Anarchy, State, and the Internet:
An Essay on Law-Making in Cyberspace (article 3)

David G. Post [FN 1]

[Cite as: David G. Post,
Anarchy, State, and the Internet:
An Essay on Law-Making in Cyberspace,
1995 J. ONLINE L. art. 3, par. _____.]

JOL Copyright Policy

Copyright to the Journal of Online Law as a collective work belongs to the editor. Authors retain the copyright to their individual articles, but unless otherwise noted in an individual article, all authors and the journal's editor agree to the following:

Classroom use. Electronic or paper copies of the journal or its individual articles may be made for classroom use, provided that the copies are distributed at or below the cost of reproduction and the author(s) and the Journal of Online Law are credited and identified as the copyright holders.

Other uses. The journal may be distributed by individuals to individuals for non-commercial purposes, but not by means of Web site postings, distribution lists, listserv lists, newsgroups, BBS postings, multiple copies, or other bulk distribution, access, or reproduction mechanisms that substitute for a subscription or authorized individual access, or in any manner that is not a good faith attempt to comply with these restrictions.

Links. Links from other sites to JOL's web site are encouraged.

Abstract

{par. 1} The legal rules that will govern cyberspace are yet to be clarified. Important as those rules will be, a prior question is "who will make and enforce those rules?" Professor Post examines various "controllers," or points from which rules can issue, ranging from technical network protocols, to private organizations like universities, to Congressional statutes. These controllers vary in their ability to enforce whatever rules they choose to adopt, depending on the existence of conflicting higher-level controllers, and on the possibility that those who are subject to the rules can change jurisdictions to seek a more favorable rule set. The Internet allows a relatively easy change of jurisdiction, or "exit," from any given controller, leading to the unprecedented-and unpredictable-situation of a "free market" in rule sets.

Introduction

{par. 2} Increasing attention is currently paid to important and interesting questions about the rules that will, or should, govern behavior within the global networked environment: What shape should copyright protection take in a world of instantaneous, costless, and undetectable copying? Should the First Amendment be interpreted to encompass a right to post anonymous messages, or commercial messages, across Usenet groups, or a right to send encrypted messages that are, for all intents and purposes, immune to eavesdropping by law enforcement? What standard of liability should be imposed on system operators in regard to the availability of "obscene" material on their systems?
This focus on the substantive content of legal rules reflects, at least in part, what Oliver Williamson has called "legal centralism." [FN 2] A "centralist" inquiry focuses on alternative sets of substantive laws-with an eye toward determining which set is optimal in terms of some pre-defined criterion such as aggregate welfare. This is an entirely appropriate model for an inquiry where some law-making body-typically a sovereign government—is in a position to choose the optimal set of laws.

My focus in this essay, however, is elsewhere. To the extent that the global network proves relatively resistant to centralized control—and I believe that it will so prove, for some of the reasons addressed below—the question "Which copyright law is 'best'" must at least be supplemented by the question "What are the forces that govern the legal system's trajectory through 'rule-space', and which configuration(s) of copyright law is likely to emerge from the operation of those forces over time?" [FN 3] Before we try to answer the substantive questions—before we try to decide what the "best" copyright law for the global network might look like—we should pause to consider a necessarily antecedent question: what mechanisms exist whereby such a law could be implemented? Who can make and enforce the rules in cyberspace, whatever the substantive content of those rules might be?

