basis for liability will too often reach the behavior of individuals with innocent (perhaps even benevolent) intentions. Moreover, such rules could deter individuals roaming the Internet from exploring new areas, since boundaries that seem clear in the courtroom are often obscure in the virtual world. The present legal reliance on system-level boundaries might therefore deter the unrestricted interaction and exploration that this highly interconnected system was designed to facilitate.

Although this Comment proposes a system of boundary definition that rejects a universal approach, it does not completely reject the utility and use of bright-line rules. Although in most cases crossing a particular boundary should not itself be dispositional of liability, courts should be able to consider clear actions, such as crossing particular boundary lines, when determining guilt.
The pragmatic approach proposed by this Comment requires courts to consider more factors than is required under current law. However, it does not mark a sea change in cyber-jurisprudence. Indeed, scholars have already recognized that reliance on a single model of virtual boundaries provides an inadequate basis upon which to regulate the Internet. Further, many of the factors that this Comment urges be incorporated explicitly in legal rules already influence and guide court decisions.

A. The Uneasy Case for Current Law and the System-Level Boundary Model

1. Ensuring privacy and security.

The conventional wisdom about Cyberspace is that there are no mechanisms—legal, technological, or social—that can ensure the security of computer systems linked to the Internet and protect the privacy of individual users of those systems. The memory of the "Internet Worm" of 1988, the steady stream of reports about sophisticated computer hackers, and anecdotal accounts of private correspondence that turns out to be not so private have combined to shake individual and corporate confidence in the viability of the Internet as a secure mode of communication and commerce. It is not surprising, therefore, that ensuring privacy and security, both as an end in itself and as a means of inspiring public confidence, has become a principal goal of those who use and manage the Internet.

To date, the battles for system security and user privacy have been fought almost entirely at the system level. The sys-

---

21 See notes 62-68 and accompanying text.
22 See, for example, text accompanying notes 55-61.
23 See Calvin Sims, *Researchers Fear Computer 'Virus' Will Slow Use of National Network*, NY Times B6, B6 (Nov 14, 1988) (quoting Russell Brand of Lawrence Livermore National Laboratories: "There is a giant danger that people will overreact and to protect themselves will not use the network and thus reduce its effectiveness.").
24 See, for example, Mary B.W. Tabor and Anthony Ramirez, *Computer Savvy, With an Attitude: Young Working-Class Hackers Accused of High-Tech Crime*, NY Times B1, B7 (July 23, 1992).
25 See, for example, Dan Pacheco, *Easy-to-Crack Passwords Leave E-Mail Vulnerable*, Denver Post 1E, 1E (Oct 27, 1994) (discussing ways to protect e-mail communications).
26 This is not to say that an individual cannot protect her own privacy on the Internet using a variety of measures, ranging from the very simple to the extraordinarily complex. See generally Alfred Poor, *Watch Your Back: It's a dangerous digital world, so protect your data*, Computer Shopper 550 (Mar 1995). For example, all users can protect themselves to a considerable degree by varying their passwords frequently and by being careful to avoid dictionary words and words and names of particular significance to the user. See
tem administrator, charged with constructing and maintaining the system-level firewall, is in the best position to protect security and privacy through use of that firewall. The firewall prevents infiltration of the system not only by shielding it from viruses spreading across the Internet but also by shutting out hackers set on either sabotaging the system or accessing individual files and e-mail records.

Federal law regarding privacy and security reflects the use of system-level boundaries. The Electronic Communications Privacy Act of 1986, for example, accepts the system border as the boundary to be protected. Liability for stealing an electronic file, for instance, requires gaining unauthorized access to a computer system or exceeding the authorized level of access on that system. Similarly, the Computer Fraud and Abuse Act of 1986 makes either accessing a computer system without authorization or exceeding the authorized level of system access the initial


27 For an excellent introduction to the technology of Internet security, see generally Cheswick and Bellovin, *Firewalls and Internet Security* (cited in note 9). For a discussion of firewalls and the gateways through them, see id at 51-83.


29 Pub L No 99-508, 100 Stat 1848, codified in relevant part at 18 USC § 2701 (1994). Section 2701(a) provides that anyone who:

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

30 See *American Computer Trust Leasing v Jack Farrell Implement Co.*, 763 F Supp 1473, 1495 (D Minn 1991), aff'd, 967 F2d 1208 (8th Cir 1992) (Although "the Electronic Communications Privacy Act [ ] bars unlawful access to stored communications," parties that had consented to another party's access cannot now claim that such access was unauthorized.).
threshold for criminal liability.\textsuperscript{31} State laws reflect a similar focus.\textsuperscript{32}

Although legal regulation keyed to system-level boundaries will not guarantee system security in all circumstances,\textsuperscript{33} it does have several advantages over both the open-system and the individual-level boundary models. First, the system administrator is more likely than the individual users of her system to possess the technical expertise needed to protect security and privacy effectively. It can also be expected that those technologically-savvy individuals who present the greatest threat to system security and user privacy—computer hackers and corporate spies—will continue to increase their knowledge and enhance their skills and techniques. The efficient solution to increasing levels of criminal competence would be to place the burden of keeping abreast of technological developments on a single system administrator, rather than on each of the many users of her system.

Second, many of the technologies that protect security and privacy operate most efficiently at the system level. It is more efficient to monitor a single firewall between the system and the Internet than it would be to monitor multiple firewalls between each and every account on the system. A single program monitoring system-wide usage, for example, uses less disk space and computer time than hundreds of customized programs, each monitoring the activity around a single user’s account.

Third, the system-level boundary model provides a clear rule for courts and criminals alike to use when determining whether a legal violation has taken place. When an individual is found to have accessed a system without authorization, the law will hold her liable. By contrast, adopting the individual-level model would entail a preliminary determination, by courts and Internet users alike, of whether an individual user has created a legally protected boundary around her account or a particular piece of information contained therein. An open-system boundary model would, of course, establish no clear "line" between liability and nonliability; the court would be required to scrutinize the character of an

\textsuperscript{31} Pub L No 99-474, 100 Stat 1213, codified at 18 USC § 1030 (1988). Recent amendments to the Act are discussed below. See notes 63-68 and accompanying text.

\textsuperscript{32} See Davis, Note, 72 Wash U L Q at 428-40 (cited in note 28) (discussing state and federal law and proposing federalizing the law in this area); Anne W. Branscomb, Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime, 16 Rutgers Computer & Tech L J 1, 30-44 (1990) (discussing criminal liability under state statutes).

\textsuperscript{33} For example, authorized users may subvert system security.
individual's conduct before making a determination as to liability.

Nevertheless, adopting a system-level threshold in matters of both privacy and security ignores the distinct natures of the interests being protected. System security is a goal shared equally by all users of a particular system. No individual user's interest in preventing the introduction of computer viruses onto a system differs qualitatively from any other user's. Respect for system-level boundaries permits a collective response to this common threat.

Privacy, on the other hand, is an individual concern, the demand for which varies from person to person. Some would take offense at the notion that anyone might try to access their account. Such people would consider it irrelevant whether an electronic visitor was merely looking for files of general interest or attempting to read private correspondence. Other users—perhaps for the purpose of inviting commerce, perhaps for the purpose of contributing to the Internet community—would allow limited access even to their personal files. While e-mail probably would be off limits, files of general interest might be open for either unrestricted downloading or purchase. Finally, some users may not care about privacy at all.

