

1994

# The Proper Legal Regime for 'Cyberspace'

I. Trotter Hardy

*William & Mary Law School*

---

## Repository Citation

Hardy, I. Trotter, "The Proper Legal Regime for 'Cyberspace'" (1994). *Faculty Publications*. 656.  
<https://scholarship.law.wm.edu/facpubs/656>

Copyright c 1994 by the authors. This article is brought to you by the William & Mary Law School Scholarship Repository.  
<https://scholarship.law.wm.edu/facpubs>

## THE PROPER LEGAL REGIME FOR "CYBERSPACE"

*I. Trotter Hardy\**

### TABLE OF CONTENTS

I.	Introduction .....	994
II.	What Makes a Legal Issue "New?" .....	996
A.	Examples of Problems That Are Not "New" .....	999
B.	New Twists on Old Problems .....	1000
C.	Why Are the Defamation and Copyright Cases New? .....	1002
D.	The <i>Playboy</i> Case and Copyright .....	1006
E.	Corporate E-mail Privacy .....	1008
F.	Custom Diverges from Real Space .....	1009
G.	Anonymous Messages .....	1010
H.	Obscenity and Local Communities .....	1012
I.	Reasonableness .....	1013
J.	Labeling Files .....	1014
III.	How Do Rules Regulating Behavior Arise? .....	1015
A.	Unilateral Self-Help: Stay Away .....	1016
B.	Law Merchant .....	1019
C.	Custom in Public International Law .....	1022
IV.	What Types of Rules Work Best? .....	1025
A.	Pure Self-Help .....	1026
B.	Contract Approaches .....	1028
C.	Privacy in the Corporate Setting .....	1032
D.	Transaction Costs .....	1033
E.	Custom .....	1036
F.	Defining "Reasonableness" Through Custom .....	1040
G.	Must System Administrators Read the Mail? .....	1041
H.	Anonymous Messages .....	1048
I.	International Torts .....	1051
V.	Conclusion .....	1053

---

\* Marshall-Wythe School of Law, College of William and Mary, Williamsburg, Virginia.  
E-mail address: thardy @ mail.wm.edu.

## I. INTRODUCTION

Much commentary in the popular and legal press these days raises legal questions relating to electronic communications over computer networks.<sup>1</sup> Popularly, the world of such communications is often called "cyberspace," a term that this article will also use as a convenient shorthand. Many academics and practicing lawyers are kept busy trying to answer those questions by determining how existing rules, such as those governing copyright or libel, apply to communications in cyberspace.<sup>2</sup> Implicit in the attention that both lawyers and the media are paying to the legal issues of cyberspace is the notion that cyberspace raises important and challenging new legal issues.

As one active cyberspace user has put it, in discussing an analogy between attempted break-ins of real property and attempted "break-ins" to a computer account, "I suggest that the problem in analyzing this matter is applying analogies from the everyday world in the first place. Things are different enough in Cyberia that our customary paradigms frequently don't fit. A person's computer account is not analogous to a store. It's far more personal turf to my mind. We may just need new rules."<sup>3</sup> This is not an isolated comment; others active in the on-line world have noted that in applying existing law to cyberspace "old analogies just don't cut it."<sup>4</sup>

The purpose of this article is in part to assess these notions: does the existence of widespread computer-assisted communications—cyberspace—really raise novel legal issues? Or does it raise the

---

1. See, e.g., Dan L. Burk, *Patents in Cyberspace: Territoriality and Infringement on Global Computer Networks*, 68 TUL. L. REV. 1 (1993); Scott Dean, *Cyberspace: The Final Frontier; Courts, Users Grapple with Legal Issues Surrounding Computer Bulletin Boards*, PA. L.J., Apr. 12, 1993, at 1; Henry H. Perritt, Jr., *Tort Liability, The First Amendment, and Equal Access to Electronic Networks*, 5 HARV. J.L. & TECH. Spring 1992, at 65; Terri A. Cutrera, Note, *The Constitution in Cyberspace: The Fundamental Rights of Computer Users*, 60 UMKC L. REV. 139 (1991); Sharon F. DiPaolo, Comment, *The Application of the Uniform Commercial Code § 2-201 Statute of Frauds to Electronic Commerce*, 13 J.L. & COM. 143 (1993); Robert Ritter, *E-mail Laws Changing; Judicial and Legislative Notice of the New Ways We Communicate*, THE QUILL, Oct., 1993, at 24; Vic Sussman, *Policing the Digital World*, U.S. NEWS & WORLD REP., Dec. 6, 1993, at 68.

2. See, e.g., Rosalind Resnick, *A Shingle in Cyberspace; Lawyers Online Find Clients—and Some Risks*, NAT'L L.J., Sept. 27, 1993, at 1.

3. Message from Bob Dunne to the CYBERIA-L listserv list (an open discussion group available over the Internet), comparing trying to "break in" to a computer with trying to break into a house. Friday, Oct. 8, 1993.

4. Shari Steele, Comments at Newjuris: A Conference on Law in Cyberspace 31 (Oct. 1993) (transcript of the electronic conference edited by Trotter Hardy, on file with the *University of Pittsburgh Law Review*).

same issues that lawyers have had to grapple with for decades, only in a different medium? The article will conclude that popular concern over the legal questions of cyberspace arises in some instances when, in fact, there is no "new" issue worth discussing. A more important conclusion, however, is that many of the circumstances of cyberspace do indeed give rise to new legal questions.

Another task of this article will be to determine what it is that makes a cyberspace issue "new" and hence worth the attention of commentators and those who are in a position to make or influence the making of rules about conduct.

This article will try to do more than just identify and characterize the cyberspace issues that are "new." In addition, we need to address the question of their best resolution. Should these issues provoke a legislative response, a case-by-case judicial response, or are there yet other mechanisms by which disputes may be avoided and resolved?

Recognizing that some cyberspace legal issues are new, some commentators and cyberspace users will inevitably call for prompt and specific legislation or regulation to clarify the problems. A statutory response along these lines has the virtue of bringing immediate clarity to immediate problems.

Of course, a specific statutory response is only one of many legal reactions. Case-by-case adjudication and its common law build-up of precedents can also be applied to cyberspace legal issues as well; an international convention can enact uniform model laws; citizens can create their own customs; service providers can specify behavior in their "part" of cyberspace through contracts; a modest degree of anarchy may even be desirable. Therefore, a second purpose of this article will be to discuss some of the other mechanisms by which individuals may regulate their conduct, including contracts, private associations, and custom.

Each of these and other forms of "self regulation" have an appropriate place. Some may be applicable to certain issues, and others may not. A third purpose of this article, therefore, will be to determine under what circumstances each of these different mechanisms for rule creation is most appropriate for several illustrative problems that are beginning to arise in cyberspace. The list of problems is by no means exhaustive. This article will conclude that the rapidly changing technology of computer communications implies a need for flexible legal regulation of behavior, and that flexible regulation in turn implies a presumption that the most decentralized rules should be applied whenever

possible. This will often entail contractual agreements worked out among the affected parties, rather than a broadly-applicable judicial or legislative resolution.

In examining all these questions, this article will draw on a number of readily-accessible materials, cited in the notes, but also on the author's own direct experience in one part of cyberspace, the Internet.<sup>5</sup> In particular, two electronic conferences that the author has conducted over the Internet, one on electronic mail ("e-mail") and its affect on law practice and teaching, and the second on an issue germane to this article: whether cyberspace should be treated as a separate legal jurisdiction. This article will rely on the insights from both conferences from time to time.<sup>6</sup>

## II. WHAT MAKES A LEGAL ISSUE "NEW?"

The question of whether an issue in cyberspace or elsewhere is "new" is largely a subjective determination. At a shallow level of analysis, every new medium is fraught with complex new legal questions, the most fundamental among them being whether existing laws designed with other media in mind should be applied to the new medium as well. On the other hand, at the deepest or most general level of analysis, no legal questions are unique: they all involve human conflict. The trick is knowing when to take a shallower and when a deeper view. Why view a question as interesting and new when a more abstract and general view will always result in the question's being seen as simply "old hat?" Or vice-versa: why view a question as "old hat" when a closer, more detailed look, will always result in the question appearing novel? There is a tension between characterizations at these two ends of the spectrum. Viewing an issue in a very high-level, general way, saves the trouble of having to create new rules and maintains an impression that the existing body of law is fairly stable, is modest in size, and hence is comprehensible.

The drawback to a very general view of problems and legal rules is

---

5. The "Internet" is a loose term for a collection of computer networks that are "interconnected" with one another such that electronic mail and other text can be sent and received among them. Roughly 20 million people are able to access the Internet today, and the number is growing. See generally John Matthews, *A Million Subscribers a Month Can't Be Wrong*, SUNDAY TIMES, June 26, 1994.

6. A copy of the transcript of the jurisdiction conference is on file with the *University of Pittsburgh Law Review*. I am grateful to the participants for helping me to begin to clarify some of my own thinking about the law of cyberspace, and therefore in indirectly helping me to write this article.

that the application of an existing body of such rules to any given problem is unpredictable. We could, for example, send every case—whether arising from cyberspace or real space—to a jury with the sole instruction that the jury should “Bring about justice between these parties as you think best.” That would allow us to have a very simple legal system (at least in appearance, if not in fact) and to accommodate technological change without any alterations to that system.

We do not do that, of course, because we also prize the consistency of decisions; we fear that such a high level of generality in the law would lead to inconsistent outcomes and an inability of citizens to order their affairs to comply with the law. Wildly varying outcomes from similar facts would strongly suggest a denial of due process and a basic unfairness that would tend to erode respect for the rule of law. That is why narrowly-drawn specific rules have appeal.

Let us put these remarks into the perspective of a particular cyberspace example. Suppose a cyberspace user receives an interesting personal message by electronic mail from a friend. This recipient decides to forward a copy of the message, also by electronic mail, to a third party. The third party, who does not know the message’s author, then decides to forward the message to all the members of an on-line discussion group (for example, Internet “listserv” list or a Compuserve or America OnLine forum). Perhaps this forum has several hundred members, all of whom now receive the original message.

Does the original author of the message, who, let us say, is unhappy and surprised by this extensive publication of the message, have a cause of action against either the friend or the third party?

At the shallowest (i.e., most detailed and specific) level of analysis, the answer is: who knows? Copying and forwarding mail is a common practice in cyberspace, but many cyber residents have not considered its possible unlawfulness and would doubtless be puzzled if they did. To be sure, there are laws of privacy and copyright in “real” space, but they were designed for a world in which copying a message to thousands of people took considerable time, effort and expense, and naturally gave the would-be forwarder pause for thought about issues such as privacy and copyright. With cyberspace, the argument goes, it’s a new ball game.

The facts may be generalized more abstractly, however: someone takes a work of authorship, makes thousands of copies of it, and distributes them to a segment of the public with no compelling educational, charitable, or other worthy-purpose reason for doing so. At this

level, the question is not new at all. It is, in fact, an easy case: the described conduct is clearly within the letter and spirit of the Copyright Act's prohibition against reproduction of copyrighted material without authorization.<sup>7</sup>

This particular issue will not be resolved by this article, but the example is used to illustrate the tension between general and specific views of legal issues. The dilemma here—what is the “right” level of abstraction from which to view cyberspace legal issues—is identical to the dilemma of all legal interpretation. At some level of specificity, nearly all cases are different from others (the parties' names may differ, among other things). With greater generality, other cases begin to look to be “on all fours” with a given situation.

In cyberspace, therefore, as elsewhere, the difficulty of formulating an issue arises because of the tension between conflicting desires. On the one hand is the desire for certainty, which argues for detailed, specific rules that are addressed to the cyberspace context. On the other hand is the desire to avoid the cumbersomeness of having a multiplicity of different rules for different situations.<sup>8</sup>

It is impossible to draw a clear line between these two competing values, but roughly speaking, we should try to draw it on either of two bases. The first is that of costs and benefits: when the uncertainty surrounding a legal issue is pervasive and hampers routine and desirable behavior, then a specific rule is worth having. When the uncertainty is minor and not a significant clog on routine behavior, then a specific rule will not be worth the additional complexity to our legal system. The second basis is that of policy: when the policy considerations that underlie an existing rule no longer make sense as applied to cyberspace, a new rule may be worth having.

Admittedly, this guide is nebulous and subjective, but it is what implicitly guides the rest of this article in the identification of those legal issues in cyberspace that are “new” enough to merit a resolution specifically tailored for the cyberspace context.

---

7. Copyright Act of 1976, 17 U.S.C. § 106(3) (1988). The privacy cause of action would likely be preempted. In any event, whether it would be preempted is independent of the cyberspace connection.

8. See, e.g., J. Robert Brown, Jr., *The Shareholder Communication Rules and the Securities and Exchange Commission: An Exercise in Regulatory Utility or Futility?*, 13 J. CORP. L. 683 (1988) (discussing tensions between keeping shareholders informed and creating too many unwieldy rules); Edward A. Jeffords, *Home Audio Recording after Betamax: Taking a Fresh Look*, 36 BAYLOR L. REV. 855 (1984) (discussing the conflicting interests of preventing mass home copying of video tapes and creating complicated legislation).

*A. Examples of Problems That Are Not "New"*

Some cyberspace issues seem wholly unremarkable: it is evident to any legal eye that they are readily governed by the same rules applicable to other forms of communication. Suppose a cyberspace user writes a defamatory message about another user and intentionally sends it over the Internet to a dozen other individuals. Is this situation materially different from sending the same message by fax, mail, or telegraph? It is hard to see how it could be. The same elements—defamatory content, publication to third parties, perhaps actual malice, and so on—must be determined in the cyberspace libel case as elsewhere.<sup>9</sup> Those issues seem indistinguishable from the same issues arising in a non-cyberspace context. In short, the fact that a communication was an electronic mail message on the Internet instead of a paper letter through the postal system makes little difference to the legal outcome.

Most lawyers would quickly reach agreement that many cyberspace issues are like the defamation example: they may or may not raise interesting legal questions (what is "defamatory?"), but whatever interesting questions they raise have nothing to do with the fact that the message was sent by e-mail.

Similarly, we could substitute for the defamatory message in our hypothetical a message that discloses embarrassing personal information about the same plaintiff. Again, assume that this revealing message is sent to a dozen e-mail recipients. Would anyone seriously argue that the issues of invasion of privacy are different from the situation where a dozen paper letters were sent to the same recipients? The answer is probably no.

We can replicate this example with any number of twists and reach a similar conclusion. For example, an author submits a collection of poems to a publisher with a proposal for a publication contract. The poems and the proposed contract are sent through the medium of cyberspace. The publisher publishes the poems—whether in cyberspace or on paper—without ever agreeing to any contract. Does the author have a copyright infringement case? Of course—and the answer does not turn on whether the original submission was through cyberspace by e-mail or by letter or fax.

None of these problems seems to raise any new issues because in

---

9. For a more detailed list of elements, see RESTATEMENT (SECOND) OF TORTS § 558 (1977).



these cases "cyberspace" is simply a means of communication directly between human beings. There is nothing about the connection medium itself that matters here or that differs from other communication means; all that has happened is that one person has communicated a libel (or an infringing text, etc.) to third parties. When cyberspace is simply a medium of direct communication between people—much like the telephone, mail, or fax—we should expect that the legal issues will not be materially different from issues in "real" space.

### *B. New Twists on Old Problems*

Clearly, then, a host of legal issues that can arise from computer communications do not pose any new legal questions, nor should they result in calls for new or revised legislation.<sup>10</sup> On the other hand, there do appear to be legal issues that are not so quickly dismissed.

For example, here is a slight variation on the "defamatory message" hypothetical that seems to be more puzzling. Suppose that an individual (or company) has set up and now runs a "bulletin board system" or "BBS." For purposes of this article, "BBS" is a short-hand way of referring to any computer service available by way of electronic communications.<sup>11</sup> The person who sets up and runs the BBS will be referred to as the "system administrator."

Our hypothetical BBS provides its users, as most do, with a facility for reading and writing electronic mail. All such mail is stored on the BBS computer; a given message will be read by its recipient when the latter next makes a connection to the BBS computer. On reading such a message, this second user, the recipient, can reply to the message, delete it, or both.