What follows is a rough sketch both of the reasons why these are particularly interesting and rich questions in the context of electronic networks, and also of a framework that may help to structure the inquiry into law and law-making on the global network. Cyberspace has itself already demonstrated the immense power of collective intellectual efforts, and I offer this essay in the hopes of spurring others to think about these important questions in new and fruitful ways. [FN 4]

**Law-Making and Social Control in Network Communities**

Robert Ellickson's framework for behavioral controls is a useful starting point for a discussion of the various forces governing individual behavior in electronic networks. [FN 5]

Ellickson identifies five "controllers" that can provide substantive rules governing an individual's behavior: the actor him/herself, other individuals being acted upon, non-hierarchically organized social forces, hierarchically-organized non-governmental organizations, and, finally, governments, i.e., hierarchical organizations "widely regarded as having the legitimate authority to inflict detriments on persons within its geographically defined jurisdiction who have not necessarily voluntarily submitted themselves to its authority." [FN 6] Ellickson's descriptive labels for each controller's substantive rules, and the rewards and punishments through which each enforces those rules, are set forth below.

<table>
<thead>
<tr>
<th>Controller</th>
<th>Substantive Rules</th>
<th>Sanctions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The actor him/herself</td>
<td>Personal ethics</td>
<td>Self-sanction</td>
</tr>
<tr>
<td>Second party controllers, i.e., the person acted upon</td>
<td>Contractual provisions</td>
<td>Various self-help mechanisms</td>
</tr>
<tr>
<td>Non-hierarchically organized social forces</td>
<td>Social norms</td>
<td>Social sanctions</td>
</tr>
<tr>
<td>Hierarchically organized non-governmental</td>
<td>Organization rules</td>
<td>Organization sanctions</td>
</tr>
</tbody>
</table>
For an illustration of the application of this framework, consider the various rules that combine to determine the frequency with which a particular behavior—say, the transmission of messages containing any of the FCC's "seven dirty words" might occur on my university's local area network. [FN 7] Each network participant may have a personal ethical position in regard to the propriety or impropriety of such messages.

One can imagine—not terribly realistically, perhaps, in this context—bilateral agreements between network users regarding the use of particular words in e-mail messages or in files stored on the network, or even resort to self-help (in the form of authorized or unauthorized file deletion) by individual network users. Each of these is, in turn, at least partially determined by each user's response to various social forces such as cultural or professional norms. Formal or informal organization rules, promulgated by the network administrators (i.e., by Georgetown University itself), may apply to this conduct, as may federal or state laws regarding the transmission of "obscene" messages.

The question I am here addressing—who's rules will govern behavior in cyberspace?—can thus be rephrased: how does the competition among these controllers proceed? What are the "controller-selecting rules" [FN 8] that determine which controller's rules take precedence in the event of conflict? To take a concrete example, how would the Communications Decency Act recently introduced in the US Senate [FN 9] affect the frequency with which "indecent" or "obscene" communications appear in any particular network community if the proscriptions in that Act conflicted with other behavioral "controllers" within that community? And most specifically, what are the special characteristics of electronic networks that might influence the way in which these controller-selecting rules operate?

The Nature of Networks

1. Networks-electronic or otherwise—are particular kinds of "organizations" that are not merely capable of promulgating substantive rules of conduct; their very essence is defined by such rules—in this case, the "network protocols". Accordingly, the person or entity in a position to dictate the content of these network protocols is, in the first instance at least, a primary "rule-maker" in regard to behavior on the network.

What we call "cyberspace" can be characterized as a multitude of individual, but interconnected, electronic communications networks, e.g., individual BBS systems, Prodigy, the Georgetown University LAN, the Cyberia discussion list, or the network of machines that can communicate across the World Wide Web. Communication networks of any kind—a number of individuals meeting together in a room or the network comprising the people who read this essay, in addition to the network of computers communicating on America Online—are defined at a minimum by a set of rules—the "network protocols"—specifying (a) the medium through which messages can travel, (b) the characteristics of the messages that are permitted to enter the network, and the manner in which messages are routed through this medium to network members.

A group of children playing the game of "telephone," for example, constitutes a network, as do the participants in a university seminar presentation. In both, the network protocols require audible sounds transmitted through the atmosphere (though at low volume in the case of "telephone"). Each network has its own message origination and routing rules; in "telephone," messages originate with the child on one side of the room and are routed
from one child to the child immediately adjacent. At the seminar, the rules may require that all messages originate from the speaker ("No questions until I'm finished") from whom they are routed simultaneously to all participants ("Can you hear me in the back row?").