A system-level approach does not recognize this crucial distinction between privacy and security interests. It simply places a wall between the system and the Internet. Although this approach protects the security of all and the privacy of the most private, it does not respect the interests of those who desire a more open Internet. The system-level approach places the burden upon these individuals, whose accounts are made inaccessible to others as a default rule, to make their information public. Take, for example, a law student who stores copies of old class outlines in her account on the school's computer system. If she is more or less indifferent about whether other students are able to access these outlines, then our choice of boundary model matters. If we adopt the individual-level model, under which the user must affirmatively delineate the boundaries that she wants the law to protect, then other students will be able to access these outlines. The same holds true if we adopt the open-system model. If, however, we adopt the system-level model, then these outlines will, absent affirmative action on the part of our hypothetical law student, remain inaccessible to other students; the system administrator, by choosing a default rule of privacy, will have diminished the supply of information available to members of the
Internet community when no one had any desire to keep the outlines out of circulation. Such a default rule, therefore, might be not only contrary to the communal spirit of the Internet, but also highly inefficient from a commercial and research perspective.

When regulating the Internet, legislators, lawyers, and judges should consider which interests they are seeking to advance. By tailoring solutions to fit particular problems, the law could encourage the Internet to tailor its defensive mechanisms to be more responsive to these particular interests.

Four examples illustrate this point. In the first example, someone acquires unauthorized access to a system and intentionally destroys a portion of the programming that runs the system. In the second example, an authorized user intentionally destroys another portion of that programming. In the third example, another person acquires unauthorized access to a system and reads several e-mail files that have been left unprotected by their owner. In the final example, an authorized user reads the same unprotected e-mail files. The first pair of examples—both of which would violate current federal laws against computer hacking—clearly implicates the interest in system security; the second pair implicates the privacy interest of the e-mail owner.

These examples reveal, first of all, that threats to both privacy and security cannot be met entirely at the system’s boundary. An authorized user of a system may disable that system’s security or violate the privacy rights of other system users as easily as an unauthorized intruder. In fact, one would expect that serious threats to privacy come from associates seeking personal information about colleagues on a shared system more frequently than they come from strangers wandering on the Internet. Nevertheless, in the context of system security, the system administrator remains best equipped to deal with both internal and external threats. Effectively defending both internal and external firewalls, the task of the system administrator, would have prevented the violations of system integrity in the first and second examples. The law has good reason, therefore, to recognize system-level boundaries in these contexts.

34 For example, an individual user of a system operating on UNIX, the most common system operating software, can take several steps—from simply making her files unreadable by other users to encrypting those files—to protect her privacy on the Internet. In the hypothetical, the user has taken no steps to protect her files, so they may be read by other authorized users of the system.
In the context of individual privacy, however, the individual user is in the best position to take the necessary steps to protect, or at the very least to request that others respect, her privacy. As discussed below, the authorized user in the fourth example would not and should not be deterred from accessing readable files on her own system. The authorized user simply should not be punished for reading files that have, for whatever reason, been left open to users of the system. Absent any notice that these files, left open to the public, are not intended for public consumption, such punishment would not only be unfair but would also discourage vigorous use of computer systems. The burden should be placed on the user who wants privacy to take at least minimal steps to protect it.

The interesting question is whether the unauthorized user in the third example should be punished. On one hand, this user has clearly gained access to the computer system. On the other hand, the unauthorized user may have accessed files that were intentionally left accessible by the "victim" with the hope that they be read and distributed by users of other systems. Whether or not the unauthorized user should be held liable turns on a fundamental policy choice that implicates many of the other interests that this Comment addresses: whether cyberlaw should seek to protect individual privacy at the expense of promoting the free flow of information and the full use of the powers of the Internet. This fundamental issue is best left to the political process.

2. Lowering monitoring costs.

The need to monitor the uses made of property might be another reason to adopt the system-level boundary model. As Robert Ellickson recently noted, one of the benefits of private property and its concomitant right to exclude lies in the reduced costs of monitoring the activities of others: "A key advantage of individual land ownership is that detecting the presence of a trespasser is much less demanding than evaluating the conduct of a person who is privileged to be where he is. Monitoring boundary crossings is easier than monitoring the behavior of persons situated inside boundaries."
This reasoning seems to support the current system-level approach to boundary definition on the Internet. Monitoring is necessary to prevent malicious use of a system and to protect the system against computer viruses. Vis-à-vis individual users, the system administrator is in the best position to perform the monitoring role, and the simplest way to monitor the system is to regulate access. In short, it is easier to detect an intruder than to watch the behavior of those already inside.

Although this argument is not without merit, it proves too much in a world where resource depletion is not a significant concern. Not every use of a system will damage it. Most uses, in fact, will have little or no deleterious effect, and quite often such uses will benefit all parties concerned.

Moreover, the system operator frequently does not know the identities of her system’s users. She may not know the communities to which they belong or the uses they make of the Internet. Her governance of the system has little, if anything, to do with the particular uses those on her system make of the Internet: her goal is simply to ensure the smooth and efficient use of the system. For this reason, her monitoring, while facilitating the efficient use of the system, does little to promote the law’s goals of regulating behavior on the Net as a whole.

Finally, the system administrator is accustomed to making rules of general applicability. She is not in the business of regulating individual conduct on a case-by-case basis. It would, in fact, be an extraordinary expansion of the system administrator’s role to require her to monitor such conduct. In the interest of efficiency and out of a justifiable desire to avoid criminal liability, the system administrator, if legally assigned a monitoring function, would likely create system-wide rules that are overrestrictive. For example, consider a system administrator confronted with the problem of obscene images being transferred onto her system. It would be much easier for her to identify files that contain images than it would be for her to identify those particular image files containing obscene materials. In order to be certain that she eliminates the pornographic image files, the system administrator might prohibit the storing of all image files on her system so that she will achieve her goal without having to devote substantial amounts of time to monitoring the contents of the files stored on her system. She would promulgate an overinclusive rule in order to promulgate an easily enforceable rule.
3. The problem of externalities.

One justification for a system of private property is found in the need to encourage users of scarce resources to internalize the external costs of their activity.\textsuperscript{37} Giving individuals rights of ownership in particular resources is one way to force them to internalize such costs.\textsuperscript{38} Each owner has incentives to use her resources efficiently and ensure that others do the same.\textsuperscript{39}

This externalities argument applies both to local computer systems and to the use of the Internet as a whole.\textsuperscript{40} Computer systems have finite computing and storage capacity.\textsuperscript{41} There will generally be more than one user on any system. Each user should be encouraged to use the system in a way that permits every other user to make efficient use of the system.

At the computer system level, therefore, the externality argument supports system-level boundary definitions and argues strongly against the open-system model. The externality argument most strongly supports system-level rules that regulate the quantity of use each individual may make of a system. The individual determinations of users as to how much use is appropriate—which carry the day in the open-system model—are inadequate because they are not based on the capacity of the system as a whole, but rather on the users' own needs and interests. The system administrator, by contrast, is in a position to monitor and regulate according to the effects of individual uses on the system as a whole.

At the level of the Internet, the externality argument provides little support for any particular boundary model. There is almost no conceivable boundary that would, if afforded legal

---


\textsuperscript{38} See Demsetz, 57 Am Econ Rev at 348 (cited in note 37) ("A primary function of property rights is that of guiding incentives to achieve a greater internalization of externalities.").

\textsuperscript{39} Id at 355 ("If a single person owns land, he will attempt to maximize its present value by taking into account alternative future time streams of benefits and costs and selecting that one which he believes will maximize the present value of his privately-owned land rights.").

\textsuperscript{40} The need to internalize the costs associated with the "use" of information available on the Internet is discussed in Section II.C.3.

\textsuperscript{41} By "computing" capacity I mean the power of a computer to run programs, make calculations, and perform other such functions. By "storage" capacity, I mean the total quantity of information (files measured in bytes of data) that can be stored in the system's memory.
significance, force the thirty million Internet users to internalize the costs their actions impose on the whole Internet. As a threshold matter, the boundary models that I have proposed simply would not allow for the level of aggregation that would render individual activities relevant at the level of the whole Internet. Moreover, a user is unlikely to view the transfer of a single document differently, however large that document might be, depending on whether she is transferring the document in a world characterized by a system-level, individual-level, or open-system boundary conception.