Suppose further that BBS user Alice enters (or "posts" as the term is often used) a message addressed to BBS user Bob. The message falsely accuses another person, Charles, of criminal wrong-doing. No

---

10. This is not to say that they will not be litigated; there will always be disputes over whether the elements of a cause of action have been met; there will always be ignorance over legal rules; there will always be those who violate known rules on the assumption that nothing will happen; and so on. My point here is simply that for some set of factual situations in cyberspace, the legal issues governing the situation will not be "new" in any helpful sense.

11. Commonly a BBS will be a computer that can accept a remote electronic connection from users at distant sites, typically from users who themselves have a computer equipped with a modem that can dial up the BBS over a telephone line. An example of such a large BBS is CompuServe; small ones are run by hobbyists from desktop computers in their homes. In this article, "BBS" will be used more generally to include any on-line service such as a discussion list, newsgroup, or information repository like Lexis or Westlaw.

legal privilege justifies Alice's communication of this accusation. If Bob later connects to the BBS—let us say, two weeks later—reads the defamatory message and thinks ill of Charles because of it, clearly the requirements of a cause of action in defamation are satisfied for Charles against Alice, as the original sender of the message. The message is defamatory by hypothesis, it has been intentionally "published" to a third party (Bob) without privilege, and we can assume it satisfies the other elements of defamation.

Now comes the new wrinkle: does the cause of action also extend to the system administrator as defendant? Should the administrator, at some time in that two week period when he had ample opportunity to do so, have read and deleted the message or at least returned it to the sender with an explanatory note?

We have no shortage of analogies and metaphors on this point. Indeed, a litigated case, *Cubby v. CompuServe*,<sup>12</sup> involved similar facts.<sup>13</sup> The *Cubby* court tried to answer the legal question by referring to analogies involving libraries, newspapers, bookstores, and so on.<sup>14</sup> In spite of this reliance on analogies, one senses that the court perceived that the computer BBS as the intermediary between the message's sender and recipient made the legal analysis different from the usual libel case involving these non-cyberspace analogs.<sup>15</sup> At the very least it is noteworthy that plaintiff's counsel thought the situation was worth a court test and its attendant costs. The situation was not routinely covered by the existing law, which has grown up around bookstores.

In short, the case seems to have the "feel" of a new issue in defamation law, one that is new precisely because of the cyberspace connection. In a similar way, had the issue been invasion of privacy or copyright infringement, the question would have had the same uncomfortable fit with "real space" examples.

---

12. *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991).

13. CompuServe contracted with a third party to maintain a "forum" or discussion area. This third party contracted with yet a fourth party, who uploaded a newsletter of sorts that contained disparaging statements about a competing newsletter. The competing newsletter sued CompuServe. *Id.* at 137-38.

14. *Id.* at 139 (citing to *Lerman v. Chuckleberry Publishing Inc.*, 521 F. Supp. 228, 235 (S.D.N.Y. 1981) and *Macaluso v. Mondadori Publishing Co.*, 527 F. Supp. 1017, 1019 (E.D.N.Y. 1981)).

15. The court actually stressed that the discussion forum was maintained by subcontractors, implying that the issue might have been harder had the forum been directly under CompuServe's control. *Id.* at 140. I suggest that it would be harder yet if the issue had been a message or file uploaded by an individual subscriber to CompuServe. See *infra* text accompanying notes 35-37, 122-38.

Recently a similar copyright case was in fact decided in *Playboy Enterprises v. Frena*.<sup>16</sup> The *Playboy* case featured what was apparently a desktop BBS<sup>17</sup> that provided a nice contrast with the giant Prodigy BBS at issue in *Cubby*.

The BBS in *Playboy* provided a service other than electronic mail, one very common with BBSs of all sizes: file sharing. Users have a facility provided to them for sending "files" to the BBS that other users may then copy onto their own computers. The process of sending files to a BBS is called "uploading;" obtaining a file from a BBS is called "downloading." "Files" can be computer programs, text, or graphic images.

In the *Playboy* case, a BBS user had uploaded graphic images that were digital copies of various photographs that had appeared in *Playboy* magazine. Playboy asserted copyright in the photographs and could have proceeded against the uploader who made and uploaded copies of the photographs. Instead, the magazine sued the system administrator of the BBS, who claimed that he was unaware of the existence of the copied photographs. The court held that his knowledge (scienter) was not an essential element of copyright infringement and decided in favor of Playboy on a summary judgment motion.

It is quite true that scienter is not a normal requirement of copyright infringement.<sup>18</sup> Yet this case will trouble many cyberspace users. It certainly will trouble system administrators,<sup>19</sup> for it seems to impose a near-impossible burden on them to screen all uploaded files. Many BBS systems experience hundreds of such uploads daily.

### C. *Why Are the Defamation and Copyright Cases New?*

Why do the *Cubby* and *Playboy* cases seem new enough in their cyberspace incarnation to justify further legal consideration? Several answers can be suggested, all showing that the policy issues in cyberspace are different from those of analogous "real" space situations.

---

16. 839 F. Supp. 1552 (M.D. Fla. 1993).

17. The opinion is not clear on this point, though the defendant's BBS was operated on a commercial basis: subscribers paid \$25 per month or purchased products from the defendant in order to access the BBS. *Id.* at 1558.

18. See *Fitzgerald Publishing Co. v. Baylor Publishing Co.*, 807 F.2d 1110, 1113 (2d Cir. 1986); *ABKCO Music, Inc. v. Harrisongs Music, Ltd.*, 722 F.2d 988, 998 (2d Cir. 1983); *Herbert Rosenthal Jewelry Corp. v. Kalpakian*, 446 F.2d 738, 741 (9th Cir. 1971); *Arice Industries v. Palmer*, 761 F. Supp. 1056, 1066 (S.D.N.Y. 1991); *Olan Mills v. Linn Photo Co.*, 795 F. Supp. 1423, 1437 (N.D. Iowa 1991).

19. I am one such person; I am the system administrator of a desktop BBS system myself.

The policies behind the rules of defamation liability for “real” space intermediaries like bookstores or libraries are nominally grounded in the observation that they should not be liable if they do not know or have reason to know of the defamatory content in the materials they carry.<sup>20</sup> But this “scienter” requirement in fact begs the question: *must* the intermediary know, that is, must it affirmatively seek to discover defamatory matter? A better rationale for the rule is practicality: bookstores carry thousands of titles, each hundreds of pages long, and most of them are not digitized. It is impractical for a bookstore to review every page of every book it carries.<sup>21</sup> Moreover, regardless of practicalities, nearly all bookstores operate similarly and would find review of their inventory equally practical or impractical. Therefore, a uniform bookstore exception to liability for republishing a libel makes sense.<sup>22</sup>

BBSs in cyberspace are not nearly so uniform, and the practicalities of screening messages may differ. For example, a BBS may carry thousands of messages, but each is likely to be only a few lines long, and they are digitized. There is at least an argument, therefore, that BBSs are “able” unlike bookstores, to screen messages through computerized text-searching techniques.<sup>23</sup> Some system administrators operate desktop BBSs that get a very low level of usage—a handful of messages a day—and charge no fees. It would be feasible (though not necessarily desirable) for them “manually” to review every message left on the system by actually reading them. On the other hand, large commercial BBSs like Prodigy and America OnLine serve as the mail box for thousands of messages a day; it is not feasible for those companies to examine every message. Indeed, that is what the *Cubby* court concluded.<sup>24</sup> It is simply not true, in short, that an on-line BBS is “like a bookstore.” Some are more like a bookstore and some less, and the

---

20. See RESTATEMENT (SECOND) OF TORTS § 581 (1977): “[O]ne who only delivers or transmits defamatory matter published by a third person is subject to liability if, but only if, he knows or has reason to know of its defamatory character.”

21. See *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135, 139 (S.D.N.Y. 1991) (citing *Smith v. California*, 361 U.S. 147, 152-53 (1959)).

22. See RESTATEMENT (SECOND) OF TORTS § 581 cmts. d, e, f and g (1977) (general discussion of news dealers, bookstores and libraries, transmitters of messages like telephone and telegraph companies, and radio and television broadcasting).

23. I am making an argument here, but not one that I am enamored of. I understand the difficulty of “scanning” for defamatory language: it is not at all like “scanning” for profanity where a simple text search may be all that’s necessary.

24. *Cubby*, 776 F. Supp. at 140.

tremendous variation should make a court uneasy about relying on generic "bookstore" analogies.

Second, even though large BBSs are something like bookstores or newsstands, BBSs are still new to society and their social value is less well established. This observation is significant not in the sense that courts will be stymied solely because BBSs are new and different, though that may happen. Rather, it is significant in that the judicial determination that bookstores need not screen all their publications for content is implicitly based on the conclusion that bookstores perform a very useful service for society, one with which judges and juries are well acquainted. They are less well acquainted with the benefits of BBS services, and cannot therefore rely on the same instinctive sense of the value to society of such services. That fact alone will make most courts hesitate before relying on "real" space analogies.

A third difference between the system administrator as intermediary and other intermediaries in real space is that certain real space intermediaries like telephone and telegraph companies are common carriers. A common carrier has no choice but to carry messages and thus in a sense gains immunity from defamation, privacy, and copyright infringement claims in exchange for agreeing to provide service on the same terms to all members of the public. Today it is easily possible, and common, for an individual or business simply to decide to be a cyberspace intermediary,<sup>25</sup> that is, to become a system administrator whose system serves as a store-and-forward message service and information repository for others, without the system administrator having to gain any governmental, regulatory approval or implicitly agree to rules applicable to common carriers.

Communications common carriers historically held a monopoly position in a given locality. Computer-based system administrators, in contrast, have proliferated with abandon today. In any city of size, there will scores of desktop BBSs and any of several large commercial systems to which one may have access. With this much competition there is little justification for considering BBS messaging systems to be "natural monopolies."

Nor do the smaller BBSs illustrate the characteristics of common carriers such as marketing to the public generally.<sup>26</sup> Many small BBSs do not "market" their services, and when they do, they are likely to

---

25. Setting up one's own desktop BBS requires a personal computer, modem, appropriate software, and access to a phone line. The total cost can easily be under \$2000.

26. Perritt, *supra* note 1, at 93.

advertise themselves through other BBSs, not to the public generally. Even larger BBSs may only advertise in computer specialty magazines. Moreover, many small BBSs do not charge for access, so the whole common carrier concept of uniform fees for service is inapplicable. Finally, the conclusion that a BBS is a "common carrier," may have the effect of triggering a vast array of regulatory responses<sup>27</sup> that would be wholly inappropriate for most smaller BBSs, and, with competition as keen as it is, wholly unnecessary for even the largest commercial BBSs.

A final difference between BBSs and bookstores is that nearly all bookstores and newsstands will carry materials from reliable publishers—that is, publishers who will remain in business and remain able to supply materials on a regular and predictable basis. Like other retail establishments, bookstores have a strong incentive not to stock materials from wholesalers who may be here today and gone tomorrow. The consequence of this self-interest by bookstores is that defamed plaintiffs will nearly always be able to turn to the publisher of the defamatory material for redress; they will have no strong incentive to include the bookstore as a defendant. More to the point, the ready availability of publishers as defendants means that courts will not feel any pressure to include the bookstore in the scope of defamation liability in order to provide compensation to the plaintiff.

With cyberspace intermediaries, the situation is very different.<sup>28</sup> An enormous amount of communication in cyberspace is made by individuals, rather than by centralized and typically solvent publishing businesses. Photocopy machines at one time threatened to turn every individual into a mass publisher, but cyberspace seems actually to have achieved that distinction in a way that photocopying never really did. Moreover, individual "publishers" who make use of desktop BBS systems that charge no fees have the option of remaining anonymous; whether solvent or not, they may be impossible to identify by the parties they are capable of defaming.

In sum, the policies behind relieving "real space" intermediaries, of defamation liability are not clearly applicable in cyberspace, or at least not uniformly applicable because (1) the practicalities of screen-

---

27. *Id.* at 94-95.

28. BRUCE W. SANFORD, *LIBEL AND PRIVACY* 48 § 2.7.4 (2d ed. 1991) ("Distinctions between those properly liable and those who are innocent middlemen are less clear in electronic publishing systems, particularly the 'interactive' type where subscribers can put their own messages into circulation."). Sanford suggests that a public access cable television channel might find its position "halfway between that of a telephone or telegraph service . . . and a regular news publisher." *Id.* By analogy, the same could be said of a BBS.

ing messages for defamatory content differ from BBS to BBS; (2) the value of intermediaries in real space situations is far more well established than the value of on-line intermediaries; (3) those intermediaries in real space that are common carriers have made trade-offs in the form of universal carriage and often monopoly positions that cyberspace system administrators do not typically make; and finally, (4) solvent publishers as potential defendants are more likely to exist in real space intermediary situations than in cyberspace. The applicable legal rules of defamation and privacy invasion surrounding the system administrator as intermediary are therefore sufficiently uncertain to make them "new" enough to merit attention.<sup>29</sup>

#### *D. The Playboy Case and Copyright*

Thus far, we have been speaking particularly of defamation, but with the copyright example of the *Playboy* case, the situation is much the same. Recall that in *Playboy* a system administrator of a BBS was found liable for copyright infringement, despite his professed ignorance of the infringement, because scienter was not a requirement of copyright infringement.

The no-scienter cases in copyright law appear to be justified by the underlying policy that ignorance of the law is no excuse: We do not want to encourage citizens to try to be "willfully ignorant," and we do not want to face the exceedingly difficult task in litigation of separating "true" ignorance from "deliberate" ignorance. Implicit in this policy applied to copyright is the belief that "ignorant" copyright infringers should be made liable so that they will educate themselves and be on guard against the possibility that they may be infringing another's rights the next time.<sup>30</sup>

This makes a great deal of practical sense in many "no scienter" cases in copyright. A typical case involves a defendant earning money from copyrighted music. The defendants are often the owner of a nightclub, a bar that hires bands to perform live music,<sup>31</sup> the proprietor of a store, an entertainment attraction that plays recorded music, or

---

29. For a good example of the attention these issues merit, see Perritt, *supra* note 1, at 95-110.

30. See PAUL GOLDSTEIN, COPYRIGHT § 9.4, at 162 (1989).

31. See, e.g., Famous Music Corp. v. Bay State Harness Horse Racing & Breeding Ass'n, Inc., 554 F.2d 1213 (1st Cir. 1977); Chess Music, Inc. v. Sipe, 442 F. Supp. 1184 (D. Minn. 1977).

the radio.<sup>32</sup> These defendants may genuinely not know that they need a license for their activities, but once they know, they know: further use of music without a license will lead to further infringement suits; the obtaining of the necessary license will solve the problem.<sup>33</sup> Even with other copyright industries, such as book publishing and television, which are also held to a no-scienter or strict liability standard,<sup>34</sup> the volume of possibly copyright infringing submissions is relatively manageable.

With the extremely wide variation in the size of BBSs in cyberspace, however, this same policy of discouraging actual or willful ignorance is far from uniformly applicable. For example, there will certainly be systems with a very few files that do not change much over time, where each file is well known to the system administrator. Holding such a system administrator liable for copyright infringement might have the salutary effect of encouraging the administrator to be more on guard next time. But much larger BBS systems are also common, ones with thousands of files and perhaps dozens or hundreds of these files uploaded or downloaded every day by dozens or hundreds of users.<sup>35</sup> It is not feasible for the system administrator of such a large system actually to look at every file uploaded, nor is there a reliable method of computer screening for these files. For that matter, there is no reliable method of manual screening, even if the system administrator could take the time to do so. A user could easily upload a third party's copyrighted short story, for example, claiming it as his own. How would the system administrator know whether it was the uploader's original work or not? Any number of other such files fall into a similar category, such as computer software that the uploader claims to have written, art work the uploader claims to have drawn, and so on.

The volume of uploads and downloads, the ease of copying, and

---

32. See, e.g., *Irving Berlin, Inc. v. Daigle*, 31 F.2d 832 (5th Cir. 1929); *Broadcast Music, Inc. v. Regal Broadcasting Corp.*, 212 U.S.P.Q. 624 (N.D.N.Y. 1981).