{par. 15} Similarly, the local area network at Georgetown University on which I am composing this essay requires that messages be transmitted through special cabling installed in our building, and further that those messages obey certain formatting and coding conventions, embodied in the LAN operating system software, that will allow them to be appropriately managed by the central LAN server.

{par. 16} In one sense, then, networks are not merely governed by substantive rules of conduct, they have no existence apart from such rules. Viewed in this light, the network protocols have a kind of first-order competitive advantage over other controllers in regard to the behavior that occurs there by virtue of their ability to control entry onto the network by excluding behavior that is inconsistent with the message entry rules. Accordingly, the person or entity in a position to dictate the content of these network protocols is, in the first instance at least, a primary "rule-maker" in regard to behavior on the network.

{par. 17} This is, admittedly, something of a definitional trick in regard to most ordinary networks, unlikely to illuminate behavioral questions of real interest, because the boundary between being "on" and "off" the network has little objective meaning with respect to whatever questions we are likely to have about the frequency with which particular behaviors manifest themselves. For example, suppose that during our game of telephone one of the children stands up and says, in an inappropriately loud voice:

{par. 18} "This is a stupid game, here's what the message is: 'Johnny and Susie were holding hands in class yesterday'."

{par. 19} If we are interested in how these children behave on the "telephone game" network, we can ignore this comment; because it violates the network protocols, we can simply deem it to have occurred "off the network." But that is unlikely to help us understand the children's behavior in any meaningful sense. The other children have heard the message, and have observed this conduct, even though it took place "off the network." To the extent that this particular network is largely an artificial construct existing almost exclusively in the mind of the observer, the fact that in some technical sense the protocols exclude this particular behavior will have few, if any, meaningful consequences.

{par. 20} Entry of messages into, and routing of messages across, digitally-based electronic networks, however, are controlled by more effective protocols than in our game-of-telephone example: each network's technical specifications (typically embodied in software or switching mechanisms) constitute rules that precisely distinguish between compliant and non-compliant messages. This boundary is less easily dismissed as an artificial construct because the rules are effectively self-enforcing. To put the matter simply, you can't "almost" be on the Georgetown University LAN or America Online-you are either transmitting LAN- or AOL-compliant messages or you are not.

{par. 21} As a consequence, the ability of this control mechanism to impose its rules on network conduct is considerably less trivial for electronic networks than for their non-electronic counterparts, because permissible behavior can be more precisely demarcated from that which is impermissible. Any discussion of rule-making in cyberspace therefore should begin by looking at the role of the entities and institutions defining the network protocols, because this level of organizational controller has what might be termed "competitive advantages" over other controllers in electronic network communities.
Are these network technical specifications, then, part of the "law of cyberspace"? I believe that they are—or at least that it would be profitable to analyze them as such. On the one hand, they would appear to govern a fairly narrow range of what we might want to call "behavior." Whether one is using an HTML-compliant Internet browser, even or odd parity to communicate over a network, fixed- or variable-length message packets, or the SMTP mail-routing protocol, would not appear to have much to do with the behavioral questions of copyright infringement, transmission of obscene messages, fraud, and the like that we’re really interested in when we speak of the "law of cyberspace." Because network technical specifications generally operate on those message characteristics unrelated to message content, they might appear to be of little relevance to our understanding of the constraints on behaviors that can only be defined with reference to precisely that content.

But we shouldn’t dismiss them quite so quickly as entirely irrelevant to our inquiry, because these technical specifications may reach further down into message content and meaning than one might think at first glance. It is easy to overlook the fact that the message traffic over digital networks consists entirely of strings of binary digits. In this environment, the line between the meaning contained in message transmissions, and the purely technical contours of those messages, is blurred indeed.