Thus, in Cyberspace, the problem of externalities is best addressed by adopting system-level boundaries. Although no strategy will solve the problem at the level of the whole Internet, a strategy that relies on system-level boundaries will at least ensure that users internalize the costs of their system use. To address the problem at one level is better, in the final analysis, than to leave it unchecked at every level.

4. Facilitating coordinated action.

Granting ownership rights to a single person facilitates the use of a piece of property. In a world of communal ownership, an individual wishing to use a piece of property would have to get the permission of all others with a similar claim to it. In a world of individual ownership, the individual may unilaterally decide to use the property as she desires.

This aspect of private ownership, when coupled with the particular expertise of the system administrator, supports the adoption of the system-level boundary model when technological actions are at issue. On the vast majority of systems, the system administrator will have more technological savvy than any of the system's individual users. She should, therefore, be given a free hand in making decisions regarding her system's level of technology and the uses to which it should be put.

Most actions that will be taken on the Internet, however, will not involve the type of collective action or technological problems best solved at the system level. This is largely a result of

42 This is true for several reasons. First, the cost of the action of any one individual, in relation to the Internet as a whole, is unlikely to be significant. Second, it is difficult to conceive of a system of boundaries that would lead to rules that affect all thirty million Internet users in the same way. If the Internet is overused, the solution will have to come from some universal mechanism, perhaps time- or quantity-based user fees that create the proper incentives to internalize costs.
the Internet's high level of interconnectivity. Actions taken by a system administrator may have adverse effects on systems other than her own. For example, consider a system administrator who decides to filter out political messages passing through her system. This action will impact users—both of the home system and of all other systems—in two ways. First, users will be cut off from each other. Users on the home system will not receive political information from other systems; they will not contribute to the political discussions occurring on those systems. Likewise, users on those other systems will not benefit from the contributions that would have been made by users of the regulated system. Second, rather than providing a conduit for the dissemination of information, the regulated system will become a filter. Where, in the past, a message received by the regulated system would likely have been retransmitted to other users, that message will now be deleted. The free flow of information will therefore be slowed, to some degree, at the Internet level.

5. The system-based model assessed.

As should now be clear, there are times when the system-based model should be adopted in Cyberspace. When regulations deal with technical or technological issues, such as computer security, or when the system's physical machinery provides the most sensible unit for regulation, as when regulations aim to control the use of system hardware, system-level boundaries make sense. In short, when interests are shared by system users and are furthered best by regulation at the system level, then system-level boundaries should be respected.

Nevertheless, the prominence of geographically defined communities in the physical world may be exercising an undue influence over legal thinking in and about Cyberspace. In the physical world, communities of interest generally overlap with physical communities. For example, a town may be predominantly blue-collar or Catholic or Republican. In these situations, respect for geographic regions as units of regulation makes sense because it allows like individuals to be treated alike.

In Cyberspace, system-level boundaries provide a convenient analogy to these familiar physical boundaries. Assuming that users of a particular system should be treated alike, however, often overlooks the unbounded nature of Internet communities.43

---

43 In recent years, the Internet has seen the birth of "virtual communities." In the
We should not allow preferences formed in a physical world of physical boundaries to exercise undue influence over our boundary choices in Cyberspace. Although computer systems may offer a ready analogy to land parcels, our boundary choices in Cyberspace must not be predetermined; we must consider alternative boundary models ready to acknowledge their respective advantages and disadvantages when compared to system-level boundaries.

B. Universal Interests and the Open-System Model

1. Protecting the Internet.

Although the battle for system security is generally best fought at the system level, in some circumstances the law must address network security, an interest shared by all users of the Internet, at a universal level. Not every security threat comes from local computer hackers, and not all hackers limit their attacks to a single system.\(^\text{44}\)

The classic example of a global assault on Internet security and of the inability of the system-level boundary approach to deal with such threats is the release of the “Internet Worm” by Robert Tappan Morris. In the fall of 1988, Morris, a graduate student at Cornell University, discovered several flaws in UNIX, flaws that would allow him free access to systems across the country.\(^\text{45}\)

Internet environment, where any person can contact any other person with relative ease, the problem naturally arose of how to communicate with members of one distinct group. The answer was the creation of idea-based communities on the Net that are differentiated along lines of common interest. These have taken the form of systems devoted to particular interests or dispositions. See John Coate, *Cyberspace Innkeeping: Building Online Community*, Internet WWW page available at <http://198.93.154.10/~tex/innkeeping> (version current on Jan 11, 1996) (on file with U Chi L Rev). See also Godwin, *The Electronic Frontier Foundation and Virtual Communities* (cited in note 16). Usenet newsgroups allow people interested in particular topics, ranging from philosophy to alternative sexual practices, to post messages which can then be read by anyone. List servers work by sending each piece of mail received by the list server to every person who has subscribed to the service.

In some cases, system-level boundaries might best be disregarded in favor of lines respecting the interest-based divisions created in Cyberspace. Many users of the Internet act within communities that are spread over numerous systems, and, frequently, their behavior is best regulated within these communities rather than within the confines of their home systems. For a discussion of community standards in the context of obscenity prosecutions, see Edward A. Cavazos and Gavino Morin, *Cyberspace and the Law: Your Rights and Duties in the On-Line World* 94-95 (MIT 1994); Godwin, *Virtual Community Standards* (cited in note 2).

See, for example, Schwartz, *Chipping in to Curb Computer Crime*, Wash Post at A1 (cited in note 2) (discussing the hunt for “computer terrorist” Kevin D. Mitnick, who allegedly penetrated computer systems around the world).

For a full discussion of the case, see generally Jonathan Littman, *The Shockwave
Morris then wrote a program, known as a “worm,” that would travel across the Internet and use the holes he had discovered to gain access to other systems.\textsuperscript{46}

At eight p.m. on November 2, 1988, Morris released the worm onto the Internet. Before sunrise, the worm had infected over six thousand computer systems, including those at the University of California at Berkeley, the Lawrence Livermore Laboratories, and the Los Alamos National Laboratory.\textsuperscript{47} The total cost of eradicating the Internet Worm and of lost computing time has been estimated at $96 million to $1.1 billion.\textsuperscript{48}

According to Morris, he did not intend for his program to damage systems or files. Rather, he designed it to reveal the security flaws that he had discovered in the programming that runs most computers linked to the Internet.\textsuperscript{49} However, the worm replicated itself at a much faster rate than Morris had anticipated, infecting many computers repeatedly.\textsuperscript{50} As more copies began to run on each system, each system operated at increasingly slower speeds until, eventually, it either crashed or slowed to the point of being unusable.\textsuperscript{51}

On appeal from his conviction under the Computer Fraud and Abuse Act (“CFAA”),\textsuperscript{52} Morris argued that the district court had misinterpreted the statute’s intent requirement.\textsuperscript{53} Relying


\textsuperscript{46} See Brett Glass, \textit{Dissecting the Internet Worm: How the Program Worked}, Infoworld \textbf{S9}, S9-S10 (Jan 9, 1989). The first and most potent tactic used by the worm was password cracking, or decrypting password files on various systems. The second attack exploited a bug in an otherwise friendly system program known as the “finger daemon.” The worm also spread by sending copies of itself to remote locations using a program called Sendmail.


\textsuperscript{48} Branscomb, 16 Rutgers Computer & Tech L J at 6-7 (cited in note 32).

\textsuperscript{49} \textit{United States v Morris}, 928 F2d 504, 505-06 (2d Cir 1991).

\textsuperscript{50} Morris had programmed the worm to ask each system it encountered whether there was already a copy of the program running on that system. If it received an answer of yes, the attacking copy would self-destruct. However, Morris recognized that a programmer could simply tell a system to answer these queries with a yes, even if no copy of the program was running. He therefore instructed the program to infect one out of every seven times that it received a yes response. As it turned out, seven was far too low a number. Id at 506.

