ARTICLES

SHRINKWRAPS IN CYBERSPACE

Mark A. Lemley*

"Information wants to be free . . ."
- Hacker Credo[1]

> The odds are always good that big power and big money will find a way to control access to virtual communities; big power and big money always found ways to control new communications media when they emerged in the past. The Net is still out of control in fundamental ways, but it might not stay that way for long. What we know and do now is important because it is still possible for people around the world to make sure this new sphere of vital human discourse remains open to the citizens of the planet before the political and economic big boys seize it, censor it, meter it, and sell it back to us.
>
> - Howard Rheingold[2]

In an influential recent article in the pages of this journal,[3] Robert Dunne offers a new solution to the problem of unauthorized computer access by computer "hackers" (and, by extension, to other problems as

---

* Assistant Professor, University of Texas School of Law. I would like to thank Rose Hagan for her advice, and the members of the cni-copyright and Cyberia-l Internet listservs for their thought-provoking discussions of these issues.

1. Dorothy Denning, *Concerning Hackers Who Break Into Computer Systems* (paper presented at the 13th National Computer Security Conference, Washington, D.C., Oct. 1-4, 1990).

2. HOWARD RHEINGOLD, THE VIRTUAL COMMUNITY: HOMESTEADING ON THE ELECTRONIC FRONTIER 5 (1993).

3. Robert L. Dunne, *Deterring Unauthorized Access to Computers: Controlling Behavior in Cyberspace Through a Contract Law Paradigm*, 35 JURIMETRICS J. 1 (1994).

well). He advocates widespread agreements among the providers of Internet access on form contracts that prohibit attempts to log on remotely to a computer system without authorized access. In recent months, some version of this "contract law paradigm" has been implemented by an increasing number of access and information providers. These providers are attempting to use contract law to protect their data and control the behavior of Internet users.[4]

In this essay, I offer a number of objections to Mr. Dunne's contract law paradigm. I suggest that the current move towards form contracts and "shrinkwrap licenses"[5] online is likely to have pernicious effects on both the culture of the Net and the optimal distribution of information. I conclude with ideas for alternative governance structures which may avoid these problems.

I. THE CONTRACT PARADIGM

The Internet (and its relatives, the National Information Infrastructure and the "information superhighway") have entered popular consciousness with a vengeance in the last two years.[6] Several facts about the evolution of the Internet help to explain the emergence of the contract paradigm.

The Internet began in the late 1960s as a Defense Department project designed for government agencies to communicate with each other and with university research facilities via computer. Because it was built at the height of the Cold War, the Internet was intentionally decentralized. While there are high-transmission-rate trunk lines that form part of the Internet; the primary means of Internet data transmission is information routed through other participating networks.[7] The government hoped that the Internet would be able to survive a nuclear war which damaged or destroyed some nodes of the network.

---

4. *See infra* notes 24-27 and accompanying text.

5. The term "shrinkwrap licenses" refers in the physical world to form "agreements" imposed unilaterally by vendors in software transactions. These vendors announce their contract terms with a printed document contained inside a box of mass-marketed software. Typically, the document asserts that opening the cellophane shrinkwrap will constitute acceptance of the contract terms. Hence the name "shrinkwrap license." In this article, I use the term "shrinkwrap licenses" in a slightly more general sense, to refer to any form contract which purports to be accepted by user performance rather than express agreement. For a detailed discussion of the nature and terms of shrinkwrap licenses in the physical world, see Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses (An Open Letter to the UCC Drafting Committee)*, 68 S. CAL. L. REV. __ (forthcoming 1995).

6. For a description of the development of the Internet, see RHEINGOLD, *supra* note 2, at 65-109.

7. To perpetuate the unfortunate highway analogy, the Internet is not an information superhighway at all, but rather a system of back roads. There is no main route to most destinations. Each driver may take one of many different paths to the same destination.

In the 1980s, the Internet grew substantially as universities, defense contractors, computer companies, and finally commercial service providers across the world joined the list of members. Gradually, the Internet evolved from a government project into a means of exchange for the academic and scientific communities, and finally into a commercial center. While the Internet has grown and its purposes have changed in the 26 years since its inception, its basic structure has remained the same. Ironically, for a government project, the result of the Internet's decentralized information routing has been the development of a worldwide community with no real government.