33. Usually a license would be obtained from ASCAP and BMI; between them, they hold the rights to nearly all U.S. music.

34. See GOLDSTEIN, *supra* note 30, § 1.15, at 44-45.

35. At least one BBS is run by an individual—not by CompuServe, or America On-Line, or other such system—that is based on a desktop computer and that carried, as of January 27, 1994, a total of 11,063 files for its users to download. It held a total of 45,782 electronic mail messages. This is high for a desktop system but not at all unheard of. The total number of BBSs in the U.S. alone is estimated by Boardwatch, a magazine that follows BBS issues, to be about 60,000. More than 12 million Americans call into a BBS every day. Kathleen Doler, *Inv. BUS. DAILY*, Feb. 17, 1994, *Computers and Automation Sec.*, at 4.



the wide array of copyrightable materials that can travel in cyberspace, all make BBS administrators poorly suited to the standards of "knew or ought to have known" about the copyright status of information held on their systems. Unlike a bar or club where music is played, system administrators cannot know in any general sense whether or not the files being up- and down-loaded from their systems should be treated with the gingerliness appropriate for commercially valuable copyrighted materials.

To be sure, there are some real-space intermediaries who will be unable to know the copyrighted status of works they review, such as book publishers or movie producers.<sup>36</sup> Yet applying the no-scienter policy to them still makes sense because the sheer volume of materials coming to them will be far less than the volume of materials arriving daily on some large BBSs. For a number of reasons, then, the role of the system administrator with regard to uploaded copyright-infringing materials seems different from real space analogs and hence "new" enough to be worthy of further attention.<sup>37</sup>

#### *E. Corporate E-mail Privacy*

Electronic mail privacy issue deserves mention because it is frequently discussed in the popular press<sup>38</sup> and is the subject of recently introduced legislation.<sup>39</sup> The question is whether employees have a privacy right in their electronic mail messages. Should employees be able to send notes to other employees or others outside the workplace without worrying that their messages will be read by a supervisor? On the other hand, should employers have a right to know whether their employees are revealing trade secrets or engaging in other wrongful conduct by way of e-mail?<sup>40</sup>

Note that this question is slightly different from the previous ex-

---

36. See GOLDSTEIN, *supra* note 30, § 1.15 at 45 ("Copyright law's rule of strict liability poses particularly hard problems for an intermediary, such as a book publisher or motion picture producer . . . ." (footnote omitted)).

37. This article will later conclude, incidentally, that in spite of these policy differences between real space and cyberspace intermediaries, strict liability ought to apply to system administrators in this circumstance, on grounds that other policies besides "ignorance is no excuse" make such a result desirable. See *infra* text accompanying notes 126-38.

38. See, e.g., James McNair, *Just How Private Is That Message?*, WASH. POST, Feb. 14, 1994, Wash. Bus. Supp. at 17.

39. S. 984, 103d Cong., 1st Sess. (1993) (the "Privacy for Consumers and Workers Act"); H.R. 1900, 103d Cong., 1st Sess. (1993) (companion bill).

40. See Stephen K. Yoder, *High-Tech Firm Cries Trade-Secret Theft, Gets Scant Sympathy*, WALL ST. J., Oct. 8, 1992, at A1.

amples. In those examples we looked at the question whether a system administrator should be *required* to look at mail or files from users that might be "wrongful" in relation to some third party. In the employment setting, we are asking whether the employer, who in this context is the "system administrator," should be *allowed* to look at mail intended for third parties that might be wrongful with respect to the employer.

Once the employment situation is looked at in this light, it becomes obvious why this situation is also "new" enough to merit attention: just as in the defamation and copyright examples, we have a system administrator as intermediary, one that is not a common carrier and with whom society has little experience and hence is unable to make an accurate assessment of value. As before, we can also expect wide variation in the scope of the system administrator's activities in regard to employees' privacy and in the scale and extent to which employees use e-mail at work.

Consequently, despite the reversal of the role of system administrator and the legal question—a shift from whether the system administrator should be required to read to whether the system administrator should be allowed to read—the fundamental question of corporate e-mail privacy strikes us as new because of the system administrator's role as a communications intermediary.

#### *F. Custom Diverges from Real Space*

The presence of the cyberspace system administrator as intermediary, with widely varying capabilities and opportunities for screening those documents for which the administrator is the intermediary, thus raises some interesting new questions. Another set of vexing questions seems certain to arise from this fact: a cyberspace community is quite likely to develop its own customs, ones that differ significantly from those of real space. To rely once again on the copyright issue, for example, we can look at the well recognized cyberspace custom of copying e-mail messages and forwarding them to others. In real space, this might be a clear copyright violation, but if everyone in cyberspace "does it all the time," and knows that others do it all the time, might not some sort of estoppel or implied waiver of copyright rights arise?

This sort of situation, where custom conflicts with established intellectual property law, has happened before. The usual rule of copyright is that rough ideas cannot be protected. Only when an idea is sufficiently developed to be an "expression" does copyright attach. At-

tempts to protect ideas under other, state law theories, usually fail as well. For example, in *Lueddecke v. Chevrolet Motors Co.*,<sup>41</sup> the plaintiff had submitted suggestions to General Motors for the placement of various mechanical components in the engine compartments of Chevrolets. General Motors adopted the suggestions without payment to the plaintiff. The plaintiff sued on a state law theory but lost, on grounds that the idea was not sufficiently "novel" or "concrete."<sup>42</sup>

Yet, when a strong industry custom exists, the results may contradict these well-established copyright and state law rules. For example, in the early days of radio broadcasting, it became the industry custom to buy and sell rough radio series concepts—exactly the sort of thing that would likely fail to achieve copyright protection for being only an idea, and fail to achieve state law protection for lack of sufficient novelty and concreteness. Here, then, was a situation in which the intellectual property laws did not provide the property right on which a whole industry depended. Under those circumstances, one court, in *Cole v. Phillips H. Lord, Inc.*,<sup>43</sup> recognized the industry custom as sufficiently strong to achieve judicial deference and recognition. In effect, the court created a pseudo-copyright right where such a right conflicted with copyright law but accorded with industry custom.

Customs are developing in cyberspace as they might in any community, and rapid growth in computer communications suggests that there may be a great many such customs before long. Many of these customs conflict with "real" space customs. As with the *Cole* case, a court might be persuaded to recognize a cyberspace industry custom as legally enforceable even though it differed from the rule applicable in real space. The potential for judicial recognition of this practice is another reason why interesting new questions will arise in cyberspace.

### G. Anonymous Messages

Strikingly lower costs for cyberspace communications will bring other activities to the forefront of our interest as well. These activities are possible in some sense in "real" space but are so much more costly there that they do not pose a real problem. It is possible, for example, with the cooperation of one or more intermediary computers, to create

---

41. *Lueddecke v. Chevrolet Motor Co.*, 70 F.2d 345, 345-47 (8th Cir. 1934).

42. *Id.* at 348.

43. 28 N.Y.S.2d 404, 409 (N.Y. App. Div. 1941); see also *Whitfield v. Lear*, 751 F.2d 90, 93 (2d Cir. 1984).

and send an "anonymous" electronic message through cyberspace—a message whose originator cannot be ascertained.<sup>44</sup>

What are the problems of anonymous messages? They are just the sorts of things we have been addressing: What if an anonymous message is libelous? Infringes copyright? Sends trade secrets to others? The obvious answer is for a court to subpoena the records of the intermediary computer, the one that strips off the sender's identifying information. Yet this may not be a practical answer if that computer systematically erases the records of its anonymously forwarded mail, or if the intermediary computer is located in a difficult to reach foreign jurisdiction.<sup>45</sup>

We have the capability of sending anonymous messages today, of course. Telephone calls can be made and letters can be sent without any identification of the sender.<sup>46</sup> Yet telephone calls cannot easily and

44. The computer used to strip off the sender's name and address is called an "anonymous re-mailer." These computers and their anonymous facility already exist. *Personal conversation with Mike Godwin*, COUNSEL FOR THE ELECTRONIC FRONTIER FOUNDATION (Feb. 4, 1994).

45. Apparently anonymous remailer computers on the Internet exist in Finland, for example. *Id.* I recently received a message that purported to be an invitation to use anonymous remailers to engage in the sale of "information" apparently in violation of any number of laws. I have no way of knowing whether the message was a joke, or was exactly what it claimed to be, but what it said was this:

BlackNet is in the business of buying, selling, trading, and otherwise dealing with information in all its many forms. Our location in physical space is unimportant. Our location in cyberspace is all that matters. Our primary address is the PGP key location: "blacknet<nowhere@cyberspace.nil>" and we can be contacted (preferably through a chain of anonymous remailers) by encrypting a message to our public key (contained below) and depositing this message in one of the several locations in cyberspace we monitor. Currently, we monitor the following locations: alt.extropians, alt.fan.david-sternlight, and the "Cypherpunks" mailing list.

BlackNet is nominally nonideological, but considers nation-states, export laws, patent laws, national security considerations and the like to be relics of the pre-cyberspace era. Export and patent laws are often used to explicitly project national power and imperialist, colonialist state fascism. BlackNet believes it is solely the responsibility of a secret holder to keep that secret—not the responsibility of the State, or of us, or of anyone else who may come into possession of that secret. If a secret's worth having, it's worth protecting.

BlackNet is currently building its information inventory. We are interested in information in the following areas, though any other juicy stuff is always welcome. "If you think it's valuable, offer it to us first."—trade secrets, processes, production methods (esp. in semiconductors)—nanotechnology and related techniques (esp. the Merkle sleeve bearing)—chemical manufacturing and rational drug design (esp. fullerines and protein folding)—new product plans, from children's toys to cruise missiles (anything on "3DO"?)—business intelligence, mergers, buyouts, rumors.

46. Whether telephone calls "should" be capable of anonymity is another debate, one that surrounds the use of "caller id" and "caller id blocking" features now offered to many telephone customers. For an indication of the problem's complexity, see *Barasch v. Pa. Pub. Util. Comm'n*, 576 A.2d 79 (Pa. Commw. Ct. 1990).

quickly be made to thousands of people, as can e-mail messages. And paper mail will usually have higher costs than e-mail, which serve as a significant deterrent. Paper mail also possesses identifiable characteristics such as the type of paper or ink that make anonymity less certain than with e-mail. Of course, these identifying paper characteristics can be masked with sufficient expenditures of money, but again, the much lower costs for the same anonymous facility in cyberspace will make enough of a quantitative difference, despite the "real space" analogies, that we can consider the problem of anonymity as a "new" one.

#### *H. Obscenity and Local Communities*

Another source of new problems in cyberspace will arise from the fact that residents of cyberspace are also residents of "real" spaces; they will thus be members of two (or more) different communities. For rules, such as those on obscenity, that turn on some sort of "community standard,"<sup>47</sup> this "dual citizenship" circumstance will likely prove vexing indeed.

There is already an exchange of pornographic images and dialog over cyberspace.<sup>48</sup> Suppose a cyber resident physically located in Cleveland downloads an erotic image from a BBS also physically located in Cleveland and tells her friends in town about it, so that all of them later download the image. Suppose further that this small "cyberspace community" within the larger community of Cleveland is not offended by the image but that the citizenry of Cleveland as a whole would be.

Assuming that Cleveland has an anti-pornography ordinance that punishes the "sale" or "display" of obscene material, may it enforce those laws against the BBS? Many of the commercial BBSs, such as America OnLine and Compuserve, provide images for downloading that are intended to be more-or-less erotic,<sup>49</sup> making this example plausible

There is an initial question about whether such images are actually being "sold," but assuming that they are (and certainly it is quite

---

47. See *Miller v. California*, 413 U.S. 15, 32 (1973); see generally FREDERICK F. SCHAUER, *THE LAW OF OBSCENITY* 116-35 (1976).

48. See *Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993); Richard Leiby, *Al Gore Takes a Spin on the Info Highway; A Few Potholes Mar "Electronic Town Meeting,"* WASH. POST, Jan. 14, 1994, at G1, G2 ("[T]he superhighway is already clogged with porn . . .") (emphasis omitted).

49. See Joel Garreau, *Bawdy Bytes: The Growing World of Cybersex*, WASH. POST, Nov. 29, 1993, at A1.

possible for such images to be charged-for individually), has the BBS violated the ordinance? There is at least a good argument that if the purpose of the ordinance is to control the moral tone of the community, then the ordinance has been violated. If the purpose is to prevent the display of images that may offend passers-by, however, there would be no violation because no one is a passer-by in this context.

But even if the policy of the ordinance is to control the moral tone of the community, is it fair to hold the BBS responsible? After all, access to most BBSs is available with a phone call from anywhere, from any jurisdiction around the world, not just from a single community with a particular standard of obscenity. Application of the "moral tone" policy seems wholly out of place.

Whether one agrees with this analysis or not, the point is merely that the ability to belong to two communities, one physical and one electronic, is likely to cause new problems relating to community standards. For that matter, it makes little sense even today, and surely will make no sense tomorrow, to speak of one "cyberspace community." There are differing interest groups all across cyberspace. The problem of "dual citizenship" is therefore likely to be played out on an even larger scale, as cyberspace users become multiple-citizens of a bewildering number of electronic—and at least one physical—communities.

### *I. Reasonableness*

Finally, a broader issue related to the "cyberspace community" standards question is what the "reasonable" person would do in a given circumstance. The concept of reasonableness is pervasive in Anglo-American law, especially tort law. There is no inherent reason why the concept cannot apply in cyberspace. The problem is that in many situations, juries—and even cyberspace users themselves—may not know and may have no basis for knowing what is reasonable in cyberspace.

Again, let us analyze a practical example. A mortgage finance company keeps extensive records on credit and other financial history information about thousands of clients on a computer in its office. The computer system is secured by a variety of access restrictions such as passwords, security levels, and so on. One day a disgruntled former employee figures out a way around the security features and, using computer communications, copies thousands of confidential financial records.

The question of the company's liability for negligence in permitting the extraction of data in the first place can be handled unexcep-

tionally: companies have long maintained data security practices, so that testimony on the reasonableness of this company's practices should be readily available. A harder question is whether, assuming that it can reconstruct all its data, the company nonetheless has a legal obligation to notify its customers of this "information theft."

Is this question any different from a question about the theft of tangible goods from a bank vault? Suppose someone breaks into the vault and manages to rob every one of the safe deposit boxes. Suppose further that the bank recovers the stolen items. What is the obligation of the bank to notify deposit box renters? The answer may not be clear here either, but that is partly because this sort of incident has never happened before. Before the days of computers, wholesale theft of the valuables of thousands of people was impractical and unlikely.

Now mass theft of information is possible. General tort principles can be applied, of course, to address the reasonableness or not of reporting the theft within some period of time. Arguments might be supported by the "duty to warn" cases much like those involving a psychotherapist's duty to notify a third party of a patient's threats to their well being.<sup>50</sup> But whatever the arguments and analogies, any decision grounded in reasonableness, whether this bank example or any other, is a decision that draws on the experience and common sense of the jury. It is unlikely with these "information thefts" that a jury will have any useful common sense experience. Hence the question, at least for a time, will remain a novel one for cyberspace.<sup>51</sup>

### *J. Labeling Files*

Other questions based on reasonableness are likely to arise until more of the reasonable practices of cyberspace are clarified, or indeed, until they develop in the first place. One such question is whether there is a requirement that a system administrator's files be given accurate, meaningful titles or descriptions. To put the question another way, can a system administrator be found liable for negligently mis-naming or describing files on his system? Or, can the system administrator be liable for the mis-description of files by those who uploaded them in the

---

50. *Tarasoff v. Regents of Univ. of Cal.*, 551 P.2d 334, 340 (Cal. 1976).

51. To say that the jury will be unfamiliar with the custom of cyberspace is not, of course, to say that the jury cannot decide a case, perhaps with the aid of expert testimony. But it is to say that the first few such cases would presumably be difficult ones and hence would benefit from clarification.

first place—that is, for “permitting” misnamed files to reside on the system?

The problem might arise in this fashion: a system administrator operates a BBS on which a mixture of general interest materials resides. Access to each “area” on the BBS is open, but areas are labelled, apparently in accord with their content. One group of files might be labelled “shareware games,” another “Windows utilities,” and so on. Each of these areas contains some files that the system administrator has placed on the system and some files that have been uploaded by other BBS users without the active participation of the administrator.

Suppose that a user has uploaded a file into the “Shareware Games” area under the file name “Chess.” In fact, the game when executed turns out to be not a chess game at all, but a hard-core pornographic video sequence. The parents of a twelve-year old have explored this BBS briefly and, on the basis of the area and file names, concluded that the BBS is suitable for their child. The child then innocently accesses the BBS, downloading “Chess,” which the child executes to his and his parents’ considerable surprise.