\textsuperscript{51} Id.


\textsuperscript{53} Morris, 928 F2d at 506-08. At the time, § 1030(a)(5), under which Morris was convicted, stated that anyone who:
on the punctuation of § 1030(a)(5), the lower court had concluded that the intent requirement applied only to the act of accessing the system, and not to other elements of the crime.\textsuperscript{54} Morris contended that the intent requirement applied to each element of the offense, requiring not only an intent to access a federal interest computer, but also an intent to “prevent[ ] authorized use” of the computer.\textsuperscript{55}

The Second Circuit agreed with Morris that punctuation did not determine the proper interpretation of § 1030(a)(5), but went on to find that the legislative history supported the district court’s interpretation of the statute’s intent requirement.\textsuperscript{56} The court quoted a report of the Senate Judiciary Committee that concluded that “[t]he substitution of an ‘intentional’ standard is designed to focus Federal criminal prosecutions on those whose conduct evinces a clear intent to enter, without proper authorization, computer files or data belonging to another.”\textsuperscript{57} According to the court, this suggested Congress was principally concerned with the act of entering the system, not any ensuing damage.\textsuperscript{58}

Morris also argued that § 1030(a)(5) did not apply to his actions because he had not accessed, in the normal sense of the word, any system for which he had not already obtained authorization.\textsuperscript{59} He was authorized to use the computers at Cornell, Harvard, and Berkeley, from which he launched his program. He was authorized, on those systems, to use Sendmail and finger daemon, the features via which his worm gained access to other systems. Morris argued, therefore, that he had at most exceeded his authorized access on those systems, but had not gained “unauthorized access.”\textsuperscript{60} The court rejected this argument:

\begin{quote}
(5) intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby —

(A) causes loss to one or more others of a value aggregating $1,000 or more during any one year period; . . .

shall be punished as provided . . . .
\end{quote}

\textsuperscript{54} In particular, the court relied on the comma between “authorization” and “and.”
\textit{Morris}, 928 F2d at 507. See text of statutory provision in note 53.
\textsuperscript{55} \textit{Morris}, 928 F2d at 507.
\textsuperscript{56} Id at 507-09.
\textsuperscript{57} Id at 508, quoting Fraud and Abuse Act, S Rep No 99-432, 99th Cong, 2d Sess 6 (1986), reprinted in 1986 USCCAN 2479, 2484 (emphasis added).
\textsuperscript{58} \textit{Morris}, 928 F2d at 509.
\textsuperscript{59} Id.
\textsuperscript{60} Id at 509-10.
While a case might arise where the use of SEND MAIL or finger demon falls within a nebulous area in which the line between accessing without authorization and exceeding authorized access may not be clear, Morris's conduct here falls well within the area of unauthorized access. Morris did not use either of those features in any way related to their intended function. He did not send or read mail nor discover information about other users; instead he found holes in both programs that permitted him a special and unauthorized access route into other computers.61

The Morris case caused considerable controversy in the legal and computer communities.62 The source of this controversy is the statute under which Morris was prosecuted, the CFAA, which focuses on system-level boundaries.63 In upholding Morris's conviction, the Second Circuit concluded that the intent requirement applied only to accessing a computer system without authorization. So long as the access is intentional, it does not matter that the damage is inadvertent. In other words, the mens rea requirement of the CFAA is applied to the potentially benign act of accessing a system, rather than to the acts that would actually harm the system or the accounts of its users.

Legal commentators have noted the difficulty of prosecuting the creators of computer viruses under the CFAA,64 and Congress recently responded by eliminating § 1030(a)(5)'s system-level focus and de-emphasizing the unauthorized-access requirement of the old statute.65 Section 1030(a)(5) now focuses on the

---

61 Id at 510.
63 See note 31 and accompanying text.
64 See, for example, Leahy, 5 Harv J L & Tech at 22 (cited in note 2) ("[A]lso demonstrated by several recent computer abuse incidents, the most severe forms of computer damage are often inflicted on remote computers to which the violator never gained 'access' in the commonly understood sense of that term."); Davis, Note, 72 Wash U L Q at 426 (cited in note 28) (While a cause of action brought under the CFAA requires proof of intentional unauthorized access to a computer, most malevolent software creators intend to access only a single computer.); Susan C. Lyman, Note, Civil Remedies for the Victims of Computer Viruses, 11 Computer/L J 607, 609 (1992) (noting that the CFAA lacks specific statutory language that would facilitate convictions for computer virus offenses).
65 18 USC § 1030(a)(5) (1994), as amended by the Computer Abuse Amendments Act of 1994, Pub L No 103-322, 108 Stat 2097, now imposes liability upon those who knowingly cause the transmission of "a program, information, code, or command" that causes damages in excess of $1,000 (or interferes with medical care or treatment) if the person intended to cause damage or acted with reckless disregard of the risk of damage.
act of transmitting malicious code, an act the perpetrator need only knowingly perform.\textsuperscript{66} Those who intend to cause damage and who knowingly transmit malicious code may be fined and imprisoned for up to ten years.\textsuperscript{67} Likewise, those who transmit a virus with "reckless disregard of a substantial and unjustifiable risk" that the transmission will cause damage may be fined and imprisoned for up to one year.\textsuperscript{68}

The congressional revision of the CFAA seems wise. Under the old statute, the focus of a prosecution was on the perpetrator's intent to violate a system-level boundary. Such reliance on system-level boundaries resulted in prosecutions, like the \textit{Morris} case, that focused not upon the resulting harm or the actions that proximately caused that harm but upon an action frequently incidental to causing harm. The transmission of the virus is now the actus reus. The severity of the punishment, quite logically, turns on the defendant's intent with respect to bringing about the harm.

More importantly for purposes of this Comment, the amendment also recognizes that such harms frequently do not occur at the system level or even within systems. For example, a virus could be designed to clog the Internet itself, cutting off communications between systems and individual users. The old statute, with its threshold requirement of unauthorized access of a particular system, could not have reached these crimes. The new statute remedies this inadequacy by recognizing damage to networks, individual computers, programs, and files as a basis of liability. The law has grown to recognize both that individually established boundaries can be violated and that the network as a whole may form the proper level at which to conduct legal analysis.

The \textit{Morris} case revealed the inadequacy of statutory schemes that blindly accept system-level boundaries as an exclusive regulatory baseline. However, neither Congress nor the courts have consistently applied the lesson of \textit{Morris}. The CFAA, to provide just one example, still relies on unauthorized access in all of its other provisions.\textsuperscript{69} Under the system-level approach

\footnotesize{\textsuperscript{66} 18 USC § 1030(a)(5)(A)-(B).
\textsuperscript{67} 18 USC § 1030(a)(5)(A)-(B).
\textsuperscript{69} 18 USC § 1030(c)(4) (1994).
\textsuperscript{69} 18 USC § 1030(a)(1)-(4) (1994), as amended by the Computer Abuse Amendments}
exemplified by *Morris*, courts were—and, in other contexts, will be—forced to look to incidental behavior when determining liability. The open-system conception, now partly adopted in the CFAA, will allow courts to consider the damaging behavior at which the law should aim when determining liability.

When evidence of behavior and damage is difficult to obtain, legal reliance on system-level boundaries makes sense. For example, under some circumstances, it may be impossible to show that someone has read a sensitive file on a system. In this situation, imposing liability on a trespasser who has crossed a system boundary will make sense.

In a case like *Morris*, however, basing liability for a distinct act—be it reading electronic mail, spreading a virus, tampering with system software, or deleting valuable files—on the act of crossing a system boundary makes for a system of regulation that takes no account of either the activities it aims to regulate or the level of regulation appropriate to each of these distinct activities. The open-boundary model will allow for a system of tailored regulation on the Internet.