However, no government does not mean no governance. As Robert Ellickson has noted, close-knit communities often can accomplish the basic purposes of government through a set of informal norms "enforced" by some type of social sanction.[8] Throughout much of its history, an unwritten but very powerful set of informal norms has governed the Internet. These norms range from the mundane (the use of capital letters in electronic mail is considered the virtual equivalent of shouting; *asterisks* are used to underline or emphasize a word) to the fundamental (unsolicited advertising which intrudes on Net citizens is strictly forbidden). These norms are "enforced" in a variety of ways, including "frequently asked question" lists which inculcate new users into the culture of a particular subset of the Internet community and "flames" (angry responses to breaches of Internet etiquette, or "netiquette").[9]

Informal social norms worked fairly well when the Internet community was small and relatively insular. As a result of the explosive growth of the Net in the last ten years,[10] however, the established social order of the Internet is breaking down. New users, who have not fully inculcated the values of the Net, overwhelm established users in many contexts. While the older users have tried to maintain their social authority by creating informal

---

8. *See* ROBERT ELLICKSON, ORDER WITHOUT LAW (1990).

9. *See generally* Dunne, *supra* note 3, at 11 ("Behavior in cyberspace has traditionally been based on a common understanding among its inhabitants about what is acceptable. The cyberian ethic has been not so much that access to computers should be unlimited and total and that all information should be free, but that this should be so to the extent possible without harming individuals or damaging their property. Until fairly recently, a large majority of cyberians shared a common intellectual framework and sense of purpose, and this understanding was sufficient to regulate matters.").

10. While precise statistics are unavailable, estimates of the number of people on the Internet five years ago ranged from 1-2 million. The estimate today is approximately 20-30 million and growing daily.

hierarchies,[11] it is virtually impossible to maintain social hierarchies in a world where access is essentially equal.

New users also change the character of Internet society by their sheer numbers. It is no accident that Ellickson's examples of private ordering tend to occur in small, close-knit, insular communities. For example, no one would argue that New York City could be governed without laws. The addition of fifteen million new users to the Internet in the last decade may have made private ordering impossible, except in a few specialized corners of cyberspace. Fraud, theft, vandalism, and defamation—often by anonymous strangers—are now a part of life on the Internet.[12]

In addition to the demographic changes, the nature of interactions on the Internet is also changing. Commercial transactions, once prohibited on the government-run network, seem poised to become the dominant form of information exchange.[13] Unlike e-mail discussions, or the posting of free information, commerce requires either a legal enforcement mechanism or a high degree of trust among market participants. At present, the Internet has neither.

As a result, "citizens" of the Internet have started turning to the legal system in their quest for order, turning primarily to state and federal laws in the United States.[14] Copyright infringement and defamation suits are

---

11. For example, certain e-mail addresses, like the Whole Earth 'Lectronic Link (WELL) in California, are coveted; by contrast, users from commercial online services like Prodigy and America OnLine are frequently disparaged by Net regulars.

12. *See, e.g.*, United States v. LaMacchia, No. 94-10092-RGS, 49 PATENT, TRADEMARK, COPYRIGHT J. (BNA) 253 (D. Mass. Dec. 28, 1994) (facilitating copyright infringement through online bulletin board does not violate federal wire fraud statute); Sega, Inc. v. Maphia, 30 U.S.P.Q.2d 1921 (N.D. Cal. 1994) (bulletin board operator liable for copyright and trademark infringement for distributing copies of Sega games); Playboy Enter. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993) (bulletin board operator liable for copyright and trademark infringement for maintaining scanned photos from Playboy magazine); Cubby v. Compuserve, 776 F. Supp. 135 (S.D.N.Y. 1991) (Compuserve not liable for defamatory statements published over its network); United States v. Riggs, 739 F. Supp. 414 (N.D. Ill. 1990) (hackers who acquired document from telephone company computers were guilty of wire fraud and interstate transportation of stolen property); Matthew Goldstein, *Prodigy Case May Solve Troubling Liability Puzzle*, N.Y.L.J., Dec. 19, 1994, at B1 (discussing defamation suit by Stratton Oakmont Corp. against the Prodigy online service); Edward R. Silverman, *A Coin Slot for CompuServe's Virtual Jukebox?*, WIRED, July 1994, at 32 (describing Frank Music's suit against Compuserve for copyright infringement).

13. For example, groups like the Internet Shopping Network conduct a booming sales business electronically. Many Fortune 500 (and a host of smaller) companies have set up Internet sites, where they distribute information about their products, and where in the not too distant future they will be making sales. Even Pizza Hut has begun delivery orders over the Internet.