Is the system administrator liable for the negligent infliction of emotional distress or on some other grounds to the child? Once again, the new role of the system administrator as intermediary brings this sort of question to the fore in a way that simply has not occurred and is not likely to occur with current technologies in real space.

### III. HOW DO RULES REGULATING BEHAVIOR ARISE?

As has been shown, new legal problems from cyberspace are likely to arise for a number of reasons: existing policies behind real space analogs to cyberspace behavior may simply not apply, particularly regarding the new role of the system administrator as an unfamiliar intermediary in communications; the falling costs of communications in cyberspace may provide incentives for conduct currently possible but heretofore infeasible; new technologies may create opportunities for new kinds of behavior like anonymity; customs in this new medium may differ from existing customs or be unfamiliar when the inquiry turns to “reasonableness,” and so on. Given that there are some “new” legal problems in cyberspace for at least these reasons, how should the legal system respond?

Commonly one thinks of legal rules responsive to the needs of new situations as being handed down by a higher authority, either courts or legislatures. One option, then, is for those affected by the new develop-



ments of cyberspace to take matters to court and seek resolution under general common law principles and whatever existing statutes might arguably be applicable. Alternatively, they can press a legislative body such as the Congress or state legislatures to enact statutes that clarify rights and obligations.

Rules guiding conduct, however, can arise in an astonishing variety of ways, many of them from individuals themselves quite apart from judicial or legislative pronouncements. For example, parties can form their own rules collectively; they can reach contractual agreements on behavior toward each other as individuals; they can form groups and associations with charters and by-laws; they can set up commissions and panels of experts to devise model rules; they can get by without rules; etc.

We have many historical and contemporary examples of what happens when a central authority does not promulgate rules: stores may hire private security guards; parties may agree on their own behavior vis-a-vis one another in the form of contracts; in international business transactions, parties often specify not only their behavior toward one another, but also under which set of laws they will resolve any disputes later arising; in relations between sovereign nations, there is no authoritative decision maker with the power to enforce decisions, yet a body of international law has nevertheless arisen over the centuries; countless private associations have formed their own rules of conduct by adopting by-laws.

For that matter, a large part of our current cyberspace, the Internet, is essentially ungoverned by any sort of "higher" authority. Other parts, the commercial service providers in cyberspace like Prodigy, Compuserve, and America OnLine, are largely governed by their corporate founders and managers, not by Congress or the judiciary.

This section of the article will therefore examine a variety of non-judicial and non-legislative approaches that have been used to regulate behavior in other contexts as a guide to the kind of regulatory mechanisms that might be usefully applied in cyberspace.

#### *A. Unilateral Self-Help: Stay Away*

The lowest level of self-help is unilateral action by an individual. We might capture the sense of this measure with the phrase "if you don't like it, don't do it." Certainly at times this is the appropriate response of the legal system. We do not have a rule prohibiting paint stores from carrying unattractive colors of paint; we assume that if in-

dividuals do not like certain colors, they will not buy them. The same will certainly be true of various activities in cyberspace.

In general, unilateral activity avoidance by individuals is an appropriate response when the activity has no significant external effects, and the costs of reaching a contractual agreement with the activity are high relative to the value of such an agreement. The lack of external effects mean that unilateral action is truly unilateral—others will not be harmed or benefited so that the interests of others need not be taken into account. High transaction costs simply mean that a contract-based solution is not feasible.

If the costs of transacting with the activity are relatively low, we move into the area of contracts—"bilateral self help"—as the next level "up" in the hierarchy of decentralized to centralized rule development. Contracts offer a richer field of examples for the regulation of behavior than unilateral self help because contracts can be tailored to an enormous variety of circumstances and can specify complex relationships and duties.

Contracts are sometimes thought to be a narrow form of behavior control; they seem to apply most comfortably to two parties and to exhibit rapidly increasing transaction costs when more and more parties seek to become members of an agreement. In fact, transaction costs are only problematical when they are large with respect to the value of the contractual agreement. When such an agreement is highly valuable, it can be quite complex, involving many parties over a period of many years, even when transaction costs are high in an absolute sense.

A particularly nice example of this comes from turn-of-the-century France, where contracts effectively substituted for a regime of intellectual property protection.<sup>52</sup> In the early years of this century, French plant growers began to realize the potential of deliberate breeding experiments for commercially significant plant improvements. They sought from the government the enactment of a scheme of intellectual property protection for plant varieties. This request was turned down on the grounds that one cannot obtain such protection for products of nature.

In response, the breeders formed elaborate associations and cooperatives, with multi-level contractual agreements, that provided for rights of ownership, including obligations to pay royalties, in experi-

---

52. This illustration is from Ejan Mackaay, *Economic Incentives in Markets for Information and Innovation*, 13 HARV. J.L. & PUB. POL'Y 867, 902-03 (1990).

mentally developed plant varieties. This contract-based scheme endured from about 1904 until 1970, when the French government enacted a legislative scheme of property rights in plant varieties that essentially followed the lines of the previous contractual agreements.<sup>53</sup>

Other contractual arrangements may similarly work to regulate the behavior of individuals in a larger group, even when the motivation of a commercial endeavor is absent. For example, several people might want to start a cyberspace church, club, charitable foundation or other interest group. Would it be possible for such groups to form in cyberspace? Of course—there is every reason to think that they will because we have ready examples of such agreements from the law and practice of private associations. Trade associations come most quickly to mind as an example of private associations because organizations that exist to further the commercial and educational needs of industry or professional groups are so common. Yet scientific, educational, religious, and charitable private associations exist as well.<sup>54</sup>

There is no impediment to individuals forming an association under ordinary association law, perhaps incorporated as most such associations are, drawing up its own by-laws for behavior in cyberspace. One would expect that most such rules would relate to the activities of the group as they apply to “real” space; but there is no reason to think that an organization’s by-laws could not also regulate members’ conduct toward each other in cyberspace. Indeed, one can easily imagine groups forming whose sole contact and interaction and perhaps purposes relate only to cyberspace.

It is hornbook law that “[t]hose who join an incorporated trade or professional association agree, by such affiliation, to abide by the association’s by-laws.”<sup>55</sup> An association, thus, has broad discretion to control its membership, an aspect of the freedom of association under the First Amendment, though with judicially enforced limitations in some areas such as anti-trust activity or violations of civil rights laws.<sup>56</sup> Con-

---

53. *Id.* at 903.

54. Indeed, although the oldest continuous association in the United States is a trade association—the Philadelphia House Carpenters, begun in 1724—the second oldest is scientific—the American Philosophical Society, which began in 1743. JERALD A. JACOBS, ASSOCIATION LAW HANDBOOK 12 (2d ed. 1986).

55. GEORGE D. WEBSTER, THE LAW OF ASSOCIATIONS § 2.03(1)(b) (1993).

56. *Id.* at § 2.07(1)(a). For the antitrust discussion, see *supra* text accompanying notes 14-17.

trol under an association's by-laws is normally enforced by means of expulsion or other by-laws-designated sanction.<sup>57</sup>

Private association law does not exist in a vacuum, of course; some aspects of such associations are regulated under state corporate law. That implies that not all relevant legal issues for an association can be handled by the association's members themselves.

For example, many state association statutes specify the need for "annual meetings" to be held either in the state of incorporation or elsewhere.<sup>58</sup> Obviously such statutes were written with physical meetings in mind; would it be acceptable under associational law for the group to hold a virtual meeting in cyberspace? Typical meeting tasks include voting on officers; there would have to be devised a form of reliable cyberspace voting procedure, as well as an assessment of the presence of a quorum.

With regard to such voting, one envisions all manner of fraudulent activities possible: phantom "virtual" members casting votes when corresponding real members are sick, "absent," or unaware of the meeting. Yet the authentication issues here are not significantly different from authentication in cyberspace generally; presumably, whatever techniques arise to verify contract offers, exchanges of promissory notes and court document will also work to establish the identity of association members. The point is simply that there is a clear mechanism for parties with strongly held common interests to self regulate through private associations.

### *B. Law Merchant*

It is also possible that many cyberspace users will interact with each other outside of any previously negotiated contracts and outside of any on-going groups operating under association or corporate law. What rules, in the absence of a statute, might grow up to govern the relations among those who deal with each other on a frequent basis, but do not have prior contracts, by-laws, or other agreements? We should expect that such situations are fertile ground for the development of customs, customs that might even evolve to the point of becoming judicially recognized and hence legally binding.

Why expect the development of customs? We have an historical parallel to cyberspace, one in which customs grew from the "bottom

---

57. *Id.* at § 2.07(2)(d).

58. *Id.* at § 2.07(3).

up" and achieved the status of legal enforceability, in the Medieval "Law Merchant." The Law Merchant was a body of customary rules—the precursor to contemporary commercial law—that grew up in Medieval Europe as a response to the needs of international commerce. We commonly think of the modern world as especially "global" in its commerce; but it is instructive to note that even in the Fourteenth Century, travelers and traders covered much of the European continent and England.<sup>59</sup>

The locus of much of the Medieval trade activity was the "trade fair." Trade fairs were periodic gatherings of merchants at central locations in Europe and England, where goods of all sorts were bought and sold for shipment or transport back to the merchant's home territory. These trade fairs featured merchants from Asia as well as Europe, and gave rise to a number of commercial instrument such as bills of exchange and bills of lading.

What exactly was the "Law Merchant?" It was simply an enforceable set of customary practices that inured to the benefit of merchants, and that was reasonably uniform across all the jurisdictions involved in the trade fairs.<sup>60</sup> Two key elements of the Law Merchant for our purposes were first, that no statute or other authoritative pronouncement of law gave rise to its existence, and second, that the Law Merchant existed in some sense apart from and in addition to the ordinary rules of law that applied to non-merchant transactions.

In other words, the Law Merchant made no attempt to displace existing rules promulgated by the jurisdiction in which a given trade fair might be held; it merely supplemented those rules with specific rules applicable to merchants' transactions.<sup>61</sup> Special courts grew up to enforce the Law Merchant. These were merchant courts in every sense:

---

59. See BARBARA W. TUCHMAN, *A Distant Mirror* 55-57 (1978).

60. The LAW MERCHANT was envisioned as

. . . a system of law that [did] . . . not rest exclusively on the institutions and local customs of any particular country, but consisted of certain principles of equity and usages of trade which general convenience and a common sense of justice have established to regulate the dealings of merchants and mariners in all the commercial countries of the civilized world.

LEON E. TRAKMAN, *THE LAW MERCHANT: THE EVOLUTION OF COMMERCIAL LAW* 11-12 (1983) (quoting *Bank of Conway v. Stary*, 200 N.W. 505, 508 (N.D. 1924) (Johnson, J.)).

61. See WYNDHAM A. BEWES, *THE ROMANCE OF THE LAW MERCHANT* 15-25 (1923); 1 WILLIAM HOLDSWORTH, *A HISTORY OF ENGLISH LAW* 543 (The Law Merchant "was a law which necessarily differed at many points from the ordinary law, for 'no technical jurisprudence peculiar to any country would have been satisfactory to traders coming from many different countries.'") (quoting JOHN WILLIAM SMITH, *MERCANTILE LAW* 1xx (ed. 1890).

their jurisdiction was that of commercial transactions, and their judges were drawn from the ranks of the merchant class itself on the basis of experience and seniority.<sup>62</sup>

The emphasis of these merchant courts and the law they applied was a speedy resolution of disputes, an important element when time is money. But another significant attribute of these courts was practicality and flexibility. Merchant practices were not static, and a reliance on local judges, taken from the merchants' own ranks and following the known customs of merchants, gave the Law Merchant an adaptability to changing times that statutory enactments would not have provided.<sup>63</sup>

The Law Merchant courts eventually declined in use, but the rules of the law merchant continued to be applied by common law courts after the close of the sixteenth century.<sup>64</sup> Here, in short, was a custom that over time acquired powerful legal force without the backing of the sovereign.

The parallels with cyberspace are strong. Many people interact frequently over networks, but not always with the same people each time so that advance contractual relations are not always practical. Commercial transactions will more and more take place in cyberspace, and more and more those transactions will cross national boundaries and implicate different bodies of law. Speedy resolution of disputes will be as desirable as it was in the Middle Ages! The means of an informal court system are in place in the form of on-line discussion groups and electronic mail. A "Law Cyberspace" co-existing with existing laws would be an eminently practical and efficient way of handling commerce in the networked world.

---

62. See also TRAKMAN, *supra* note 60, at 15. Holdsworth noted that "Though the court [of piepowder, the merchant court at a fair] was held by the mayor, bailiffs, or steward, the judges of the court, in the thirteenth and fourteenth centuries, were the merchants who attended the fair." HOLDSWORTH, *supra* note 61, at 536.

63.

The strict law prevailing within the ordinary courts of the realm, generally being unable to adjust to changing commercial custom with the same ease as could a commercial system, played only a minimal role in the development of the Medieval Law Merchant. Strict rules lacked the flexibility to vary in response to the peculiarities of the merchants, to their trade background and to their form of bargaining.

TRAKMAN, *supra* note 60, at 16.

There was evidently a fair amount of local variation (and some local prejudice) in the merchants' rules, however—perhaps an inevitable by-product of decentralized rule-making. See *id.* at 17-20.

64. HOLDSWORTH, *supra* note 61, at 569.

### C. *Custom in Public International Law*

Reliance on custom alone as a regulator of behavior may strike some readers as ineffective, notwithstanding the historical evidence of the Law Merchant. But we have contemporary examples of "customary law" as well that exemplify the practice of such a regime.

Many lawyers would be surprised to learn that an enormous amount of law governs transactions between nations, provides the rule of decision in disputes, and affects the willingness of nations to enter into treaties and, yet none of this law has ever been "enacted" or otherwise created by a sovereign. This is public international law. The sources of international law include treaty, custom, and "general principles of law."<sup>65</sup> Of these three sources, treaties are much like contracts between nation states, with obvious parallels to contracts formed between individuals. A discussion of contracts was made earlier and will not be revisited here.

"General principles" of law is a concept based on observations that many nations' legal systems contain fundamental provisions that are widely similar to those of other nations. When these common provisions are frequently observed as binding within each nation, they form the basis of a kind of "law" that will be recognized implicitly as legally binding when nations deal with one another.<sup>66</sup> Since cyberspace is not a recognized legal jurisdiction with an existing sovereign and cannot deal as a nation with other nations, however, this aspect of public international law is also not relevant to our inquiry. It is rather the third source, "customary international law," that I want to focus on here.

Some international law scholars argue that adherence to custom can never gain the force of law, basing this view on the jurisprudential principle that "law" is the command of a sovereign.<sup>67</sup> Yet there are quite clearly times when nations themselves show a willingness to abide by an international custom, and a willingness to be bound by the decisions of international courts.<sup>68</sup> This willingness is not contradicted by

---

65. Statute of the International Court of Justice, June 26, 1945, art. 38, 59 Stat. 1031, 3 Bevens 1153; *see also* MARK W. JANIS, AN INTRODUCTION TO INTERNATIONAL LAW 4-6, 10 (1988).

66. JANIS, *supra* note 65, at 54-58.

67. Generally this line of thinking follows philosopher John Austin's views that the only true "law" is "positive law," that is, law enacted by a sovereign. *See id.* at 2-3 (JOHN AUSTIN, THE PROVINCE OF JURISPRUDENCE DETERMINED 208 (1st ed. 1832)).