2. Protecting scarce resources.

The social cost of resource depletion is one externality that a system of private ownership should force owners to internalize.70 A problem, sometimes referred to as the "tragedy of the commons," results when a person has unrestricted use of a communal resource.71 In the absence of legal rules, that person can be expected to deplete the resource to the point of exhaustion without considering either the desires of others or the potential needs of future generations.

This problem, however, does not exist with informational resources.72 Copying a file, unlike pasturing animals or hunting

---

Act of 1994, Pub L No 103-322, 108 Stat 2097 provides liability for whoever:

(1) knowingly accesses a computer without authorization . . .;
(2) intentionally accesses a computer without authorization . . .;
(3) intentionally, without authorization to access any computer . . . accesses such a computer . . .;
(4) knowingly and with intent to defraud, accesses a Federal interest computer . . . .

71 Id at 1244.
72 By "informational resources," I mean a file or other piece of data transmittable over the Internet.
beaver, does not deplete the resource. As others have noted, copying a file actually doubles the quantity of that resource. With respect to informational resources, then, the existence of any legal boundaries will decrease the potential availability of informational resources on the Internet.

Courts and legislatures should not fashion rules or recognize boundaries that prohibit the dissemination of documents intended for distribution. In such situations, the open-system model is clearly most appropriate because it will facilitate the free flow of this informational commerce.

3. Ensuring development of the Internet.

Unblinking observance of system-level boundaries will stunt the development of the Internet itself. The more that individuals are encouraged to think in terms of their own systems, the less inclined they will be to think of the Internet as a whole. Conversely, a system of legal rules that respects, in appropriate circumstances, boundaries other than at the system level will be more likely to encourage the technological development of the Internet.

For example, a shift away from reliance on system-level boundaries and toward the open boundary model would create incentives for developing technologies that could overcome many of the collective action problems on the Internet. A system linked to the Internet is only as secure as the most insecure system to which it grants access. If, however, the law shifted its focus from individual systems to the Internet as a whole, all users would have incentives to develop universal solutions to the problems of Internet security. A single intelligent network could perform many of the functions now being served by the countless firewalls that protect individual systems.

---

73 See Hardin, 162 Science at 1243 (cited in note 70) (pasturing animals); Demsetz, 57 Am Econ Rev at 351-53 (cited in note 37) (hunting beaver).

74 See John Perry Barlow, Selling Wine Without Bottles: The Economy of Mind on the Global Net, Internet WWW page available at <http://www.eff.org/pub/Publications/John_Perry_Barlow/HTML/idea_economy_article.html> (version current on Jan 11, 1996) (on file with U Chi L Rev) ("The central economic distinction between information and physical property is the ability of information to be transferred without leaving the possession of the original owner. If I sell you my horse, I can't ride him after that. If I sell you what I know, we both know it."). Admittedly, this argument assumes a world of preexisting resources on the network. The need to preserve incentives to produce is discussed in Section II.C.3.

75 For a fuller discussion of the current trend toward developing a "smart network," see generally Andy Reinhardt, The Network With Smarts: New Agent-based WANs Presage...
A regulatory system that relied on system-level boundaries would also tend to produce legal rules that would hold system administrators liable for the actions of individuals over whom system administrators exercise little, if any, real control. For example, a Florida bulletin board service recently lost a copyright infringement case involving pictures that users had uploaded to the system. The system operator was unaware that the pictures were on his bulletin board, much less that they were copyrighted. A similar result was obtained in a case involving uploaded copies of video games. Government law enforcement activity, moreover, has often been arbitrary, excessive, and, in perhaps one case, a violation of the civil rights of a bulletin board operator. The result has been confusion among bulletin board operators and a general sense of fear in the Cyberspace community.

This fear has not been confined to operators of bulletin boards. Recently, Carnegie Mellon University decided to restrict access to Net sites where pornographic images are available. Other universities are likely to follow suit. Thus, the result of legal rules that impose liability at the system level is not difficult to predict. If a university faces civil or criminal liability for materials placed onto its system by a user without its knowledge, it will craft increasingly stringent rules to prevent users from gaining access to those materials. Such restrictions will hobble the Internet as a common resource.

---

the Future of Connected Computing, Byte 51 (Oct 1994).

76 Playboy Enterprises, Inc. v Frena, 839 F Supp 1552, 1554-59 (M D Fla 1993).

77 Id at 1554.


79 See, for example, Steve Jackson Games, Inc. v United States Secret Service, 36 F3d 457, 459 (5th Cir 1994), in which seizure of bulletin board system computer, coupled with reading and deleting the e-mail on the system, was held to violate the Privacy Protection Act of 1980, 42 USC §§ 2000aa et seq (1988). For a discussion of the Steve Jackson Games case and the Secret Service sting operation of which it was a part, see generally Barlow, Crime and Puzzlement (cited in note 2); Ric Manning, Feds pull plug on Louisville bulletin board, Louisville Courier-Journal E5 (Oct 16, 1994).

80 See generally Manning, Courier-Journal E5 (cited in note 79).

81 George McLaren, Colleges begin to limit access to pornography on computer systems, Indianapolis Star D1 (Jan 1, 1995). Carnegie Mellon University restricted access to several bulletin board services as well as Usenet newsgroups that carry sexually explicit images. On the decision, Erwin Steinberg, Vice Provost for Education at Carnegie Mellon, commented: "We were just told by our lawyers we were vulnerable." Id.

82 Id.
Adopting the open-system model as the basis for apportioning responsibility and liability would, by contrast, tend to open up the Internet. Consider a university president who must decide whether to provide local high schools with access to the university computer system. A system-level model would force the university president to say no to the schools' request; she could not risk subjecting the university to liability not only for the actions taken by the children on the Internet but also for any harms—pedophilia and child pornography spring quickly to mind—that might come to the children as a result of their contact with the Internet. Under an open-system model, however, expanding the scope of service provided would not expand one's exposure to liability. Liability would be imposed on those directly responsible for the harms being regulated—in this case, those individuals who placed the child pornography on the Internet or who contacted children for reasons in no sense benign. Our hypothetical university president, therefore, would find no grounds for hesitation in the legal rules that would evolve under the open-system model.

4. The problems of allocation and access.

As described above, the Net was born out of a desire to allow scientists at different locations to share the use of powerful computers at other locations. See text accompanying note 12. This use is no longer a dominant feature of the Internet. Most current users do not need access to computer power in the way advanced researchers in the sciences do. Nevertheless, it is worth considering the potentially negative effects that the system-level boundary model could have on the future development of a nationwide base of computer power.

Computer time is a limited resource, and an operable computer that is unused or underused is a wasted resource. The law should take account of this problem when developing its baseline rules for the Internet; we must recognize, at every step in the evolution of a law of Cyberspace, that the more permeable system boundaries become, the more those who need to will cross

---

83 See text accompanying note 12.
84 Guaranteeing access to the Internet is an issue of increasing concern. See note 87 and accompanying text. If Net access were extended to secondary schools and other lower level educational institutions, then the benefits of accessible computer power would become more pronounced. Although secondary school students have little to offer immediately in return for the information and computer resources they might use, the long-term societal benefits of allowing them access to information and computer resources are apparent.
those boundaries and make use of those systems. Legal rules could, for example, encourage users to more efficiently allocate computer time, shifting operations from systems that are overused at certain hours to systems that are underused at those times.

The same argument applies to the use of computer memory. A computer system with substantially more memory than its users require could be used to store information for others, perhaps by creating a duplicate "FTP site" for anonymous downloading.85 Such an arrangement would facilitate information distribution without any serious impairment to the owner of the underused system.86 Thus, a system of open boundaries would facilitate efficient allocation of computer power by permitting computer users on overused systems to execute applications and store data on underused systems.