One can hardly imagine, to be sure, a rule regarding, say, fraudulent transactions that would be capable of digital embodiment in these engineering specifications. One can imagine, however, a digital embodiment of rules regarding other activities—for example, the transmission of anonymous messages, or encrypted files—that can be more easily expressed in digital form and thereby enforced at the level of the technical network specifications. The scope for digitizing behavioral rules represents a particularly fruitful avenue of inquiry in any attempt to determine the role that these specifications may play in setting the rules of conduct on these networks. [FN 10]

And note also that these digitally-embodied network specifications are not the only means by which the network organization controller can impose its rules regarding permissible or prohibited network behaviors. Any centralized network architecture involving a single location through which all messages must pass—whether it is a client-server LAN or a moderated Internet newsgroup—allows for the examination of all transmissions for compliance with specific behavioral rules. That is, whether or not Georgetown University's LAN can implement in its operating system software a rule excluding "obscene" messages, the LAN administrator can, though perhaps at significant cost, screen all messages for compliance with a rule prohibiting such transmissions. [FN 11] Similarly, a discussion group moderator can announce and enforce a rule providing that any messages not meeting certain criteria—relevance to the group’s focus, or taste or propriety, etc. will be deleted.

My thesis, then, is that this controller—the individual network "organizations" themselves—possesses at least certain inherent advantages in the competition for rule-making precedence in cyberspace, and that this controller is therefore potentially the locus for much of the substantive rule-making that will take place there.

"Potentially" is the operative word. Saying that cyberspace may consist of a large number of individual networks, each with its own rules (about, e.g., the propriety of obscene text and the definition of "obscenity") does not tell us whether or not the law of cyberspace will in the aggregate consist of a diverse set of such rules or will converge on a single, or a small number, of such rules. To analyze that question we need to examine one additional feature of the competition among controllers.

2. The competition among controllers is asymmetric, at least insofar as the State holds a monopoly on the imposition of coercive sanctions on controllers lower down
in the controller hierarchy. The State's ability to impose its substantive law by means of such sanctions, however, is substantially constrained by the existence of the global Internet itself, which provides a credible exit strategy for networks and other lower order controllers.

{par. 29} There is something of an asymmetry in the ranking of controllers, at least insofar as the State has a monopoly on the use of coercive sanctions when faced with violations of whatever rules it promulgates. Thus, we can speak of the ability of this controller to impose its laws on the individuals, contracting parties, or organizations lower down in the controller hierarchy, but not vice versa; neither individual actors, nor contracting parties, nor organizations, can similarly impose their preferred substantive rules on the State where the State's laws are in conflict with theirs. The effectiveness of the State's sanctions, generally speaking, is an inverse function of the ease with which the lower-order controllers can "exit" from the regime defined by those laws-by evading detection of rule-violating behavior, evading the State-imposed sanctions for such violations, or somehow withdrawing from the rule-making jurisdiction of the State as controller. [FN 12]

{par. 30} This notion of "exit" may be generalized to apply across the entire controller hierarchy, i.e, it may be useful to think of each controller possessing the ability to impose its rules on lower-order controllers, each of whom needs to rely on some form of exit in order to counter that imposition. Thus, the organization by whom I am employed, Georgetown University, can impose its rules regarding proper faculty conduct on my behavior, subject to my ability to evade detection should I behave in contravention of those rules, my ability to evade the sanctions that Georgetown imposes in the event such behavior is detected, and, finally, my ability to obtain substantially equivalent employment elsewhere and thereby leave Georgetown's jurisdiction entirely.