68. Nations do in fact follow international law most of the time. LOUIS HENKIN, HOW NATIONS BEHAVE—LAW AND FOREIGN POLICY 47 (2d ed. 1979).

the fact that in international jurisprudence it is common for there to be no clear ranking of authoritativeness in court decisions.<sup>69</sup>

Despite the lack of a "world authority," custom in international law has a long history. Roman law recognized it with the notion that "long-continued custom approved by the consent of those who use it imitates a statute."<sup>70</sup> The United States Supreme Court officially recognized it as enforceable in U.S. domestic courts in 1900, in *The Paquete Habana* case.<sup>71</sup> In *The Paquete Habana*, Cuban fishing vessels had set out to sea, their proprietors not knowing that war had broken out between the U.S. and Spain, then colonial owner of Cuba. United States warships seized the Cuban fishing vessels as prizes of war, but the Supreme Court declared that "[b]y an ancient usage among civilized nations, beginning centuries ago, and gradually ripening into a rule of international law, coast fishing vessels, pursuing their vocation of catching and bringing in fresh fish, have been recognized as exempt, with their cargoes and crews, from capture as prize of war."<sup>72</sup>

Note that under the facts of *The Paquete Habana* the U.S. was not a party to any treaty or other documented requirement to release the vessels; the Court's decision was based solidly on long-standing custom, and nothing more. Thus, custom alone can give rise to an enforceable legal requirement; but how does one know when a custom has reached the exalted state of legal enforceability? In international law, a custom becomes enforceable when it has become more or less historically uniform, and when nations follow the custom as much from a sense of legal obligation as from habit or convenience.<sup>73</sup> This is not exactly a well-defined circumstance; indeed, it is a bit circular: a custom will be legally enforceable when nations follow it from a sense of legal obligation. How does one know that nations feel a sense of legal obligation? At least in part, the answer is that a court will treat the custom as legally enforceable!

Nonetheless a few guidelines exist to help in the determination of the sense of moral obligation. One indication comes from non-enforceable agreements in international fora such as the United Nations. Member nations vote on resolutions and hence indicate their views on the

---

69. JANIS, *supra* note 65, at 6.

70. THE INSTITUTES OF JUSTINIAN, THE ELEMENTS OF ROMAN LAW 45 (bk. I, tit. II, § 9) (Lee ed., 4th ed. R.W. Lee, 1956), quoted in JANIS, *supra* note 65, at 35.

71. 175 U.S. 677, 708-09 (1900).

72. *Id.* at 686.

73. See JANIS, *supra* note 65, at 39-40.



issue at hand. Such resolutions are not directly legally binding, but they may form evidence of a nation's sense of moral obligation, which in turn is evidence that a custom has become, if not exactly legally binding, then "quasi-binding" as a kind of "soft" customary international law. These in turn may gradually acquire the status of "hard" law and become actually binding.<sup>74</sup>

Another earmark of enforceable custom of greater relevance to a "law of cyberspace," however, is the writings of scholars. "Much of the work of discerning and developing customary international law is done . . . by scholars in researching and writing legal doctrine."<sup>75</sup> An especially strong form of evidence of custom is the publication, whether by an individual scholar or a nation's government, of a digest of customary international practice.<sup>76</sup> Closely related to reliance on scholarly writings to ascertain international customs is a reliance on model codes and recommendations by various international bodies. Resolutions of the United Nations and reports from the U.N.'s International Law Commission can be influential in court decisions.<sup>77</sup>

A reliance on customary law has its drawbacks, of course, including the potential for nations' to disagree on what a "custom" is, how it applies to a given factual circumstance, and the problem of strategic behavior—a nation behaving in a certain way precisely for the purpose of trying to "create" a custom.<sup>78</sup> But the remarkable thing for our purposes is that despite these complications, and the murkiness of the philosophical question of what is "law," the basic principle remains that practices developed by parties themselves can eventually rise to the level of enforceable, that is, judicially recognizable, rules of behavior without ever being codified by a legislative body.

These contemporary international practices, like the Medieval Law Merchant, have obvious relevance to a developing law of cyberspace. First, they have direct relevance in that more and more international dealings will take place over computer networks; presumably existing international rules and customs will apply to these dealings whenever appropriate. Second, unique customs will certainly develop in cyberspace. The history of international customary law suggests that

---

74. *Id.* at 43-44 (citing Bernhardt, *Customary International Law*, 7 ENCY. PUB. INTL. L. 61, 62 (1984) and Seidl-Hohenveldern, *International Economic 'Soft Law'*, 163 HAGUE RECUEIL 165, 194-213 (1979)).

75. JANIS, *supra* note 65, at 48.

76. *Id.* at 42-43.

77. *Id.* at 43-45.

78. *Id.* at 46.

when sufficiently developed and widely adhered to, these customs will acquire the force of law, even in the absence of positive enactment by a sovereign.

#### IV. WHAT TYPES OF RULES WORK BEST?

Part II identified an illustrative list of cyberspace legal issues that merit further attention, and tried to understand why these issues and not others raise new questions. Part III discussed a number of ways in which rules for regulating behavior can arise, many of them from the “bottom up” by the affected individuals themselves rather than being issued “top down” by a court or legislature. Part IV will address the question of which of the ways for regulating behavior in cyberspace are most appropriately relied on for a number of the problem areas already identified. Clearly when there is a sovereign with authority, a statute can address almost any problem. Yet statutes are not always necessary—there are occasions when “live and let live” is a useful rule. How do we determine when a “top down” rule such as a statute is best, and when a “bottom up” rule such as private contract or no rule at all, is best?

The key to answering this question is the recognition that the technology of computer communications is rapidly changing. The number of people using cyberspace, and the number and variety of services being offered on-line, are both growing with astonishing rapidity. In the face of this very dynamic situation, we ought to be reluctant to impose behavior control that is inflexible and uniform beyond the needs of the situation. As a general matter, the most flexible rules are those that are issued at the “lowest” possible level: bottom up rules like those embodied in contracts or the rule of “live and let live” can be changed more easily by their makers than statutes or judicial precedents.

One factor that suggests the avoidance of self-help or contractual solutions is the existence of externalities. When unilateral or bilateral measures significantly harm third parties, the justification for top-down rules such as statutes to minimize harmful effects is strong. Yet even here one should be cautious in turning to centralized rule-making, for rapidly changing technology is likely to change the notion of what is or is not an “externality” in a given transaction. For example, a number of organizations have felt at liberty to subscribe to a single newsletter, which they then reproduce for individual members of the organiza-

tion.<sup>79</sup> Whatever effect this reproduction has on the newsletter's copyright holder is an externality with regard to that holder. But this externality is only a function of the fact that currently it is desirable to circulate newsletters in paper form. Suppose a future technology makes access through an on-line BBS both the cheapest and most desirable method of access? Suppose further that on-line access can technically be arranged so that downloading or copying from the computer's screen is not possible. Then we would have a situation in which the advantages of paper reproduction had diminished and the replacement technology would not be accompanied by harmful externalities.

All the foregoing observations in turn lead to a clear policy that when a "new" problem is identified in cyberspace, we should initially respond with the lowest, most decentralized level of control possible. After all, a problem that can be worked out satisfactorily between two people neither requires nor benefits from the adoption of a federal statute, let alone a multi-lateral international treaty. It makes sense, therefore, to start with the presumption that the lowest level of resolution can solve control problems, working "upward" in control mechanisms from there as necessary.

This section therefore begins with pure self-help remedies, which are appropriate for a limited class of problems. The remainder of the section discusses contractual approaches to behavior regulation, which can work well in quite a variety of cyberspace circumstances. After a review of contractual solutions, the appropriateness of cyberspace customs as a regulatory mechanism will be addressed. Finally, this section will analyze some specific problem areas not already addressed in the previous discussion.

#### *A. Pure Self-Help*

The most modest response to a new problem in cyberspace is for the legal system to do nothing whatever. In some situations, that response will prove perfectly fine as a regulatory mechanism. Situations appropriate for self-help are characterized by a lack of externalities, and the presence of a wide range of choices for the "consumer" of cyberspace services.

For example, cyberspace users often participate in discussion

---

79. See *Television Digest Inc. v. United States Tel. Ass'n*, 28 U.S.P.Q.2d (BNA) 1697; 21 Media L. Rep. (BNA) 2211 (D.D.C. 1993); *Pasha Publications, Inc. v. Enmark Gas Corp.*, 22 U.S.P.Q.2d (BNA) 1076; *Copyright L. Rep. (CCH)* ¶ 26,881; 19 Media L. Rep. (BNA) 2062 (N.D. Tex. 1992).

groups called "listservs" or "newsgroups." These groups occasionally feature acrimonious commentary that some recipients will find offensive. An obvious solution for those who are offended is to exercise self-help by withdrawing from participation in the discussion group and finding or starting another group. There are probably thousands of existing groups that may be joined, and the requirements for starting a discussion group on many networks, both the Internet and the private desktop networks, are modest and low in cost. This "solution" is, of course, the preferred one under First Amendment law generally as it avoids government intervention into the exercise of free speech rights; it is not suggested that the cyberspace problem is different—merely that for the legal system to "do nothing" is sometimes the best solution in both real and cyberspace.

For another example, advertisements on the current Internet computer network are not common because of that network's not-for-profit origins.<sup>80</sup> Today, when someone does put out an e-mail message on the Internet that is an advertisement, it is often greeted with vigorous objections by others and assertions that the objectors will avoid the advertised products assiduously.<sup>81</sup> This is unilateral self help at its best.

The issue of pornography is similar but a bit more complicated.<sup>82</sup> At first blush, many users of cyberspace would no doubt make the same claim about pornographic materials as is made about abrasive debate: do not look at what you do not want to be exposed to; supervise your children so they do not look; pornography is just a matter of contract if you want it (willing buyers and willing sellers abound in this market), and unilateral self-help if you do not.

The difficulty in identifying self-help as the appropriate level of remedy here is that there is wide-spread disagreement over whether pornography is really just a contract matter without externalities or whether it has significant externalities. The latter view holds that por-

---

80. Advertising on the Internet may soon become a problem. After this article was completed, the author learned of a controversial advertising message over the Internet from a law firm indirectly seeking clients with questions about immigration law. The controversy centered on the fact that the message apparently went literally to millions of Internet users. It seems likely that this use of the network as a mass medium for advertising will increase in the future.

81. See John Burgess, *On The Internet, Frontier Justice*, WASH. POST, Feb. 28, 1994, Bus. Sec. Supp., at 19, 25.

82. To the extent that one believes acrimonious debate to have externalities, of the sort that "hate speech" codes are designed to prevent, then that situation becomes similar to that of pornography and equally intractable.

nography affects the moral tenor and perhaps even the physical safety of the entire community, particularly women.<sup>83</sup>

For those who believe that pornography has no significant externalities, self-help is clearly the preferred solution as it is the least intrusive and most flexible (one can change one's mind about it). For those who believe that pornography has significant externalities, the externalities are usually thought to affect large groups ("women," the "community," etc.). With wide-ranging and pervasive externalities, self-help remedies are inappropriate, leaving a statutory response as likely to be the only effective remedy.

The matter of pornography's external effects is thus highly dependent on one's personal views and is not amenable to solution here. Perhaps the best that can be hoped for in this context is that courts handling prosecutions under anti-obscenity laws will have some sense that a cyberspace "community" may be quite different from a real space community with which it intersects. System administrators can perform a limited amount of self-help in this context by clearly identifying their materials and taking steps to screen out minors from access. It might make sense for the cyberspace community (or communities) to set standards for itself in the form of customs as discussed more fully below.<sup>84</sup> Self classification of BBSs not unlike that of motion pictures (X, R, G, etc.) might help suggest that such communities are well established and worthy of judicial recognition.

### *B. Contract Approaches*

Simply withdrawing from participation in a cyberspace activity is not always the best solution, of course. It may be that all affected parties would be better off if, rather than never dealing again with one another, they instead reached agreement about limits and obligations on their own behavior with respect to one another. They can make their transactions better, in other words, by forming contracts, which is a step up from pure self-help in the scale of remedies from most decentralized to most centralized.

In the case of acrimonious debate, for example, if the discussion is held on a private BBS in cyberspace, the system administrator can gauge the relative desirability of censoring discussions and offer con-

---

83. For an objective discussion of externalities of pornography, see RICHARD A. POSNER, *SEX AND REASON* 366-74 (1992).

84. See *infra* text accompanying notes 106-20.

tractual commitments to censor or not, as seems most desirable to most participants. Naturally, some systems would feature a great deal of such control, and others none at all. That is a good outcome because it allows people with different thresholds of tolerance for acrimony to seek out the system that matches that threshold.

Can we identify in general the situations in cyberspace for which contracts are an appropriate response? We know that parties who deal with each other in regard to transactions that have high value to the participants, relative to the costs of the transaction, can be expected to form their own contracts. The Coase theorem,<sup>85</sup> moreover, tells us that in such circumstances, the parties will reach an economically efficient result. In the absence of some compelling contrary social policy or significant detrimental effects to parties external to the contract, then, there is good reason to allow parties in cyberspace to form their own contracts to their own mutual agreement.

We have seen that a great many of the new problems of cyberspace revolve around the role of the system administrator. The presence of a system administrator as a service intermediary also means in most cases that a user of the system administrator's BBS must gain some sort of entry "permission" in the form of an account for or subscription to the BBS. This entry point situation suggests the presence of low transaction costs because the parties must already enter a transaction of some sort for the user to gain access to the BBS. In addition to low transaction costs, we have the wide variability among BBSs and the range of system administrator roles, from active to inactive, in the flow of messages through their systems suggesting that a uniform statutory approach to control will be far less than optimal. Under these facts the appropriate rights and duties should be defined in the most decentralized way, again arguing for a contracts approach.

Contracts between users and system administrators also appear, at least with a first-cut analysis, to have few if any external effects. There is no pollution of surrounding users' property from the use of a BBS; no increase in accident costs to others; no (presently known) danger to the public's health generally; and so on. We should therefore start with a presumption that contracts will arise to resolve whatever conflicts and disputes may occur in regard to the use of BBS services.

In fact, contracts already form the bedrock control mechanism with privately supplied BBS services. For example, access to Prodigy,

---

85. Ronald H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1 (1960).

Compuserve, America OnLine, the Well, Genie, Lexis Counsel Connect, as well as the countless small desktop BBSs run by hobbyists, is already subject to contractual agreements. Users must go through some form of initial "sign-on" procedure, whether on-line or by a paper transaction, by which they identify themselves, agree to make payments (for those BBSs that charge an access fee), agree to abide by whatever rules the system administrator imposes, and so on. At that point of entry the controlling system administrator can require adherence to a contract that specifies "legal" and "illegal" behavior.

Universities, most of which are connected to the Internet, could incorporate such rules in any faculty employment contract. Typically, such a set of rules would be included in a "faculty handbook," which would list a variety of university policies and requirements and could therefore readily incorporate guidelines and policies for use of the Internet or other networks. Students similarly agree to abide by certain university rules, which could easily include rules regarding appropriate cyberspace behavior.<sup>86</sup>

Let us take an example of something that is commonplace in cyberspace and see whether a contractual solution could be used for its resolution. A very typical cyberspace service is electronic mail. Besides reading and writing e-mail, many BBS users also rely on the ease of copying already-digitized messages to forward copies of such messages to others who might find them of interest.

Written messages, even if electronic, are copyrighted.<sup>87</sup> Users who forward others' messages are, in short, reproducing and distributing copyrighted material in violation of the copyright laws. One could argue that the copyright statute should be changed to accommodate this practice, but that is a very centralized and drastic solution. After all, some individuals may prefer not to have their electronic writing fall outside the scope of copyright protection; a statute would sweep them together with those who preferred otherwise.

The contract solution, in contrast, can work here; it already does on at least one commercial BBS, the Lexis Counsel Connect service which is a large BBS service for lawyers. Subscribers to this service sign an initial contract whereby they grant the right of reproduction of

---

86. My university has few rules, but certain behavior relating to unauthorized access is prohibited, as well as certain game playing activities.

87. Any work of authorship is copyrighted as soon as it is fixed in a tangible medium of expression. 17 U.S.C. § 102 (1988 & Supp. IV 1993).

their messages to others.<sup>88</sup> By clarifying copyright issues ahead of time, the contract resolves the tension between frequent practice and copyright law.

This contractual outcome in effect reverses the presumption of the copyright statute, but without the global effects of a statutory reversal. Moreover, users who object to this regime can exercise unilateral self-help by choosing not to become Counsel Connect subscribers, by arguing with the management to change the rule, or by setting up a competing service with the opposite presumption. In short, the contract solution here is decentralized because it applies only to Lexis Counsel Connect and its subscribers, and that seems appropriate.

The problems become more complicated when we consider that messages originally left on one BBS may be copied and distributed to other BBSs. What if other BBSs have different contractual presumptions? On closer inspection, the problem is no different from the single-BBS example, for if users of one BBS copy messages onto another BBS then they can also be governed by the first BBSs contracts. Such a contract might state, for example, that users consent to waive copyright in their messages, or perhaps waive it to the extent of noncommercial reproduction,<sup>89</sup> whether on the BBS in question or other services. This again would resolve issues of broader message distribution without need of statutes or other relatively more inflexible rules.