Finally, as the Internet continues to develop, not only as a commercial mechanism but also as an educational resource and communications medium, it will become increasingly desirable to ensure that the underprivileged gain access.87 Thus, legislatures and courts should consider whether the legal rules they devise will likely result in a more open system, to which such groups will be able to gain access, or a more closed system, from which those lacking financial and technological resources will be excluded. The example of the university president again comes to mind. The law should create rules that will, at the very least, not attach potential liability to altruistic behavior. In short, if our hypothetical university president wishes to provide Internet links to

---

85 An FTP—or, "File Transfer Protocol"—site is a location on the Internet at which a certain amount of computer memory has been dedicated to storing files. At many such sites, no restrictions are placed on downloading these files. They are free to all comers.

86 This potential has been recognized by at least one group of Internet users: computer hackers. One particularly audacious group used the computers of the Lawrence Livermore facility to store a collection of obscene images. See The Case of the Internet Mole: Livermore finds itself the repository of a most unwanted photo collection, LA Times A10, A10 (July 13, 1994).

87 The problem of ensuring that underprivileged groups will have access to the Internet is discussed in Alison Gardy, Forging Links Between Inner Cities and the Internet, NY Times Section 3 at 10 (Mar 12, 1995) (noting that less than 40 percent of black students have access to computers, compared to 60 percent of white students). For analyses of access as a First Amendment question, compare Cass R. Sunstein, The First Amendment in Cyberspace, 104 Yale L J 1757, 1762, 1774, 1792-94 (1995) (arguing that the First Amendment would not prohibit government regulation designed to ensure access), with Fred H. Cate, The First Amendment and the National Information Infrastructure, 30 Wake Forest L Rev 1, 18-19, 36-50 (1995) (arguing that government regulation to ensure access would violate the First Amendment).
underprivileged high school children, the law should not discourage her from doing so.

5. The open-system model assessed.

When confronted with Internet-wide problems that are best dealt with at the Internet-wide level, the law should adopt rules that govern without creating or recognizing any boundaries in Cyberspace. Protecting the programming and hardware that run the Internet offers the clearest example of an Internet-wide problem that is best addressed by legal rules that rely on behavior instead of boundaries. Legal rules that are tied to system-level boundaries will be eluded by the computer viruses and Internet worms that know no limitations from these firewalls and system boundaries.

The open-system model also allows the law to encourage certain behavior on a network-wide level. First, by not recognizing boundaries, the law could facilitate the free flow of information. As far as commerce is concerned, boundaries are synonymous with obstacles and should be disfavored at law. Second, by recognizing the Internet as an open system, the law would encourage individuals to think about and develop the Internet as a single system. Whenever problems are best addressed at the Internet level—computer viruses represent one example; improving transmission efficiencies another—the law would do well to encourage individuals to develop solutions that can be implemented once at the Internet level rather than countless times at the system level. Finally, boundaries serve only to hinder the sharing of resources on the Internet; a user on one system who wishes to use another, underused computer system will be able to do so more easily if faced with fewer access boundaries.

C. Individual Interests and the Individual-Level Boundary Model

We have now considered how the law, by relying on the system-level model, can promote interests common to all users of particular systems, and how, by relying on the open-system model, it can promote the interests of the whole Internet. We now turn to consider the interests of the individual user, and when, by affording legal protection to each user's choices, the law can create solutions that are both efficient and respectful of each user's autonomy.
1. Minimizing transaction costs in commercial contexts.

Under the current legal regime, owners of information must take affirmative steps if they want to make their information accessible to others on the Internet. Given that would-be users will not be able to gain legal access, the existence of largely impermeable system-level boundaries ensures that information will remain effectively nonexistent as long as users keep that information in their individual accounts.

One might dispute the existence of a problem here. If the owner of a file wishes that file to be available to others, she can, after all, place it into the stream of commerce. The fact that she has not done so, then, should indicate that she has made a judgment that the file is not commercially valuable or is valuable only if kept out of the stream of commerce.

The premises of this objection, however, are flawed. First, one ought not to assume that a file owner's inaction indicates such reasoned calculation. The failure to act may reflect no more than indifference or a misconception about the value of the file.

Second, the objection relies on a formalistic notion of commerce that may be inappropriate in the context of Cyberspace. The division between commercial and private domains, which can be drawn with a comparatively high degree of clarity in the real world, blurs in Cyberspace. There are, at present, no specialized commercial zones or distribution agents on the Internet. Moreover, in the physical world, there is a genuine need for these distributional systems—railroads, barges, and trucks for transporting goods; wholesale and resale outlets from which the goods will be sold; advertising agencies and salesmen to provide consumers with product information—which might be both superfluous and inefficient on the Internet. Given both the high level of interconnectivity on the Net and the ease of conducting transactions without intermediate actors, there is no reason to think that there is a need for a uniquely commercial area on the Net.

Third, the high degree of interconnectivity on the Internet calls into question the feasibility of traditional notification tools—the virtual equivalents, as they are developed, of blanket advertising on television or through printed media. It is difficult to tailor a notice to reach only a certain segment of the Internet since the population of Cyberspace is not yet commercially differentiated. Attempts to reach a particular group will, as a result, often reach a substantially larger audience. If the law creates incentives for information providers to send messages advertising their availability, the result will be a mindless cacophony of ad-
vertising that reaches everyone but informs no one. Therefore, an open-system model of Internet commerce would, in all likelihood, prove unworkable.

Finally, were the law to adopt a system-level model when regulating commercial matters, it would shift to the system administrator the task of determining what search costs would have to be expended prior to the formation of contracts of sale. The administrator would determine the extent to which outsiders could learn about users on her system, and, thereby, the extent to which outsiders could acquire knowledge about potential partners in commerce. Thus, a third party would control the extent to which communication between information seekers and information producers on a given system will ever occur. However, the system administrator is particularly ill suited for making these determinations. Generally, system administrators are chosen for their computer expertise. They are familiar with computer systems and security, not with the nature of the business that users of their systems conduct. From an informational standpoint, system administrators are the parties least able to determine whether a transaction should, or is likely to, take place between an information producer and the information seeker. They are also in a poor position to set the efficient level of search costs for transactions on the Internet. Nevertheless, under the system-

---

88 There are several reasons for believing that this model of providing notice would be inefficient. First, there is currently no way to reach a large passive audience without over-running not only the ability of the network to transmit data but also the ability of individuals to sort through and process the large volume of information they would receive. One company has tried such a saturation approach. The Phoenix law firm of Cantor & Siegel posted a short message to every Usenet newsgroup advertising the services the firm provided. The Internet community was not sympathetic to this saturation of the information marketplace. The firm received such a large amount of "hate" e-mail that the computer company that provided its Internet link experienced fifteen computer crashes. See Peter H. Lewis, An Ad (Gasp!) in Cyberspace: Lawyer's Message vs. Netiquette, NY Times D1, D1 (Apr 19, 1994).

Second, even if an information producer takes an active role in providing notice that she now possesses information that may be commercially valuable, it will still be necessary for the consumer to take active steps in order to receive notice of desired information products. See Internet Advertising: Ethics and Etiquette, Online Libraries and Microcomputers (Information Intelligence, Inc., Phoenix, Ariz) (June 1994) ("This type of service [one that provides a location on the Internet that is dedicated to commercial information] is typically considered good etiquette because it is not barraging thousands of unsuspecting users with electronic 'junk mail' but is providing a place where interested persons can come to electronically 'window shop'."). Requiring producers to put their information into circulation, in short, does nothing to facilitate the task of finding that information; it only creates an additional step in the preliminaries to commercial transactions.
level boundary model, these administrators have the power to set the rules that will determine the likelihood of such transactions.