14. There are two reasons for this. First, the United States remains ahead of most other nations in the world in private ownership of computer and communications technology, which means that most people on the Net are from the United States. Second, the United States has

starting to spring up,[15] and several people have already been convicted of unauthorized computer access under U.S. criminal laws.[16] These suits are the tip of the iceberg as the Internet encounters the legal system.

Many Net denizens are bothered by what they see as the intrusion of the laws of the physical world into their virtual community. The early Internet settlers "put great store in individualism and dislike rules."[17] There is good reason for this concern. As Mr. Dunne suggests, the criminal laws of the physical world are generally ill-suited for cyberspace. Prosecutors and judges generally are not familiar with the culture and norms of the Internet. They may lack the technical expertise necessary to identify and prosecute offenders. Also, the international nature of the Internet creates jurisdictional problems that can be overcome only by the most extreme means.[18]

Dunne suggests that these problems can be solved by relying on contract law rather than criminal and tort law. He argues that contract law preserves the individual responsibility so dear to libertarian-minded Net citizens. Additionally, it permits local enforcement by attorneys for online information providers or access services, who presumably have greater expertise in Internet law than local prosecutors. Finally, because contracts transcend national boundaries, agreements provide a way of avoiding the jurisdictional difficulties inherent in criminal statutes.[19] Dunne expressly contemplates that such online contracts would cover conduct which has traditionally been the province of tort or criminal law.[20]

Dunne's proposal works as follows: First, someone will write a "model code of network conduct" which would specify the undesirable behavior to be prohibited. Internet information and access providers "would be expected to endorse this code and enforce it" by requiring all users to sign an agreement to abide by the model code. Additionally, "[p]articipating sites and providers would limit access to their resources by other sites and

---

shown few qualms about extending the reach of its laws beyond its own physical borders.

15. *See, e.g.*, Sega, Inc. v. Maphia, 30 U.S.P.Q.2d 1921 (N.D. Cal. 1994) (bulletin board operator liable for copyright and trademark infringement for distributing copies of Sega games); Playboy Enter. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993) (bulletin board operator liable for copyright and trademark infringement for maintaining scanned photos from Playboy magazine); Cubby v. Compuserve, 776 F. Supp. 135 (S.D.N.Y. 1991) (Compuserve not liable for defamatory statements published over its network).

16. United States v. Morris, 928 F.2d 504 (2d Cir. 1991); United States v. Lewis, 872 F.2d 1030 (6th Cir. 1989) (unpublished table decision); United States v. Riggs, 739 F. Supp. 414 (N.D. Ill. 1990); *but cf.* United States v. LaMacchia, No. 94-10092-RGS (D. Mass. Dec. 28, 1994). The federal criminal statute is 18 U.S.C. § 1030. In addition, 49 states have "computer crime" laws. For a list of these statutes, see Dunne, *supra* note 3, at 4-5 n.9.

17. Dunne, *supra* note 3, at 10.

18. For example, one country could physically assert its criminal jurisdiction beyond its borders. *See id.* at 9-10.

19. *Id.* at 12.

20. *Id.* at 12-13.

providers to those who had endorsed the code."[21] Dunne acknowledges that his proposal will work only if the model code is adopted and enforced by a certain "critical mass" of Internet sites.[22]

A number of information and access providers have begun to use contracts in this way by setting norms of behavior and prohibiting access to those who do not conform. For example, one law firm's "home page" on the World Wide Web[23] restricts the ability of companies to link to the home page if the linking company charges its users for the privilege.[24] Another law firm includes a "contract" at the bottom of its electronic mail messages prohibiting the copying, distribution, and disclosure of the message in its contents and the "taking of any action in reliance on the contents" of the message.[25] Furthermore, large Internet access providers are including electronic "terms and conditions" for the general use of their services and for access to specific databases.[26] Even the United States Patent and Trademark Office has begun endorsing so-called "electronic licenses" in which "[p]roviders may inform the user that a certain action—the entering of a password, for instance, to gain access to the service or a particular work, or merely the use of the service—will be considered acceptance of the specified terms and conditions of the electronic license."[27]

---

21. *Id.* at 13.

22. *Id.*

23. The World Wide Web is a part of the Internet which works like a giant hypertext stack. Each computer screen points to other sources of similar information, and the use can "jump" to any source identified on any screen by clicking on it. Thus, it is possible to jump to Web cites all over the world while pursuing a single piece of information. Each of these programmed "jumps" is called a "link."