It would even be possible, with the low cost of communications in cyberspace, for a large number of system administrators to create a set of "by-laws" that would guide system administrator behavior. Recall that by-laws may be viewed as a contract among the members of a private association, a contract designed to outlast any particular transaction between any particular set of parties. Here such a contract would be a way to "codify" custom. If a substantial number of system administrators around the world reached agreement on basic customs

---

88. The contract specifies that:

members who submit material shall be deemed to (i) grant to [Counsel Connect] and subscribers to the system a paid up, perpetual, world-wide irrevocable license to use, copy and redistribute such materials and any portions thereof and any derivative works therefrom and (ii) warrant that such submitting member has all rights necessary to submit such material and that the use of such material by [Counsel Connect] and subscribers to the system will not infringe any other party's rights.

Counsel Connect Contract: Counsel Connect Rules § II (Aug. 1993) (copy on file with the *University of Pittsburgh Law Review*).

89. With the "noncommercial" limitation there would naturally arise occasional disputes over what was "noncommercial," but these are the sorts of disputes that always occur at the margin of any rule.



and practices in cyberspace, they could provide an effective discipline for users and other system administrators who violated the by-laws by expelling them from participation in affiliated BBSs. Courts would have good reason to defer to the result as long as the by-laws dealt only with the behavior of the contracting users and system administrators. Such a set of cyberspace "by-laws" might achieve the effectiveness of an international treaty without the official participation of the nation-states where the various systems reside.

### C. *Privacy in the Corporate Setting*

Let us now examine the question of an employer reading an employees' e-mail. It is apparent that the parties in question, employees and employers, are already in a contractual relationship, so that the additional transaction cost of bargaining over e-mail privacy will be quite low. There is also likely to be wide variation in the desires of different employers and employees for privacy. Employers in industries with serious risks of employee theft of trade secrets, for example, might put a high value on being able to monitor their employees' e-mail. Other employers may experience little or no threats to corporate well-being through their employees' e-mail and might have correspondingly little or no interest in monitoring. From the employees' perspective, the same variation will occur. Employees in some industries may value highly the certainty that their messages are not monitored; in other industries, the employees may be indifferent to this possibility.

At this writing, legislation has been introduced in Congress to address e-mail privacy in the work place by a uniform statute.<sup>90</sup> At least one commentator has also expressed the argument that employees ought to be granted a uniform right of privacy in their communications.<sup>91</sup> There are possibilities that state wiretap laws or state constitutional provisions about privacy may yet be held applicable to workplace privacy.<sup>92</sup> In Canada, government officials have issued calls for legislation protecting privacy.<sup>93</sup> There is no shortage, in other words, of pro-

---

90. S. 984, *supra* note 39; H.R. 1900, *supra* note 39.

91. See Steven Winters, Comment, *The New Privacy Interest: Electronic Mail in the Workplace*, 8 HIGH TECH. L.J. 197 (1993).

92. See *id.*; see also Julia Turner Baumhart, *The Employer's Right to Read Employee E-Mail: Protecting Property or Personal Prying?*, 8 THE LAB. LAW. 923, 943-47 (1992).

93. The Commissioner of the Ontario, Canada Information and Privacy Commission has recently called for the adoption of privacy "principles" for electronic mail. See TOM WRIGHT, COMMISSIONER, PRIVACY PROTECTION PRINCIPLES FOR ELECTRONIC MAIL SYSTEMS (1994) (on file with the *University of Pittsburgh Law Review*).

posals and possibilities for something other than a contract solution to workplace e-mail privacy.

Nevertheless, the low transaction costs that follow from the existing contractual relationship and the wide variation in desires for privacy by both employers and employees in the employment setting—not to say the rapid technological changes that make it hard to know what “e-mail in the workplace” will look like in only a few years’ time—show that a uniform statutory response for all industries is very much inappropriate here. To the contrary, the situation has all the hallmarks of one that is suitable for the flexibility of contractual resolution.<sup>94</sup> Such a resolution would likely take the form of a corporate policy about e-mail, delivered to all employees. Guidelines for just such policies are already readily available,<sup>95</sup> suggesting that the contract approach is in fact being implemented.

#### *D. Transaction Costs*

We have seen how contracts often meet the test of an appropriate behavior control in cyberspace, but they will not always do so with equal ease. They will prove less practical, in the most general sense, when contract transaction costs are great relative to the value of the agreement desired, or there are serious externalities to the contracting parties. For example, the more people who are affected by a cyberspace problem, the harder it will be for them to come to agreement, making some form of non-contractual arrangement, such as a statute, more appropriate.

We have been looking at contractual relationships between a system administrator and a BBS’s users. Contracts made as a requirement of “entry” are appropriate for a number of behavior controls. It is possible for an authorized subscriber of a BBS to do more than just access that one BBS. In the world of universities connected to the Internet communications network, it is possible for a user to access a first BBS, say a student’s own university computer, as a base for an attempt to make an unauthorized access to another BBS, typically at another university.

---

94. Readers who think that “unequal bargaining strength” is a significant factor in the analysis of contract relationships may disagree with this conclusion.

95. See DAVID R. JOHNSON & JOHN PODESTA, ACCESS TO AND USE AND DISCLOSURE OF ELECTRONIC MAIL ON COMPANY COMPUTER SYSTEMS: A TOOLKIT FOR FORMULATING YOUR COMPANY’S POLICY (1991). This booklet is published by the Electronic Mail Association, 1655 N. Fort Myer Drive, Suite 850, Arlington, VA 22209.

Here we have an example of a contract "externality" in cyberspace: the parties to the contract, the home university and the student, may reach agreement on terms, but the non-contracting university or BBS is affected by the access attempts. Even if the original university's contract with the student specifies that such attempted access is forbidden, the contracting university has little incentive to pursue disciplinary measures against the student who violates the agreement because it is another university that suffers the harm.

This is not idle speculation; in one instance of which the author is aware,<sup>96</sup> a university experienced attempts by someone to gain access to the university's computing facilities. The individual in question was not local to the university, but was evidently a student obtaining access from another university. When the university that experienced the attempted access approached the other university about the possibility of their controlling the student's conduct, the other university was uninterested: no harm had been done, and no attempt had been made to break into that university's facilities, and that was that.

A similar problem of apparent externalities occurs when BBSs serve as temporary repositories of electronic mail. A great deal of mail, whether over the Internet or the loose confederations of desktop BBS systems known as "FidoNet" and other networks, travels through a great many "host" systems which hold the mail for a time, then forward it to another such system. In FidoNet, for example, most of the mail is carried at night when long distance telephone rates are lower. A given message may therefore take several days to travel from originator to sender, and in that time may pass through dozens of separate BBSs.

Is there any requirement that a BBS properly forward the mail that is routed to it? Here we are dealing with a cyberspace service, electronic mail, that is at a different level from the previous user-to-BBS example. Instead, we are dealing with a set of BBSs that must cooperate in order to provide wide routing of users' mail from the whole collection of BBSs.

The lowest level solution for both attempted break-ins from remote sites and for the forwarding of mail is still contract, but it would require a substantial number of contracting parties. With the FidoNet network of desktop BBSs, for example, each desktop BBS that wants to

---

96. I have discussed the matter with a member of the affected university's computer center but chose not to disclose the university's name, other than to say that the event did not happen at my own university. No doubt countless other incidents like this take place every day; this is simply one incident about which I have direct information.

join the network must make an application and agree to certain terms. When any university wants to join the Internet, it also makes arrangements with other parties, though the Internet is far more decentralized than even the desktop BBS networks. This "point of entry" would therefore be the logical place to find agreements about obligations with regard to mail, remote break-ins and the like.

In fact, after writing the description of the user attempting a remote break-in and the issue of forwarding mail on FidoNet, and determining that a contract solution was still a possibility, this author set out to determine whether such a solution had been attempted for either the Internet or FidoNet.<sup>97</sup> With FidoNet, for example, probably the oldest such network of desktop BBSs, the founders of the network have developed a "policy" statement that is essentially the by-laws of a private association.<sup>98</sup> A hierarchy of services is specified, with managers at various levels in the hierarchy being assigned the power to discipline system administrators who fail to comply with the policy. Among the policies is a series of specifications about forwarding mail and what the system administrator should do when mail cannot be forwarded through the network.<sup>99</sup> As might be expected, the ultimate sanction for failure to comply with the policy is exclusion from the network.<sup>100</sup>

In addition, although universities on the Internet have a much less formal set of policies than FidoNet, there does nonetheless exist a kind of summary of customary practice on the network.<sup>101</sup> Little is said in this summary about the requirement of forwarding mail, but there are definite requirements for network managers to read their mail and be available to others to help diagnose network problems and to take action on security problems. There is even a provision addressing the problem of remote access: "it is important for managers to be willing to accept and act on *other sites' security issues*, warning or denying ac-

---

97. I really did do things in the sequence described: I first wrote a description of the problem, then looked to see if a contractual solution had been tried.

98. The most recent copy available to me is FidoNet POLICY4 (June 8, 1989) (on file with the *University of Pittsburgh Law Review*).

99. See generally *id.* at §§ 2 and 4.2.

100. *Id.* (prescribing expulsion from the net as one sanction for "excessively annoying behavior," and describing expulsion as "excommunication."). See also *id.* at § 2.1.12 (defining "excommunication"); § 1.3.5 (defining "excessively annoying"), §§ 4.3, 5.2 (authorizing various levels of the net's hierarchy to discipline others); and § 9 (defining grievance procedures and disciplinary action).

101. See Memorandum from J. Van Bokkelen, *Responsibilities of Host and Network Managers: A Summary of the "Oral Tradition" of the Internet* (Aug. 1990) (on file with the *University of Pittsburgh Law Review*).

cess to offending users.”<sup>102</sup> Host systems are even advised not to have “open access” accounts because with such accounts, it is impossible to deny access to an offending user.<sup>103</sup>

Two observations can be made here. One is that despite the presence of many parties and apparently high transaction costs, contract solutions or at least contract mitigations of problems may yet be feasible. If a large enough group can cooperate, then otherwise external problems become once again internalized. Second, it seems clear that really large networks of contracting users may find it hard to monitor the users as closely for enforcement purposes as they might desire. The sole available sanction of denial of access to the network<sup>104</sup> may not be serious enough to curtail all the problems that one would wish to control. Some network sites might refuse to abide by the rules, particularly if they do not themselves have facilities that appear to offer interesting files or accounts to be “hacked” undetected. In addition, the willingness of different network sites to monitor and punish the prohibited conduct according to the by-laws may be substantially unequal.

Thus, these problems seem on the margin of requiring more than contractual agreements. It is not surprising, therefore, that statutes exist that attempt to control at least the worst of these problems, the unauthorized access attempts.<sup>105</sup>

### *E. Custom*

Like a reliance on contracts for control of cyberspace behavior, a reliance on custom works well in some circumstances, less well in others. We must address two basic issues with regard to custom in cyberspace: how does a court know when a custom is well-established; and what are the circumstances that prompt a court to follow (or ignore) a concededly well-established custom.

On the matter of establishing a custom, expert testimony will of

---

102. *Id.* at 4.

103. *Id.* at 4-5.

104. The Internet summary of practices specifies that the “solution of last resort [is] ostracism of the offending net.” *Id.* at 4.

105. Some of the problems of intercepting e-mail specifically are dealt with in the federal Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C.) [hereinafter ECPA]. At least 48 states have some sort of law about “computer crime,” including prohibitions on “unauthorized access to a computer, computer trespass, computer tampering, computer hacking, unauthorized use of a computer, and alteration or damage to computer data or software.” RAYMOND T. NIMMER, *THE LAW OF COMPUTER TECHNOLOGY* ¶ 12.04 (2d ed. 1992) (footnotes omitted).

course be relevant. But the example of public international law shows that codifications of practices by scholars and others provide strong, persuasive evidence to courts.<sup>106</sup> Private international law involving business contracts is also heavily influenced by model codes and guides. The International Chamber of Commerce, for example, is a non-governmental organization that over the years has produced definitions of terms used in international business transactions that are widely adhered to and incorporated into international contracts.<sup>107</sup>

Consequently, an important task for those who care about the development of law in cyberspace will be to devise model codes, guides to good practice, and the like. At this very early stage in the legal history of cyberspace, such codes and guides should prove extremely influential in future legal disputes. A logical approach to the creation of such guides would be to rely on a voluntary task force or committee formed in cyberspace and that solicited wide input through the same medium. Voluntarily adopted customs can also be enforced through private arbitration. Private commercial arbitration provided by the International Chamber of Commerce has been influential in developing a modern-day "Law Merchant,"<sup>108</sup> so that precedent for cyberspace arbitration already exists.

The second basic question with regard to custom is, when do courts follow a custom and when do they ignore it? Richard Posner has suggested a clear distinction here: courts tend to defer to custom when the plaintiff and defendant were already in a contractual relationship, and to pay less attention to custom otherwise.<sup>109</sup> This makes sense, according to Posner, because the custom surrounding a contractual arrangement is likely to be mutually beneficial—else it would have been altered by contract. The custom of an industry with regard to those not in a contractual relationship, however, is another example of an externality. There is no particular reason to suppose that an industry custom endangering by-standers should receive deference; indeed, imposing liability when a defendant follows such a custom is precisely what is needed to internalize the otherwise external costs of the custom.

A number of cases support this distinction. The strongest example

---

106. See *supra* text accompanying notes 75-76.

107. See INTERNATIONAL CHAMBER OF COMMERCE, INCOTERMS 1953 (1974 ed.), cited in JANIS, *supra* note 65, at 203 n.16.

108. See W. LAWRENCE CRAIG ET AL., J. PAULSSON, INTERNATIONAL CHAMBER OF COMMERCE ARBITRATION § 35.01 (2d ed. 1990), cited in JANIS, *supra* note 65, at 202.

109. See RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 229-45 (3d ed. 1986).

of judicial deference to custom occurs in professional specialization cases, typified by medical malpractice cases. Plaintiffs must establish that the defendant practitioner failed to meet the standard of customary medical care.<sup>110</sup> Disputes turn on the establishment of the proper custom under the circumstances—not on whether the custom, once proved, should be followed. Medical cases, of course, involve parties who are in a contractual relationship.

Contrary examples, where courts are least deferential to industry custom, can be found in the products liability area. Note that consumers and by-standers are not in a contractual relationship with manufacturers—that was the problem of the “lack of privity” limitation applied in products cases.<sup>111</sup> Industry custom is relevant in these products cases, but it receives less deference than in medical cases.<sup>112</sup>

Interestingly, the two most famous examples of courts not deferring to industry custom in the face of a contractual relationship, *The T.J. Hooper*<sup>113</sup> and *Helling v. Carey*,<sup>114</sup> were probably just the opposite from what they appear to be. *The T.J. Hooper* involved a tugboat that failed to have a radio on board that would have warned the crew of an impending storm and saved the tug’s tow. Hand assumed that even if the lack of a radio was customary in the tug industry, the defendant would be held liable anyway, noting in regard to the weight to be given custom that “Courts must in the end say what [standard of care] is required.”<sup>115</sup> *Helling* involved an ophthalmologist who had failed to give a routine glaucoma exam to an asymptomatic patient who later developed glaucoma. The Washington Supreme Court held the physician liable despite what it determined to be the custom of ophthalmologists not to perform such tests.<sup>116</sup>

Both cases dealt with parties in a contractual relationship, which suggests that the court should have deferred to the industry custom. Consistent with Posner’s view, however, it appears that in both cases

---

110. For medical professionals, “the standard of conduct [is] one of ‘good medical practice,’ which is to say, what is customary and usual in the profession.” W. PAGE KEETON ET AL., *PROSSER AND KEETON ON THE LAW OF TORTS* 189 (5th ed. 1984).

111. See *Winterbottom v. Wright*, 152 Eng. Rep. 402, 403 (Ex. 1842); *MacPherson v. Buick Motor Co.*, 111 N.E. 1050, 1053 (N.Y. 1916).

112. “[R]ecent [products] cases . . . allow the jury to impose liability upon a defendant who has complied with all statutes and common practice . . . .” RICHARD A. EPSTEIN, *MODERN PRODUCTS LIABILITY LAW* 77.

113. 60 F.2d 737 (2d Cir.) (Hand, J.), *cert. denied*, 287 U.S. 662 (1932).