{par. 31} Returning, then, to our question of diversity and uniformity of network rule-sets, imposition of governmental laws on those individual network rule-sets is one way that a measure of rule-uniformity may emerge in cyberspace. The State will experience obvious difficulties in attempting to monitor the behavior of individual network users, who are numerous and dispersed across many such networks. Because each such network functions as a gatekeeper for its users in cyberspace, however, we might expect that governments will try to rely instead on their ability to impose coercive sanctions on network administrators (and thereby on the network rules) in order to implement their own particular preferred set of rules on behavior in this environment. [FN 13]

{par. 32} The extent to which this will occur, and the substantive areas in which this strategy is most likely to be tried and in which it is most likely to be effective, are important and complex questions the full explication of which is far beyond the scope of this essay. I have, again, a single observation that may shed some light here: the existence of the global internetwork functions as a significant constraint on any sovereign's ability to implement this strategy.

{par. 33} The Internet, like any network, is not a physical object with a tangible existence, but is itself a set of network protocols that has been adopted by a large number of individual networks allowing the transfer of information among them. There may well be no principle more important for understanding rule-making in cyberspace than that of distinguishing between the Internet as a whole and the individual networks that are its component members; it is indeed the interplay between the vast number of largely centralized individual networks and the decentralized internetwork through which they can communicate that will prove to be of fundamental importance in determining the efficacy with which State law can be imposed on individual network communities. [FN 14]
The State's ability to impose sanctions on law-violators is fundamentally constrained by the need for physical proximity and physical control. This is by no means an absolute constraint; mechanisms do exist, of course, whereby individual sovereigns can impose their rules on persons or entities not physically present in the area over which the sovereign has control.

Such mechanisms, however, entail additional enforcement costs, both in terms of the direct costs of projecting sovereign power extra-territorially and the costs of coordinating and harmonizing the legal regimes of competing sovereigns. Thus, United States law is not ordinarily applicable to, nor can the United States ordinarily apply sanctions on, a network operator in, say, Singapore; attempts by the United States to go around these limitations require either some means of obtaining control over the network operator or its assets, or some measure of cooperation with State authorities in Singapore or other jurisdictions where the operator maintains physical assets on which judgments can be executed.

The Internet, of course, is multi-jurisdictional in the obvious sense that messages can travel from a network in Washington to one in Singapore, or Kazakhstan, or anywhere on the globe where there are computers with access to the Internet's medium of communication. But the Internet is not merely multi-jurisdictional, it is almost "a-jurisdictional:" physical location, and physical boundaries, are irrelevant in this networked environment in a way that has, I believe, no parallel elsewhere.

Moving through the World Wide Web, for example, by following hypertext links from one Internet site to another, the user is almost completely indifferent (and, indeed, may have no way of knowing) whether the file she is viewing resides on a computer down the street or across the globe; similarly, whether control of the Cyberia listserver is exercised by a computer in Williamsburg, Virginia or Williams Corner, New South Wales, has almost no effect on the functional capabilities of that particular network or the ease with which any individual with Internet access can participate in the activities taking place on that network.

This independence from geographical constraints results from both the electronic nature of the message transmission, which largely de-couples the physical distance between communicating machines from message travel times and, more significantly, from the decentralized design of the Internet. Because the Internet, unlike most of its constituent networks, was designed without a centralized control mechanism or any single location through which all internetwork traffic must travel, all network nodes are effectively equipotent, each equally capable of performing the key internetwork message routing functions.

As a consequence, the Internet itself is an "exit strategy" for individual network rule-makers, in two senses. First, the Internet allows one to exit by evading detection. Decentralization implies that the costs of monitoring behavior are substantially higher, and rule-violative behavior substantially more difficult to detect, than would be the case under a centralized internetwork design.

The second sense pertains to exit by withdrawal from jurisdictional control, the relocation of rule-violative behavior so that it is outside the jurisdiction of any physically-based sovereign. Should a particular network rule-set be incompatible with the law of sovereign X, the network rule-set itself can, with relative ease, be transferred elsewhere on the internetwork, outside of the sovereign's jurisdictional boundaries. Georgetown University, that is, may indeed choose to implement a particular rule prohibiting the transmission of certain kinds of pornographic images across the Georgetown LAN, and it may well do so because the District of Columbia, or the United States, government has forced it to do so (i.e., has decided to impose sanctions on networks within its jurisdictional control who do not...
implement such rules). And Georgetown may indeed be able to enforce this prohibition in regard to its own network, subject to whatever difficulties it may encounter in trying to detect violations of this rule.