24. *See* Internet address http://www.commlaw.com/pepper.

25. Electronic mail from Jon Jackson of Jackson & Wilson, Inc., firm@ni.net, received Jan. 14, 1995 [on file with author].

26. For example, Dialog Information Services requires assent by performance to an entire booklet entitled "terms and conditions." Compuserve contains restrictive language in its Knowledge Index database, accessed from Compuserve by typing GO KI, and its Dun & Bradstreet financial database, accessed from Compuserve by typing GO DUNS. *See generally* electronic mail from John Rosenberg (john@onliners.com) to Mark Lemley (mlemley @mail.law.utexas.edu), received Jan. 23, 1995, 3:19 pm [on file with author]. Similarly, America Online requires certain warranties and the grant of certain copyright rights as a condition of posting messages on its service. America Online Terms of Service, § 2.6, *quoted in* Carl Drott, electronic mail to cni-copyright listserv, Feb. 21, 1995, 1:51 pm. For an exhaustive collection of restrictive terms in information provider form contracts, see John S. Rosenberg, *(Copy)Right of Way on the Information Highway*, 2 SEARCHER, Mar. 1994, at 36, 38-40.

27. United States Patent and Trademark Office Information Infrastructure Task Force, Intellectual Property and the National Information Infrastructure: A Preliminary Draft of the Report of the Working Group on Intellectual Property Rights 115 (July 7, 1994). The "Green Paper" report, as it is commonly known, has no legal effect whatsoever. It is merely a preliminary recommendation to Congress by the PTO's Task Force on the NII. Congress has

None of these "contracts" are bargained for in the traditional sense. They are "take it or leave it" agreements, and in most cases they contain terms of which users are not aware when they begin the transaction. These contracts are the cyberspace equivalent of shrinkwrap licenses.

II. THE PROBLEM WITH SHRINKWRAP LICENSES

Shrinkwrap licenses in the physical world do not fare well in the courts. Virtually every court that has considered the validity of a shrinkwrap license has held the license unenforceable for one reason or another.[28] There are two basic reasons for this. First, most shrinkwrap licenses are not really "contracts" at all. They are form agreements over which the parties do not bargain, and they are never expressly acknowledged by the parties to the transaction themselves. Purchase of mass-market software in the physical world generally occurs by phone or at a retail store. In either case, the parties agree on the basic terms of the transaction—goods to be delivered, price to be paid, etc. A shrinkwrap license is a unilateral attempt by the software vendor to add terms to a market transaction which is effectively over when the money is paid and the software is received. Contract law is understandably unsympathetic to such an attempt.

Shrinkwrap licenses have other problems as well. The "assent" a user supposedly manifests to the terms of the license by opening the package and using the software is a thinly disguised fiction. The user may not read the license terms. Also, it may be impossible or impractical for the user to comply with the license and reject the software for a number of reasons.[29] Overall, the shrinkwrap license unilaterally and fundamentally changes the nature of the bargain between the parties, making it difficult or impossible for the user to object to whatever terms the vendor chooses to include.[30]

The second problem with shrinkwrap licenses is that they conflict with important legal rules that have been carefully crafted by Congress and the

---

taken no action to introduce or adopt any of the Green Paper proposals.

28. *See* Step-Saver Data Sys. v. Wyse Technology, 939 F.2d 91 (3d Cir. 1991); Vault Corp. v. Quaid Software, 847 F.2d 255 (5th Cir. 1988); Ariz. Retail Sys. v. Software Link, Inc., 831 F. Supp. 759 (D. Ariz. 1993); *see also* Foresight Resources Corp. v. Pfortmiller, 719 F. Supp. 1006 (D. Kan. 1989) (dictum).

29. Most shrinkwrap licenses provide that a user who rejects the proposed terms can return the software to the vendor for a full refund within a certain period of time. Many users do not even open the software within the time allotted, particularly in the case of gifts. Others may not be able to obtain new software in time, or may not be able to wait for a promised refund. Further, several people who have tried to return software to the vendor have been told that the retail outlet has a "no return" policy, notwithstanding the terms of the shrinkwrap license.