It is too early in the course of the Internet's development to make judgments about the superiority of one method of commerce over another or predictions about which mode will prevail. However, it is also too early to foreclose, through the rigid application of legal rules, the possibility that a nontraditional system of exchange will, in fact, prove the most efficient. In the case of Internet commerce, a system of regulation that respects boundaries defined by individual users appears preferable to either the open-system or the now dominant system-level boundary models. Individuals are, first and foremost, best positioned to determine the value of information in their possession. This being the case, the law should adopt rules that will respect individual choices regarding how the information they own is to be disposed of commercially.

2. Protecting freedom of expression.

This Section first evaluates the effect of traditional notions of private property and boundary definition on freedom of speech in Cyberspace and then proceeds to argue that the individual-level boundary model is best suited to protecting this interest. While at first glance this connection may seem somewhat attenuated, closer examination reveals that the degree to which legal significance is afforded system-level boundaries will likely determine who bears the responsibility for what is said on the Internet.

Boundaries create units for monitoring the activities of others. As Professor Ellickson has observed, this is particularly efficient when the monitor is charged only with excluding those not authorized to enter. However, when the state recognizes and protects property rights, the law also tends to place responsibility for the actions of others upon the monitor. The right to exclusive use, it seems, brings with it a duty to ensure that property is used in a way that is acceptable to the state.

There is a growing body of literature on other aspects of the First Amendment in Cyberspace. See generally, Sunstein, 104 Yale L J 1757 (cited in note 87); Philip H. Miller, Note, New Technology, Old Problem: Determining the First Amendment Status of Electronic Information Services, 61 Fordham L Rev 1147 (1993); Cate, 30 Wake Forest L Rev 1 (cited in note 87).

Ellickson, 102 Yale L J at 1327-28 (cited in note 36).

See Red Lion Broadcasting Co. v FCC, 395 US 367, 388-92 (1969) (Holder of broadcast license may be forced to give "equal time" to opposing viewpoints.).
In Cubby, Inc. v CompuServe Inc., a federal district court considered whether a national computer bulletin board service should be held liable for failing to perform this type of monitoring role. CompuServe provides subscribers with access to thousands of online information services, including 150 special interest forums, interactive online conferences, and topical databases. Someone posted an article onto one of these services that allegedly defamed a competing bulletin board service operated by Cubby. Although management of the service to which the article was posted was the responsibility of another firm, Cubby brought an action for libel against CompuServe. CompuServe moved for summary judgment on the grounds that, first, it had acted as a distributor, not a publisher, of the statements; and, second, as a distributor, it could not be held liable for the statements because it did not know and had no reason to know of their content.

In granting CompuServe's motion for summary judgment, the court first determined that CompuServe was a distributor of information, similar to a library or bookseller, rather than a publisher of information. Extrapolating from the Supreme Court's decision in Smith v California, the Cubby court refused to impose liability on an information distributor unless that distributor knew or had reason to know of the material's defamatory nature.

Although it grounded its decision in First Amendment jurisprudence, the Cubby court was well aware of the novel technological context to which it was applying the First Amendment:

---

93 Cubby, 776 F Supp at 137.
94 Id at 138. The allegedly defamatory remarks included a suggestion that individuals at the Cubby service gained access to information first published by CompuServe through "some back door," a statement that a Cubby official was "bounced" from his previous employer, and a description of the Cubby service as a "new start-up scam." Id.
95 Id at 137. CompuServe is primarily an access provider and does not create or maintain most of the services to which it provides access. Id at 138.
96 Id at 138.
97 Id at 140 (CompuServe's product is "in essence an electronic, for-profit library that carries a vast number of publications and collects usage and membership fees from its subscribers in return for access to the publications.").
98 361 US 147, 152-53 (1959) (Ordinance imposing strict liability on booksellers for selling obscene materials violated constitutional guarantees of free speech and free press.).
99 776 F Supp at 139-41.
Technology is rapidly transforming the information industry. A computerized database is the functional equivalent of a more traditional news vendor, and the inconsistent application of a lower standard of liability to an electronic news distributor such as CompuServe than that which is applied to a public library, book store, or newsstand would impose an undue burden on the free flow of information.\textsuperscript{100}

After acknowledging the difficulties inherent in monitoring all of the publications carried by the service, the court held that the First Amendment protected CompuServe even in the absence of any effort to perform such monitoring:

[I]t would be no more feasible for CompuServe to examine every publication it carries for potentially defamatory statements than it would be for any other distributor to do so. "First Amendment guarantees have long been recognized as protecting distributors of publications . . . . Obviously, the national distributor of hundreds of periodicals has no duty to monitor each issue of every periodical it distributes. Such a rule would be an impermissible burden on the First Amendment."\textsuperscript{101}

The Cubby decision raises the possibility that, even if the law recognizes system-level boundaries, the First Amendment might forbid assigning monitoring functions to the owners of computer systems. Any legislative or legal attempt to require systems linked to the Internet to monitor the information flowing into or out of their systems would raise the First Amendment issues addressed in Smith and Cubby. The courts may still respect system-owners' rights—for example, the right to exclude certain individuals from the system or to prohibit certain behavior on the system—but they should not automatically assign liability to system owners for actions taken on the system. For example, under the conception proposed in this Comment, a system owner could still prohibit storing obscene images on her system and could exclude those individuals who had done so from the system; nevertheless, system owners who chose not to regulate their systems or whose attempts at regulation failed would not be held liable. The net benefit to society of having additional

\textsuperscript{100} Id at 140-41.

\textsuperscript{101} Id at 140, quoting Lerman \textit{v} Flynt Distributing Co., 745 F2d 123, 139 (2d Cir 1984) (alteration in original).
systems contributing to free and unfettered debate on the Internet outweighs, I believe, the risks of not legally requiring private monitoring of the activities taking place on those systems.

The Cubby court's decision not to assign a monitoring function to system administrators also seems correct as a matter of boundary definition. As in the commercial context, the information producer is the person best suited to judge the import of its content and should accordingly bear the responsibility for its dissemination. In the context of regulating the content of speech, therefore, the boundary line should be drawn at the level of the individual, not the system.

The reach of the Cubby decision, however, remains unclear. The First Amendment has not prevented other district courts from applying strict liability to bulletin board operators where copyrighted material was found on their bulletin boards. In 1994, a California couple was convicted of distributing obscene materials for operating an adult-oriented bulletin board service out of their home. Most recently, Congress amended the Communications Act of 1934 to regulate the transmission of pornographic images and messages on the Internet. The Act as amended imposes criminal liability on any system operator who "knowingly permits" his system to be used for the transmission or posting of prohibited materials. In so doing, it assigns lia-

102 See, for example, Playboy Enterprises, Inc. v Frena, 839 F Supp 1552, 1554-59 (M D Fla 1993).

103 See United States v Thomas, 74 F3d 701 (6th Cir 1996) (affirming conviction). A Tennessee postal inspector became a member of the service and proceeded to download sexually explicit images, order a sexually explicit videotape (which was delivered to him via UPS), and send the couple operating the service an unsolicited child-porn video. The couple was tried before a jury that applied the community standards of Memphis, Tennessee, and convicted on ten counts of obscenity related to the downloaded photographs. Godwin, Virtual Community Standards (cited in note 2).

104 The Telecommunications Act of 1996, Pub L No 104-104, 110 Stat 56, to be codified in relevant part at 47 USC § 223(a). For a full draft of the Act, see Conference Report on S 652, Telecommunications Act of 1996, 142 Cong Rec H1078, H1099 (Jan 31, 1996). The new law criminalizes knowingly initiating the transmission of any "comment, request, suggestion, proposal, image, or other communication which is obscene, lewd, lascivious, filthy, or indecent, with intent to annoy, abuse, threaten, or harass another person."