114. 519 P.2d 981 (Wash. 1974).

115. *The T.J. Hooper*, 60 F.2d at 740.

116. *Helling*, 519 P.2d at 982-83.

the courts misunderstood the actual custom, which supported rather than contradicted the decisions. Despite Hand's assertions, carrying radios was apparently a widespread tugboat custom;<sup>117</sup> medical treatises of the *Helling* time period apparently recommended that ophthalmologists give exactly the sort of routine glaucoma exam that defendants in that case failed to give.<sup>118</sup>

There seems to be some predictive value, then, in Posner's observations about custom. How would those observations play out in cyberspace? Many of the contractual relationships described earlier, such as that between user and system administrator, or among system administrators in a private association arrangement (e.g., the members of a computer network) will eventually give rise to disputes about which the contract is silent. In these cases, if there is a clear custom, then courts can be expected to defer to the custom.

Suppose, for example, that it becomes customary for system administrators to retain messages left on their BBS systems for no more than thirty days, though this fact is not expressly communicated to the BBS's users. Suppose further that a particular BBS features retail buying and selling activities well known to the system administrator. A BBS user posts a message that involves an offer of contract or an acceptance of a contract offer, for a specific recipient. The intended recipient of this message does not pick up her mail for over thirty days and the system administrator's automated mail clean-up program deletes the message. The recipient later learns of this situation and has lost money as a result. Thereafter, she sues the system administrator.

Let us assume that the system administrator is sufficiently familiar with the types of messages exchanged on the BBS that the *Hadley v. Baxendale*<sup>119</sup> rule on consequential damages is not a limitation on liability. Should the court defer to the custom of over-thirty day deletion of messages? In a word, yes. Here the parties are in a contractual relationship, there are no significant externalities, and no strong public policy cutting in either direction. There is every reason for a court to use

---

117. There was testimony in the trial court that "90 per cent of the coastwise tugs operating along the coast were . . . equipped" with radios. *The T.J. Hooper*, 53 F.2d 107, 111 (S.D.N.Y. 1931), *aff'd*, 60 F.2d 737 (2d Cir.) (Hand. J.), *cert. denied*, 287 U.S. 662 (1932).

118. RICHARD POSNER, *TORT LAW: CASES AND ECONOMIC ANALYSIS* 288 n.1 (1982) (quoting B. BECKER & R.N. SHAFFER, *DIAGNOSIS AND THERAPY OF THE GLAUCOMAS* 183 (2d ed. 1961)) and other treatises.

119. 156 Eng. Rep. 145, 151 (1854).



the industry custom to fill in the contract gaps between user and system administrator with an implied thirty-day-delete term.<sup>120</sup>

To take a contrary example, suppose it becomes customary for cyberspace users freely to forward copies of computer software to a wide audience. Perhaps the custom has become solidly entrenched with regard to public domain and "shareware" computer programs, with those not desiring such free distribution prominently labelling their software accordingly. A particular user finds a piece of software to be especially helpful, and following the custom, forwards copies to several others. Unfortunately, the author of this program has not authorized such distribution, but has failed to restrict it explicitly as the custom dictates. Should the court defer to the well-established custom of wide distribution in the absence of explicit restrictions? Plainly not. If the affected party, the author and copyright holder of the program, is not in a contractual relationship with those who distributed or received the software, there should be no presumption that the custom will be mutually beneficial to all affected parties and no reason to defer to it.

#### *F. Defining "Reasonableness" Through Custom*

In general negligence actions, the notion of "reasonableness" often plays a crucial part. We have seen already how many possible cyberspace disputes, such as the theft of financial records and the obligation to disclose the theft, will likely turn on the reasonableness of the defendant's actions. Similarly, issues surrounding a system administrator's obligation to label files accurately are likely to turn on the reasonableness of the system administrator's behavior. Given that there is little basis for a court or jury today to know what in cyberspace is "reasonable" and what is not, there is a great deal that cyberspace users can do to establish a basis for the determination of reasonableness.

First of all, in garden variety negligence cases what is "reasonable" is often what is "customary." Thus, all that has been said earlier about customs in cyberspace applies to the negligence context as well.

---

120. See *supra* text accompanying notes 58-65 for the example of established commercial customs overriding other, more general, law from the Law Merchant. However, instances are not confined to Medieval times. See, e.g., *Ghen v. Rich*, 8 F. 159 (D. Mass. 1881) (whaling); *Titus v. Bradford, B. & K. R. Co.*, 20 A. 517 (Pa. 1890) (railroads); *E. Clemens Horst Co. v. Biddell Bros.*, 1912 App. Cas. 18, 22-23 (H.L. 1912) (shipping); *Sledd v. Washington Metropolitan Area Transit Auth.*, 439 A.2d 464, 468 (D.C. 1981) (subways); but cf. *Mayhew v. Sullivan Mining Co.*, 76 Me. 100 (Me. 1884) (mining).

That is, custom can be a source of judicially recognized affirmative obligations, as with the Law Merchant and with public international law, but custom can also be an indirect way of establishing what conduct in cyberspace is considered "reasonable."

In short, though reasonableness may be ultimately determined by a court, the cyberspace community can do much to influence that ultimate determination. Among other things, just as was true with the establishment of cyberspace customs, that community can help establish reasonableness by developing codes of conduct and guides to "best practices" to which various users can voluntarily adhere. System administrators, for example, could form system administrator model codes that specify obligations regarding the accurate labelling of files. Courts often give considerable credence to such codes.<sup>121</sup>

Such codes might also specify conduct relative to the forwarding of messages. If a model code of behavior required that all messages destined for other BBS's users be forwarded without screening, for example, perhaps a court's incentive to find system administrators liable for forwarding without screening would be reduced.

#### *G. Must System Administrators Read the Mail?*

Having reviewed the differing levels of behavior regulation that might apply in cyberspace, we can now examine the remaining cyberspace problems, identified earlier in this article, to see whether a self-help, contractual, or other solution can best resolve any difficulty. The first problem is that of the user who uploads a message or file to a BBS that is "wrongful"—that is, the message is defamatory or copyright infringing or privacy invading, etc. Should the system administrator be liable for any harm that results? We are essentially asking whether system administrators have a duty to examine and review the materials deposited on or flowing through their systems, and more specifically, asking what is the most decentralized approach to resolving the issue. Let us start with defamatory messages.

The first recourse of a defamed plaintiff might be unilateral self-help. If we assume that access to cyberspace will be low cost for all who want it—comparable, say, to telephone access today—then the defamed plaintiff has an immediate and effective way to rebut defamatory statements: answer them through cyberspace communications, the

---

121. See generally John M. Winters, *The Evidentiary Value of Defendant's Safety Rules in a Negligence Action*, 38 NEB. L. REV. 906 (1959).

same medium in which they were originally published. Technology in this instance gives the plaintiff a guaranteed access to the relevant "media" for a reply. This access may have the unintended by-product of turning every libel plaintiff into a public figure<sup>122</sup> under court precedents emphasizing that "public figures" are those who have "ready access . . . to mass media of communication . . . to counter criticism of their views and activities."<sup>123</sup> With comparable rights by defendants and plaintiffs to make and reply to libels, the argument to immunize the system administrator and leave the whole defamation matter to unilateral self-help solutions is strong.

If pure self-help is not sufficient—it may not be for all defamations and it will not be for copyright infringement or trade secret theft—then what is next? The variation in system sizes of BBSs and the relative unfamiliarity of courts with the role of the system administrator continue to argue for a flexible solution, suggesting a contract approach. The difficulty here is that a BBS user's behavior with regard to third parties is a clear externality. A contract between user and system administrator may prohibit wrongful messages, but what happens if a user violates the contract, uploads a defamatory or infringing text or image, and it is downloaded by others? Injured parties who are not in a contractual relationship with either the defendant or the system administrator are precisely the problem here.

The next "level up" for resolution would be to rely on a judicial decision or a statute fixing liability or providing immunity for the system administrator. Either a case-by-case resolution or a statute seem roughly equivalent here. Both would clarify the law, at the expense of its (necessarily) greater complexity. A judicial precedent might not be quite as predictable as a statute, but judicial decision-making retains a correspondingly greater flexibility compared to statutes; future cases in which the facts or policy concerns differed significantly can more easily lead to appropriately different results than is true with a statute.

With commercial BBS systems, one approach might be to immunize the system administrator from damages liability. After all, system administrators will want to maintain accurate records and deal with

---

122. The possibility that a ready reply by defamed plaintiffs might turn every cyberspace plaintiff into a public figure for libel law purposes was first suggested by Mike Godwin. Mike Godwin, *Libel, Public Figures, and the Net*, INTERNET WORLD, June 1994 (on file with the *University of Pittsburgh Law Review*).

123. *Curtis Publishing Co. v. Butts*, 388 U.S. 130, 164 (1967) (Warren, C.J., concurring). Access to the media is only one factor of several used by courts; for a discussion of those factors, see RODNEY A. SMOLLA, *LAW OF DEFAMATION* § 2.09[3] (1991).

solvent users or they cannot earn a profit. These records will provide injured plaintiffs with the ability to locate these solvent users and proceed directly against them. Moreover, large commercial systems will likely experience a volume of uploads that precludes, as a practical matter, screening of messages and files. An action directly against the wrongdoing party is thus appropriate, and is precisely what has happened in one case already,<sup>124</sup> where an injured party sued the uploader of an allegedly defamatory message to the Prodigy BBS service.

On the other hand, subscriptions to many large commercial BBS systems can be obtained for relatively small amounts of money, sometimes as little as ten to fifteen dollars a month.<sup>125</sup> Users paying this little cannot necessarily be equated with "solvent defendants" who would be able to respond in damages to defamed or infringed plaintiffs.

The availability of identifiable solvent defendants is even less certain with many small, desktop BBSs. Defendant users of such systems may not be identifiable or solvent because accurate identification is often not a requirement for such systems. Counterbalancing that concern is the fact that smaller systems will more likely be capable of the actual screening of uploaded messages and files. Yet, other BBS systems may not be able to screen due to high volume, but may be able to charge a substantial amount for access. Injured plaintiffs would almost certainly be able to locate a solvent defendant-user of such a BBS service if such a defendant engaged in uploading wrongful messages.

Once again, we are faced with a situation in which the relevant policies and circumstances vary substantially from one BBS to another. A uniform rule, whether judicial precedent or statute, would appear to be suboptimal in this case: it will be exactly right for some circumstances, and unnecessary or inappropriate for others. The ideal here would be some form of control that forces the different system administrators to make their own calculation of "safety" precautions. In other words, we would like system administrators with solvent defendants to ensure that those defendants are amenable to suit allowing the administrator to take fewer precautions against wrongful uploads. Other system administrators may lack solvent user defendants, but may find it feasible to screen uploaded material; we should encourage them to do so.

---

124. *Prodigy User Feels Vindicated After Libel Suit*, THE ATLANTA CONST., Dec. 30, 1993, at E2. The case was settled.

125. I have received advertisements with such offers from America OnLine and CompuServe.

Precisely because the variables of identifiable and solvent user population, the likelihood of wrongful communications, and the ability of system administrators to take precautionary measures, are so diverse, we need a behavioral control that will bring about the optimal result by forcing the relevant parties to determine the best precaution themselves, rather than having a court or legislature make it. This is exactly the result that is brought about by the imposition of strict liability on system administrators. In fact, one of the principle differences between negligence liability and strict liability is that strict liability removes the cost-benefit calculation from the court and imposes it on defendants.<sup>126</sup> Here that means that strict liability will force the system administrator of each BBS service to determine the most advantageous mix of preventative measures for that BBS, including the need to ensure user solvency, to perform message screening, to limit uploading, and so on.

This conclusion will doubtless run against the thinking of many interested in the legal questions of cyberspace. Yet, strict liability policies apply nicely in this context. Losses from wrongful messages can be spread over all users of the BBS service. If one of the costs of running an electronic messaging system is that wrongful messages will damage third parties, we would want the system to internalize those external costs to make the proper decisions about the scope of activity. In addition, there is some tendency in the law to hold new activities, whose safety is not well understood, to strict liability until more is known about them, and that fits well with the new communication services.<sup>127</sup>

Would strict liability also mean putting many BBSs out of business? It could, but only if system administrators themselves determined that the risk of liability exceeded the possibility of indemnification from their users or their ability to screen messages ahead of time. Those are exactly the circumstances under which injured plaintiffs would otherwise fail to obtain redress. Conversely, system administrators with highly solvent users can contractually shift liability to those users for the latter's own conduct through the mechanism of indemnification. Smaller BBS services may be able to screen messages and files in some instances (such as may have been the case with the photographs at issue in the *Playboy* case), though clearly not in all instances (such as

---

126. Richard A. Epstein, *A Theory of Strict Liability*, 2 J. LEG. STUD. 151, 188 (1973) (Under strict liability, "[t]here is no need to ask the hard question of which branch of government is best able to make cost-benefit determinations, because the matter is left in private hands.").

127. POSNER, *supra* note 109, at 163-64.

when a user uploads an image or text file that the system administrator would have no way of recognizing).

Even system administrators of services who are unable to shift liability in this fashion, and are unable as a practical matter to screen their messages and files, would not necessarily go out of business. The question is whether the benefits of the business, measured either in dollars received from users or satisfaction received by the system administrator for running the system, exceed the potential liability costs, discounted by their likelihood. If the benefits do exceed the costs, then the system administrator would take the risk, paying off judgments when necessary. Moreover, the smaller the BBS service, the less likely that even the system administrator will be an attractive target for suit—and as a practical matter, the small number of users of a small BBS make it less likely that wrongful messages will do wide-spread damage.

Implicit in this proposal to impose strict liability on system administrators is a crucial predicate. Administrators must be able to adjust liability between themselves and their users. That is, they must be able to contractually shift liability when they and their users determine that such a shift is cost effective. In the case of a BBS, the system administrator must be able to enforce any indemnification agreements entered into by BBS users. The beneficial effects of imposing strict liability on system administrators would be lost if courts in practice were to find indemnity or other liability-shifting agreements to be unconscionable or unenforceable because of unfair bargaining strength or for other reasons. Recall that the fundamental concern behind the imposition of such liability is not that system administrators “ought” to screen all messages or “ought” to bear all responsibility for their users’ message. Rather, it is that strict liability forces system administrators, rather than courts, to make the calculations of what conduct is worth undertaking.

A BBS administrator and the BBS’s users, for example, might mutually determine that a BBS messaging facility was desirable, but only feasible if each user bore his or her own liability for “wrongful” messages. An agreement that carried out that conclusion would therefore be beneficial to all parties. A court that did not uphold such a contractual agreement would force all similar BBSs to shut down—the wrong outcome from all parties’ perspectives.

In sum, in the case of wrongful messages uploaded by others, the imposition by courts of strict liability on the system administrator, coupled with enforceable indemnity agreements where made between ad-

ministrators and users, is the option that seems most appropriate. Will courts in fact apply strict liability to system administrators? Two impediments appear to stand in the way, the existence of the Electronic Communications and Privacy of Act 1986<sup>128</sup> ("ECPA"), and the Supreme Court's requirement<sup>129</sup> that strict liability not apply in defamation cases. The first will prove on closer examination not to prevent the imposition of such liability; the second will prevent it in defamation cases but not in other cases such as copyright.

The ECPA specifies that it is unlawful to intercept a private electronic communication sent over a public messaging system; if a system administrator were to read private e-mail intended for others, it appears that this would constitute the prohibited conduct of "intercepting an electronic communication."<sup>130</sup> Imposing liability, strict or otherwise, on system administrators for "wrongful" messages residing on their systems would in effect be imposing a duty on them to read messages and thus seems to create a conflict with the ECPA. But the ECPA is only a problem in regard to private messages: when messages or files are uploaded to "public" areas of a BBS for anyone to read or view, then, the ECPA will not be relevant. Thus, imposition of strict liability on system administrators for the content of public messages would not run afoul of the statute.