30. For a detailed exposition of these problems, see Lemley, *supra* note 5.

or impossible for the user to object to whatever terms the vendor chooses to include.[30]

The second problem with shrinkwrap licenses is that they conflict with important legal rules that have been carefully crafted by Congress and the courts. For example, federal intellectual property policy reflects a delicate balance between the interests of the authors, inventors, purchasers, future authors or inventors and the general public. Each of these groups has rights and interests that are affected by the scope of the intellectual property laws. Intellectual property law reflects a compromise between these competing interests. Because only some of these interests are represented in a licensing transaction, contracts that "opt out" of some but not all intellectual property rules are likely to upset that balance. This is particularly true in the case of shrinkwrap licenses, in which the interests of only one party are represented.[31]

To be sure, some of the problems with shrinkwrap licenses in the physical world can be addressed easily online. For example, the relationship most Internet users have with their access provider is a continuing one, rather than a one-time sale of goods. Consequently, the formal problem that the shrinkwrap terms are not offered until after the transaction has taken place arguably does not arise in cyberspace.[32] For this reason, at least one author has argued that the user manifests acceptance of the terms of a shrinkwrap license online by paying monthly access bills.[33] However, courts have been skeptical toward such "course of dealing" arguments in the past.[34]

---

30. For a detailed exposition of these problems, see Lemley, *supra* note 5.

31. *See id.*

32. Further, it is much easier to require some form of *express* agreement by users online than it is in the physical world. For example, the user logging in to a World Wide Web site for the first time may be confronted with a "contract" screen and the options "accept" and "reject." The user must select one option in order to proceed, and if she selects "reject," she is denied access to the site. *See* Jimmy Eaton, electronic mail to cni-copyright listserv, Jan. 24, 1995, 1:28 p.m.; Christopher Pesce, electronic mail to cni-copyright listserv, Jan. 23, 1995, 10:22 p.m. (both suggesting methods of designing such systems).

33. Joel Rothstein Wolfson, *Information Transactions on the Information Superhighway: It's Not Just Software Law Anymore*, 6 J. PROPRIETARY RIGHTS, Nov. 1994, at 2, 2-3. However, Mr. Wolfson recommends that Internet access providers obtain signed contracts from their users and premises much of his analysis on the assumption that they will do so.

34. For example, in Ariz. Retail Systems v. The Software Link, 831 F.Supp. 759 (D. Ariz. 1993), the district court enforced the shrinkwrap terms sent along with an "evaluative" copy of software. The court's decision was based on ARS's admission that it did not decide to keep the copy until having read and opened the shrinkwrap license and used the software for several hours. Thus, unlike the Third Circuit's decision in *Step-Saver*, ARS was aware of the terms of the shrinkwrap license at the time the agreement was formed. However, the court refused to enforce the same license when it accompanied subsequent software purchased

unlikely to object to shrinkwrap licenses still exist online. A user has arguably invested more in joining an online service for a month before "manifesting assent" to the provider's terms than the purchaser of computer programs who takes the program home. If the latter user is unable or unlikely to return the program, the same will certainly be true of the user of an online service. After all, the online user has invested time and money in learning the system and may have developed ties to a community which he does not want to break.

Further, the arguments from federal intellectual property policy have at least as much force online as they do in the physical world. Federal intellectual property policy reflects a balancing of the competing interests of several different parties, something that cannot be accomplished by private contracts between a few of those parties. This problem with shrinkwrap licenses is even worse online, because the shrinkwrap licenses Dunne contemplates would supplant criminal law as well as intellectual property law. Most policymakers would find such a suggestion astonishing in the physical world. For example, society would be unlikely to permit its citizens to "contract away" their right to be free from rape or murder.

Shrinkwrap licenses, then, would seem to be a poor model on which to base an online society. Experience in the computer industry has demonstrated that they unfairly disadvantage users and the general public by allowing one party, the vendor who drafts the license, to set unalterable policy rules. This is particularly problematic because, for a variety of institutional reasons, different software vendors tend to use similar terms in their licenses, destroying even the illusion of user choice.