105 The Act amends 47 USC § 223(a)(2) to provide that anyone who:

knowingly permits any telecommunications facility under his control to be used for [a prohibited activity] with the intent that it be used for such an activity [ ] shall be fined . . . or imprisoned not more than two years, or both.

110 Stat at 133.
bility in a way that will likely discourage the openness that currently characterizes the Net, and may ultimately have a severe chilling effect on both commerce and free speech in Cyberspace. If the system administrator is civilly or criminally liable for anything that the users of her system do or say, then she is likely to create restrictions designed to insulate herself from such liability. These restrictions will produce results inimical to First Amendment values.\textsuperscript{106} The Supreme Court has recognized the dangers of such a chilling effect in other First Amendment contexts.\textsuperscript{107} Whether courts will acknowledge the chilling effect in Cyberspace remains to be seen.\textsuperscript{108}

The chilling effect of overly restrictive liability rules poses as large a threat to First Amendment values in Cyberspace as it does in other contexts. Courts should avoid this threat by defining the relevant boundaries in the context of content regulation—as the Cubby court did in the context of libel law—at the level of the individual responsible for disseminating the materials in question.

3. Protecting incentives to produce.

The analysis of the "tragedy of the commons" in the discussion of the open-system model\textsuperscript{109} assumed a world of preexisting resources. This Section starts from a different baseline; it considers the effect of Internet boundary rules on the behavior of the those who produce information resources.


\textsuperscript{107} See, for example, Smith, 361 US at 152-53 (striking down a California ordinance imposing strict liability on a bookseller who possessed any book determined to be obscene).

\textsuperscript{108} Consider, for example, the possible chilling effects of the adult-oriented bulletin board cases discussed in note 103 and accompanying text. For discussions of the liability of bulletin board operators for messages they transmit, see generally Gilbert, Note, 54 Fordham L Rev 439 (cited in note 106); Loftus E. Becker, Jr., \textit{The Liability of Computer Bulletin Board Operators for Defamation Posted by Others}, 22 Conn L Rev 203 (1989); David Loundy, \textit{E-Law: Legal Issues Affecting Computer Information Systems and System Operator Liability}, 12 Computer/L J 101 (1993). The particular case of bulletin board operator liability is distinguishable from the case of system administrator liability in the present context. Bulletin boards are generally limited in size. Monitoring costs may still be high, see Gilbert, Note, 54 Fordham L Rev at 447-48, but the cost of monitoring the limited number of messages on a bulletin board would be much less than that of monitoring all activity occurring on an entire system.

\textsuperscript{109} See Section II.B.2.
The argument regarding incentives to produce is fairly simple. An author, or any other producer of an information resource, will not be inclined to produce information if she cannot control or profit from its dissemination.\footnote{Posner, Economic Analysis of Law at 38 (cited in note 37).}

One could argue that system-level boundaries would preserve incentives to produce by protecting property placed on the Net. Access to a system can be controlled, and only those interested in acquiring information stored on a system would be allowed to enter. Such control would protect a producer’s interests in the property she has created and, thereby, preserve incentives to produce information.

The individual-level boundary model, however, is better suited to protecting an individual’s property interests in her information and, thereby, her ex ante incentives to produce that resource. This is true at two levels: the psychological and the legal. At the psychological level, the owner of a piece of information will feel more secure in her possession of that information if she is able to consciously determine the level of legal protection that it will receive. She will feel more secure, in other words, if she knows that when she performs certain actions—for example, marking a file as unreadable or encrypting a file—she is calling upon the law to protect her. At the legal level, the law could make these significant actions triggers of legal protection. For example, the law could criminalize all attempts to override the encryption used by individuals to protect their files or to read files that have otherwise been designated unreadable.

All of the arguments for system-level and individual-level boundaries, however, assume that it is the theft, or the unauthorized downloading of a file, that destroys that file’s value. In Cyberspace, however, a single theft, in itself, neither removes the information from the possession of its owner nor radically diminishes its value. A theft, with no more, results only in the loss to the producer of one potential customer, and therefore in the vast majority of cases the resulting loss in value would be negligible.\footnote{I do not address cases in which the value of information depends on absolute confidentiality. Although commercial, such information is not intended for commerce. This type of information—for example, corporate secrets—would best be considered under the privacy analysis outlined in Section II.A.I.}

The real loss in value in Cyberspace results from the widespread dissemination of a resource.\footnote{Barlow, Selling Wine Without Bottles (cited in note 74):
larly severe in the highly interconnected medium of the Internet, where a piece of information can be sent effortlessly around the globe within seconds and disseminated to hundreds of locations within minutes.\textsuperscript{113} Moreover, because a purchaser of information can disseminate that information as easily as a thief, preventing theft will have only a marginal impact on preventing dissemination.

The solution to this problem remains elusive. What should be clear, however, is that the system-level model does little, if anything, to protect an owner’s interest in exclusive control over the information she possesses. While enforceable system-level boundaries may protect owners of information resources from persons outside the system, they do nothing to protect against predators already inside the system. This defenselessness against “internal” predators increases in significance when one considers that it is persons relatively close to a creator who are more likely to know about and profit from stored intellectual property.\textsuperscript{114} Protection for such interests is better found either at the individual level, perhaps by the use of encryption tools to conceal and copyprotect valuable commercial information,\textsuperscript{115} or at the level of the Internet as a whole, perhaps by implementing protocols for tracing the source and destination of particular files. Legal rules designed to protect incentives to produce by drawing boundaries at the system level will most likely slow the development of technologies that aim at affording non-boundary-based methods of protection in Cyberspace.

4. The individual-level model assessed.

When individual choice, initiative, or innovation are desirable, particularly in the commercial context, the law should adopt an individual-level model of Internet regulation. Regulations

---

\textsuperscript{113} See text accompanying notes 17-18.

\textsuperscript{114} See text accompanying notes 34-35.

\textsuperscript{115} Barlow, \textit{Selling Wine Without Bottles} (cited in note 74). Barlow suggests encrypting files to prevent their theft or duplication. This is one possible option, but, in my opinion, any network-based solution to these sorts of problems would be better than either individual or system-level monitoring. The efficiency of having one monitor rather than hundreds or millions of monitors is obvious. The downside to this approach, however, is the risk associated with putting all of our security eggs into one basket.
embodied the individual-level model—by, for example, placing the burden on the individual of deciding whether a file will be readable or unreadable—will encourage individuals to make informed judgments about whether a piece of information is economically valuable. Given their informational advantages, individuals are generally best suited to determine whether their own possessions are valuable and take the necessary steps to preserve and exploit that value.

In the context of encouraging free expression, the law should do no more than look to the speaker herself. Entrusting others to monitor speech on the Internet—which would result from adopting the system-level model in the context of speech regulation—would produce a chilling effect on the Internet. Adopting the individual-level model in this context will produce a minimum of regulation antithetical to the values of the First Amendment, without producing the undesirable cacophony that would result were the law to adopt an open-system conception in the context of speech regulation.

Finally, respecting individual autonomy will encourage production of information on the Internet. If, in short, an individual is given the power to control whether and how the law will protect her possessions in Cyberspace, she will feel more confident about introducing those resources onto the Information Superhighway.

**Conclusion**

Given the unconventional nature of the Internet, the boundaries that define property rights will sometimes best be drawn along nontraditional lines. Some situations will call for the recognition of boundaries at the system level. When the interests of system users are united, and the need to exclude is paramount, this is certainly the case. However, when legislatures and courts are called upon to craft boundary rules in other contexts, respect for traditional boundaries may be inappropriate. In such circumstances, lawmakers must consider relevant interests, communities, and distributional aims when determining what boundaries to protect.

If people are to function in the Internet’s virtual environment, predictable lines must be drawn. To accomplish this goal, the law will have to enter and understand the virtual environment in which those it hopes to regulate have chosen to conduct their business. The law, in short, must be made applicable if it is to be applied.