Even with private communications, however, imposition of liability—a duty to screen messages—may not be inconsistent with the ECPA's prohibition because of two exceptions. First, consent of the user is a defense to liability,<sup>131</sup> and there is some authority that reasonable expectations of privacy are imported into the question of consent.<sup>132</sup> Many system administrators of BBSs caution users not to expect privacy of e-mail messages; such a caution might function to relieve the administrator from ECPA liability under the "consent" and "reasonable expectations" exceptions, and hence would eliminate any conflict between that statute and other legal liability. Second, the ECPA also exempts the provider of an electronic communications service, which would include a BBS, from liability for intercepting com-

---

128. Pub. L. No. 99-508, 100 Stat. 1848 (codified in various sections of 18 U.S.C.).

129. See *Gertz v. Robert Welch, Inc.*, 418 U.S. 323 (1974).

130. "[A]ny person who . . . intentionally intercepts . . . any . . . electronic communication" is subject to liability. 18 U.S.C. § 2511(1)(a) (1988).

131. See *United States v. Barone*, 913 F.2d 46, 49 (2d Cir. 1990) (consent exception applies to criminal prosecutions); *Griggs-Ryan v. Smith*, 904 F.2d 112, 116-17 (1st Cir. 1990) (consent exception applies to civil suits).

132. See *United States v. Carroll*, 337 F. Supp. 1260, 1262-63 (D.D.C. 1971).

munications when the interception "is a necessary incident . . . to the protection of the rights . . . of the provider of that service."<sup>133</sup> If liability were imposed on a system administrator for wrongful messages, it would then become a necessary incident to the protection of the administrator's rights that the administrator read the e-mail passing through the system. The ECPA exception to liability would therefore apply and any conflict between strict liability and the ECPA would be eliminated.

Among the various kinds of wrongful messages that might appear on a BBS, defamatory messages raise an additional issue with regard to the system administrator's liability. The Supreme Court has made it clear that there are strong First Amendment underpinnings behind a scienter requirement for those who only transmit the libels of others.<sup>134</sup> The *Cubby* court noted these underpinnings,<sup>135</sup> though the case appears to have turned on the fact that the defamatory material carried on CompuServe was placed there by an independent contractor of another independent contractor of CompuServe.<sup>136</sup> For our purposes, the presence of an independent contractor means that other solvent defendants besides CompuServe were available for suit, lessening the pressure for a court to find the system administrator liable. A stronger argument for the administrator's liability would be made when no other solvent party was available as a defendant. But even here, barring an unlikely reversal of Supreme Court defamation precedents, holding a system administrator strictly liable for defamatory messages would not be possible because of those precedents. Copyright and trade secret cases do not wear the same First Amendment armor that defamation cases do. Placing strict liability on system administrators for wrongful messages of those types is therefore an appropriate outcome, much as was reached in the *Playboy* case.

In all, holding system administrators strictly liable for wrongful messages on their systems fits well with the rationale for strict liability

---

133. 18 U.S.C. § 2511(2)(a)(i) (1988).

134. *Gertz v. Robert Welch, Inc.*, 418 U.S. 323, 348-50 (1974). Strict liability was unavailable against information distributors like bookstores even before *Gertz*. See *Smith v. California*, 361 U.S. 147, 152-53 (1959). Note that whether a system administrator is at "fault" (and hence can be held liable without violating the Court's "no strict liability" rule) is a bit circular: if the law requires monitoring e-mail for defamatory messages, then a system administrator can be described as negligent for not doing so.

135. *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135, 139 (S.D.N.Y. 1991).

136. See *id.* at 140 ("CompuServe carries the publication as part of a forum that is managed by a company unrelated to CompuServe."); *id.* at 142-43 (discussing and rejecting CompuServe's vicarious liability).



and is an appropriate outcome for all cases but defamation, where First Amendment concerns impose at least a negligence requirement.

#### *H. Anonymous Messages*

One problem mentioned at the outset of this article was that of "anonymous remailer" computers that allow authors to send truly anonymous messages to others. The policies applicable to the regulation of such messages, when they are wrongful in the ways we have been examining, vary somewhat from those applicable to identified messages. In particular, anonymous messages bring two competing values into conflict: On the one hand, there is the desire of the law to provide redress to injured plaintiffs who have been defamed or had their copyrighted work distributed without authorization. On the other hand, there is the desire of individuals to be able to "speak their mind" without fear of retribution, a policy primarily applicable to defamatory statements, and one certainly furthered by anonymity.

With reference to the fear of retribution, defamation specifically is an area for which the U.S. legal system has to some extent already provided an accommodation. The First Amendment generally insulates individuals from retaliation for their criticism of the government. Not only may the government itself not officially punish such speech, but as already discussed, the incorporation of First Amendment restrictions into defamation law provides generous protection for libel defendants.<sup>137</sup> Thus under, U.S. law, the need to provide for anonymous messages in order to permit uninhibited public commentary is much less than it might otherwise be.

Private commentary that is identifiable (not anonymous) exhibits a balanced set of incentives. A defamatory message concerning a private individual does not invoke any issue of government retaliation, so that fear of retaliation is no deterrent to the defendant-defamer. On the other hand, the high standard of proof that public figure libel plaintiffs must meet does not apply to private figure plaintiffs, so that the threat of such a suit is a deterrent to the defendant-defamer.<sup>138</sup>

When unidentified, anonymous messages defame private individuals, however, the balance disappears. To be sure, the threat of government retaliation never existed, and that fact is no different because the

---

137. See *New York Times v. Sullivan*, 376 U.S. 254 (1964).

138. Private figure plaintiffs must prove the defendant's "fault," but they need not prove that the defendant knew the statements were false or were reckless in disregarding truth or falsity. *Gertz*, 418 U.S. at 342-50 (1974).

message is anonymous; but now the threat of a civil defamation suit is eliminated because the defendant who defames cannot be identified. In economic terms, the "cost" of a privately defamatory communication to its author is reduced to near zero by anonymity, leading one to predict that the incidence of such communications will rise, perhaps dramatically.

How should the law respond? Recall that we are not talking about the defamation issue directly; rather we are asking whether anonymous messages, which create the possibility of costless defamation, should be permitted. More precisely, we must analyze whether that issue is appropriate for statutory, judicial, contractual, self-help, or other methods of control.

Instinct might dictate that this is an area for judicial or statutory control, much like the case of identified defamation discussed above. Injured plaintiffs and the defendants who defame them are not in a contractual relationship. The plaintiffs are, therefore, "external" to the activities in question (the sending of a defamatory message). There is no necessarily identifiable group of which both plaintiffs and defendants will be mutually advantaged members and for whom a private association and its by-laws might therefore be suitably designed.

Yet perhaps the context of anonymous defamation is one in which injured plaintiffs have an even stronger self-help remedy than was true with identified defamation: they can ignore the defamatory remarks or rebut them, and they can count on others to sharply discount the defamatory remarks. The key here is the recognition that anonymous defamation is nearly costless and hence trivially easy to create. When remarks are essentially costless, the impact of such remarks on the plaintiff's actual reputation will be far less than were the same remarks issued from an identified, reputable individual. The outcome here is like monetary inflation: when more money is put into circulation, each dollar is worth less. When more defamatory remarks are put into circulation, from no known source, each such remark becomes worth less—that is, carries less of a sting and is less harmful.

The very power of anonymity, in short, is the plaintiff's own protection, for anonymous remarks will be greatly devalued precisely because they are anonymous and easy to make. This devaluation will be furthered if defamation suits become known to be unfeasible, as presumably anonymity would make them. Thus, when everyone can defame with impunity, defamation means very little. Coupled with the access to the means of effective response that cyberspace provides to

plaintiffs, this devalued quality of anonymous defamation argues that plaintiffs can unilaterally care for themselves.

An adequate first response to the issue of anonymous defamatory messages is therefore for the legal system to do nothing, trusting instead to individuals' self-help in the form of the plaintiffs defending themselves through the same cyberspace medium by which they were defamed, and to the general devaluation and lowered importance of defamatory messages that are from anonymous sources.

It is not likely that the self-help solution for anonymous defamation will ever have time to take hold, however, because other remedies will be necessary for the problem of anonymous copyright infringement. Once a copyrighted work has been released into cyberspace, it is available for consumption; wide distribution would not devalue it for readers, but it would certainly "devalue" the work for authors who would lose the opportunity for royalty payments. With infringing works distributed by anonymous sources, what remedy could the infringed author seek? The infringed author is certainly not in a contractual relationship with the infringer, nor necessarily with a common cyberspace service. From the perspective of the infringer, the author is very much an external effect of the anonymous distribution of the author's work.

Is it possible to "internalize" the harms of anonymous copyright infringement by contracting at a "higher level" than that existing between user and system administrator? That is, although an infringed author is not privy to the contract between the anonymous remailer's system administrator and the anonymous infringer, the system administrator could be in a contractual relationship with all other BBSs in the network. Perhaps that contract can form the basis for a limitation on forwarding copyright infringing works through the network.

The difficulty with this approach is that the mutuality of benefits that characterizes association by-laws does not apply here. Very likely all members of the association will not see themselves as copyright authors—perhaps few if any will. The need for limitations on anonymous forwarding of copyright infringing material will therefore lack the appeal of, say, requirements to forward mail generally, which has clear benefits for all parties.

It seems apparent that neither self-help nor contract-based solutions will be of much service in this copyright matter. That suggests either of two remaining options. The first is an outright statutory prohibition on "anonymous remailers," the BBSs that provide the anony-

mous message mechanism; the second, as proposed earlier,<sup>139</sup> is to impose strict liability on the system administrators of such facilities. The case for the system administrator's strict liability is certainly strong here: to put the matter informally, the system administrator of an anonymous facility looks like the "bad guy" and will not be a sympathetic defendant in court.

One further complication clouds the picture. It is possible that BBSs in cyberspace might function as anonymous remailers some of the time, and not others. They might, therefore, be difficult to identify. More particularly, it may be difficult to identify from which of several anonymous remailers a given copyright infringing work was distributed. Plaintiffs might be able to find a court congenial to the application of strict liability, but not be able to find a defendant to whom it should apply.

This complication leads to the final conclusion that the only effective deterrent to the problems of anonymous remailers will be to prohibit them altogether. This is, in terms of the various levels of behavioral regulation discussed in this article, a rather drastic solution, but the sharp externalities and the problems of identifying the BBS origins of anonymous messages suggest that this will prove to be the only recourse. Because of the ease with which messages in cyberspace may be routed across national borders, it is also likely that some form of international cooperation, such as a treaty, will be necessary for the prohibition to be effective.

### *I. International Torts*

We have been discussing the liability of system administrators of anonymous remailer facilities for "wrongful" messages. Even without regard to the arguable wrong-doing of an intermediary like the system administrator, cyberspace as a conduit permits wrongful messages to be sent internationally with ease.

Without cyberspace, it is today possible for a citizen of one country to commit a tort with regard to a plaintiff in another country. The easiest example is our familiar one of defamation. A citizen of country X can mail letters to country Y defaming a citizen of that country. As a practical matter, however, this does not seem to occur with any frequency. Yet with cyberspace, the possibilities seem far less remote. For one thing, cyberspace makes it dramatically easier for citizens in one

---

139. See *supra* text accompanying notes 126-38.

nation to get to know citizens of other nations. This is in fact a strikingly common occurrence on the Internet already today. The extremely low cost of cyberspace communication makes practical the distribution of defamatory or other wrongful communications on a scale not before possible.<sup>140</sup> For these reasons, the issue of international torts is likely to be much more significant in cyberspace than it has been to date in real space.

What is the "lowest level" solution for this problem? By hypothesis we are talking about torts, that is, wrongful conduct typically directed toward strangers, so the contract approach is ruled out. To be sure, as with anonymous defamation, self-help in the form of ignoring or responding is eminently possible, but now we are talking about identified wrongdoers, not anonymous ones. Furthermore, the sting of a libelous communication from an identified source is likely to be greater than from an anonymous one. Moreover, other wrongful communications besides defamation are readily possible, including disclosure of trade secrets and copyright infringement. For these wrongs, ignoring or replying to the wrongful communication is no answer.

With the broad international scope of this problem, it is tempting to look toward international agencies like the United Nations to devise appropriate rules. But international agencies have no authoritative jurisdiction; when international courts hear cases, it is typically between sovereign nations who have consented to jurisdiction because they see themselves as repeat players on the international scene. An individual in Singapore defamed by an individual in Nebraska is not likely to have access to the World Court, even if international defamation rules were promulgated. Local courts in Nebraska would be prohibitively expensive for the Singapore plaintiff; Singapore courts prohibitive for the Nebraska defendant. Trade secret theft is more likely to involve businesses with the ability to bring suit, but again, pursuing a foreign defendant overseas will in many cases simply not be economically feasible.

Instances like these suggest, though it may seem a bit odd, that cyberspace users form their own virtual courts. How such a court

---

140. A recent case in Australia demonstrates the reality of this scale of distribution. The defendant wrote a defamatory message about an Australian university professor who had been denied tenure. This message was distributed to an estimated 23,000 world-wide members of a cyberspace discussion group. The court's judgment, entered when the defendant defaulted and which recapitulated the defamatory message, was itself also circulated to an untold number of Internet users, including the author. See *Rindos v. Hardwick*, unreported judgment 940164 (Supreme Court of Western Australia) 31 March 1994.

would work mechanically is not entirely clear at this point, but the desirability of such action for just such circumstances as we are discussing seems indisputable. The capability of communications networks is rapidly growing; almost certainly audio and full-motion video will be routinely available to cyberspace users in a matter of few years. It is easily possible to imagine on-line cyberspace hearings, with judges, juries, attorneys, and whatever assortment of bailiffs and observers might be appropriate. The sanctions imposed could be the usual private association sanction of expulsion or suspension from the relevant part of cyberspace.

To be sure, such a court system and its threat of expulsion would require a great deal of international cooperation among a wide array of groups. Yet the cooperation would be cost-effective if the resulting structure served to resolve many disputes over many years. Cost (including time and effort) is only important relative to the value of the object sought, and a cyberspace court system might prove extremely valuable. Besides, much of the cost of setting up an internationally coordinated set of procedures and rules is incurred in communicating back and forth among those who are engaged in the project—and cyberspace is nothing if not a low-cost means for communicating internationally.

## V. CONCLUSION

Some of the legal problems of cyberspace are indistinguishable from those that arise in real space. For the most part, these situations are characterized by the use of cyberspace as merely another means of transmission from individuals directly to other individuals. Defamatory e-mail messages from “A” to “B” in regard to “C” are no different from defamatory letters or phone calls.

Cyberspace does raise other interesting legal questions that are new enough to merit attention and to call for solutions. “Newness” here means that some sort of legal solution tailored to the cyberspace problem will bring clarity and predictability to the rules attending cyberspace conduct, the benefits of which outweigh the additional complexity thereby added to the legal system, or that the underlying policy concerns of “real space” law are inappropriate when applied to activities in cyberspace.

The questions that are “new” in this sense come in several varieties. Some are new not because they are unprecedented in real space, but rather because they will occur so much more frequently in cyber-

space that a clearer resolution is required. The ease with which anonymous messages can be sent in cyberspace is one example.

Other legal problems of cyberspace will be new in a stronger sense, such as questions that turn on the reasonableness of behavior when "reasonableness" in this new medium is yet ill-defined. Still other problems will be worth addressing as new because they invoke the new role of the "system administrator" as a communications intermediary. System administrators function in cyberspace something like bookstores, something like telephone companies, something like publishers . . . and something like none of these. That makes their rights and obligations difficult to define.

The definition of rights and obligations generally in cyberspace can be accomplished in a variety of ways. The obvious ways are the "top down" implementation of rules through legislative enactment or judicial decision. But countless varieties of other, "bottom up" rule making processes are also workable. Unilateral self help (individuals avoid exposure to that which they do not like), contracts, private associations (which are contracts in the form of by-laws designed to outlast the individuals who form them), and the development of customs, are all mechanisms by which behavior in cyberspace might be regulated.

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. This presumption means that the first answer to how a legal problem in cyberspace should be solved is to "do nothing." That is, let the affected individuals withdraw from activities they do not like.

Cases in which unilateral self-help are inappropriate are often self-correcting: individuals who can further their interests best through cooperative rather than unilateral behavior will naturally turn to contracts as the second level of behavior regulation. Contracts can govern a wide variety of problems in cyberspace and should form the basic control mechanism for much cyberspace activity.

Contracts cease to function well when they create or allow significant external effects, such as when a user of a cyberspace service like electronic mail on a bulletin board system uses the service to store defamatory or other wrongful messages in regard to third parties. In cases like these where the primary effect is harm to third parties, exter-

nal to any contracts, the only solution will be a statutory or judicial one.