III. A DANGEROUS PARADIGM

One of the greatest dangers of shrinkwrap licenses stems from their potential uniformity. In the physical world, as a practical matter it is not possible to get certain kinds of software without encountering a shrinkwrap license. Users do not face a real choice about which terms they will be deemed to have agreed to because all the shrinkwrap licenses in the computer industry look pretty similar. The result is "private legislation"—a new uniform rule of law which alters the legislated rules of tort, contract, and intellectual property law, but which was "passed"without any of the classic political forms of deliberation or debate.[36]

---

50 BUS. LAWYER 151, 166-69 (1994); Rosenberg, *supra* note 26, at 36.

36. Robert P. Merges, *Intangible Rights and Commercial Contracts: A Review Essay on Transactions and Complex Property Rights*, MICH. L. REV. (forthcoming 1995). Professor Merges bases his argument in part on an earlier work by Friedrich Kessler, who coined the term "private legislation" to describe contracts of adhesion which were standardized throughout an industry. Friedrich Kessler, *Contracts of Adhesion—Some Thoughts About Freedom of Contract*, 43 COLUM. L. REV. 629 (1943).

Arguably, the same phenomenon is beginning to happen online. The current "pressure points" in the growth of the Internet are commercial online services and access providers. Virtually all of them have form contracts online which purport to restrict their duties and their users' rights.[37] If access requires using a commercial service, and if all commercial services use the same shrinkwrap license, the result is a world that gives "freedom of contract" to Net suppliers (who wrote the contracts), but none to Net users.

This argument against uniform shrinkwrap licenses runs into a vociferous objection of "it can't happen here." In the words of Internet pioneer John Gilmore, "[t]he Net interprets censorship as damage and routes around it."[38] In the context of shrinkwrap licenses, the decentralized nature of the Internet arguably provides considerable solace. If in the near future there are hundreds of Internet access providers and thousands or millions of information providers,[39] competition should force the most egregious restrictions out of shrinkwrap licenses. Furthermore, if there are numerous routes to any particular piece of information, no one shrinkwrap license will be able to "lock up" that information.

If the Internet is left alone, the decentralization argument has some force. Perhaps it is reasonable to expect that different access and information providers will develop in different directions. But Dunne's suggestion is precisely that shrinkwrap licenses on the Net should *not* be left to develop alone, but ought to be *made uniform*. He proposes:

> * A model code of network conduct would specify offenses, such as unauthorized access . . .
> * Internet host sites and other providers of Internet access would be expected to endorse this code and enforce it.
> * Participating sites and providers would limit access to their resources by other sites and providers to those who had endorsed the code . . .
> * All Internet users at participating sites or obtaining access through participating providers would be required to sign an agreement accepting the terms of the code of conduct.[40]

---

37. *See* I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. PITT. L. REV. 993, 1029-30 (1994).

38. *See* RHEINGOLD, *supra* note 2, at 7.

39. There is considerable debate on this point. In a recent exchange on the cyberia-l listserv, for example, Professor Trotter Hardy extrapolates from the current rate of creation of home pages on the World Wide Web and states that "I'm not worried that the Internet will only be home to a small number of suppliers; the contrary seems more likely (home to a HUGE number of suppliers)." Trotter Hardy, electronic mail to cyberia-l listserv, Jan. 29, 1995, 3:23 p.m. By contrast, Tom Rowland argues that the entry of large phone companies into the Internet access market will result in a relatively concentrated market for Internet providers. Tom Rowland, electronic mail to cyberia-l listserv, Jan. 28, 1995, 7:08 a.m.

40. Dunne, *supra* note 3, at 13.

Indeed, Dunne expressly relies on the widespread adoption of a single "model code" by a "critical mass" of the Internet community.[41]

If a uniform code is adopted by any significant number of online providers, it will have one of two possible negative effects. First, adoption by a significant, but not overwhelming number of Internet providers would divide and therefore destroy the Internet. A model code strikes at a core assumption that allows the Internet to operate in its current, decentralized fashion—the assumption of reciprocal access. Information on the Internet travels a decentralized path, crossing into the virtual territory of third party computer networks on the way to its destination. Dunne suggests that we fence this boundary. Each Internet provider would guard its domain, allowing entry only to those who were subject to the proper contracts. The virtual world would be divided into a gated community (the "inside") and an unregulated wilderness (the "outside"), to the detriment of both.[42]

Second, if a model code is adopted by virtually all Internet providers, the result would be even more troubling. The model code would be the law of the Internet for all intents and purposes. By definition, there could be no variation in the rule, and no room for bargaining. The proposed punishment for failing to acknowledge the primacy of the model code is expulsion from cyberspace.

But this new law of the Internet would be unlike any form of legislation known to modern society. No one elected its drafters or the Internet providers who adopted it. They are accountable to no one. There is no provision for varying the model code in individual cases, or for amending the code itself at popular request. Nor is there any provision for "opting out" of this new social contract, other than by withdrawing from cyberspace. Of course, the resulting Internet oligarchy could be benevolent and the model so well drafted that it would be satisfactory to everyone involved, but this seems unlikely. Humans have had little success drafting such universal codes in the past. It would be a sheer accident if the model code drafted (presumably) by the Internet providers themselves, or at least with their active

---

41. *Id. See also* Hardy, *supra* note 37, at 1029, 1030 (discussing the possibility of requiring users to sign contracts at their "entry point" into cyberspace).

42. Steve Zorn elaborates this point:

> [I]sn't there a danger that [corporate] centers of power would become dominant within the Net, as they have within the economy as a whole? William Gibson's, or Marge Piercy's, novelistic visions of the future certainly seem inherently plausible, if not inevitable.
>
> So one question is, if we have a Net where private spaces can be created (as we do now, where there are restricted mailing lists, and fee-charging services whose resources are not generally available to all), then how do we preserve some sort of general, public area?

Steve Zorn, electronic mail to cyberia-l listserv, Jan. 25, 1995, 8:01 p.m.

cooperation, happened to be the optimal means of regulating behavior in cyberspace.

IV. ALTERNATIVES

In the final analysis, my disagreements with the "contract paradigm" can be traced to differing visions of the future of the Internet. Dunne calls his model "Contract as Control."[43] That description is both the virtue and the flaw in his proposal. To cede control of the Internet to those who write form contracts is to establish a centralized private government. Centralization will help to prevent legal abuses on the Internet, but a centralized government may not be desirable in cyberspace. As Trotter Hardy has argued:

> The decision as to which of these several mechanisms is most appropriate for the different problems of the law relating to cyberspace is best made by applying a presumption of decentralization: the most flexible, least intrusive rule-making process is best because communications technology is changing so rapidly.[44]

I agree with Professor Hardy that decentralized rulemaking is a goal worth striving for.[45] But the lesson of shrinkwrap licenses in the physical world is that "contracts" are not necessarily decentralized. Moreover, centralized contracts (uniform shrinkwrap licenses) may actually be worse than other forms of government regulation. Those who control the contracts are not subject to any of the normal checks on power that constrain government action.

Is there any realistic alternative to the use of shrinkwrap licenses in cyberspace? Perhaps a better way to approach this question is to ask what would happen if electronic shrinkwrap licenses were unenforceable in most circumstances (just as their physical counterparts are today). Would Internet commerce be stymied? I suspect the answer is no. People will find other ways to conduct their business. In particular, there are at least three partial alternatives to the use of shrinkwrap licenses online. No alternative alone is totally satisfactory, but together they may establish an effective and largely decentralized system of Net governance.

The first alternative is self-help. The best way to protect information of commercial value online is to be selective when disclosing it. The development of universal encryption will make it difficult (though not impossible) for others to intrude on private conversations, helping to maintain secrecy. Technical means can make unauthorized copying more

---

43. Dunne, *supra* note 3, at 11.

44. Hardy, *supra* note 37, at 1054.

45. Professor Hardy is an advocate of contract law as a means of governing the Internet. I suspect that our disagreement on this issue stems from our different views about the flexibility and intrusiveness of form contracts.

difficult. None of these technical means are perfect, and they work better for some purposes than others.[46] Self-help has the advantage that it requires no government intrusion whatsoever.

Second, commerce can and will be conducted online through the use of signed, bargained contracts. One of the greatest (and most overlooked) advantages of the Internet is the dramatic decline it has produced in the transaction costs of bargaining. It is remarkably easy to communicate with information providers online. There is no reason why "writing" a bargained contract cannot be as simple as exchanging electronic mail. The law should take advantage of this simplicity by requiring parties to enter into actual, not form, agreements on issues of importance to them.

Finally, there will always be problems on the Net that are not transactional, but involve third parties who cannot be identified in advance. In such cases (access crimes, some torts, and some copyright infringement), we may have to rely on legal intervention to regulate private conduct. While the law has not kept up well with the pace of technological and social change online, the solution is to change the law, not abandon it. Ultimately, the Internet may warrant its own government, which presumably will be better equipped than national governments to regulate in this new environment. Whatever government regulates the Net in those few cases in which government intervention will be required, at least the citizens of the Net will have some say in how it conducts its affairs.

---

46. For example, self-help is perfectly adequate as a means of maintaining trade secrets and the privacy of discussions between contracting parties, but it fails in circumstances in which information must be made publicly available.