{par. 41} The effect of Georgetown's rules on the behavior itself, however-on the availability of pornographic images and the frequency with which such images are transmitted across the aggregated internetwork-may be considerably attenuated or even non-existent. To the extent that those conducting this behavior on the Georgetown LAN can, by virtue of their access to the Internet, equally easily access some other network whose rules are not subject to the control of the District of Columbia or United States, this rule-set, and the images themselves, can migrate to the less restrictive jurisdiction.

Conclusion

{par. 42} The model sketched out above implies that although each individual network can be constrained from "above" in regard to the rule-sets it can, or cannot, adopt, the aggregate range of such rule-sets in cyberspace will be far less susceptible to such control. A kind of competition between individual networks to design and implement rule-sets compatible with the preferences of individual internetwork users will thus materialize in a new and largely unregulated, because largely unregulatable, market for rules. The outcome of the individual decisions within this market-the aggregated choices of individual users seeking particular network rule-sets most to their liking-will therefore, to a significant extent, determine the contours of the "law of cyberspace."

{par. 43} What kind of rules will emerge from this process? We have almost no experience with unregulated markets for social control rules, and hence have little basis for predicting the criteria that people are likely to use in choosing among these alternative rule-sets and to predict the outcome of this competition. [FN 15] Two points seem clear, however. First, the prospect of relatively unfettered individual choice among competing sets of rules is surely an attractive prospect, to the extent that what emerges represents the rules that people have voluntarily chosen to adopt rather than rules that have been imposed by others upon them.

{par. 44} Second, rules governing behavior in individual networks may generate negative externalities in regard to participants in other networks in much the same way that an individual geographical community's laws (regarding, say, water pollution) can impose costs on neighboring communities. [FN 16] All communities may benefit from an agreement establishing a rule prohibiting polluting activities, but absent a means to enforce that agreement it may be in each individual community's interests to "cheat." This, of course, is the familiar Prisoner's Dilemma, and to the extent that my description of rule-making in cyberspace is accurate, there may be no more important task facing those interested in the future course of cyberspace than to develop ways in which this coordination problem can be solved with a minimum of interference with the freedom of individuals to choose the rules under which they wish to operate.

FOOTNOTES

NOTE 1: Copyright 1995 David G. Post, Visiting Associate Professor of Law, Georgetown University Law Center, and Policy Fellow, Electronic Frontier Foundation. I want to thank the many participants on the discussion groups on Lexis Counsel Connect, as well as on the
Cyberia listserver, for their innumerable interesting and instructive comments which have helped me formulate some of the ideas expressed in this essay. A version of this paper was delivered at the Georgetown University Faculty Research Seminar, and I thank participants in that forum—Avery Katz, Marc Rotenberg, Steve Salop, and Warren Schwartz in particular—as well as Eugene Volokh, for helpful comments on earlier drafts. The ideas expressed, and all remaining errors are, of course, my responsibility alone. I can be reached by e-mail at Dpostn00@Reach.com or Postd@law.georgetown.edu.


**NOTE 3**: Evolutionary biology illustrates these differences in approach. To understand why cockroaches are the way they are, biologists do not begin with questions of the form "what is the optimally-designed cockroach?" or "would a cockroach with 8 legs, or one capable of photosynthesis, be a 'better' cockroach?" Those questions might well be appropriate if we were in the business of designing some organism to do cockroach-like things. But biological evolution proceeds without a central design authority that chooses among alternative versions of the cockroach, and questions regarding "optimal cockroach design" make no sense until an antecedent question—"what is the process by which changes in cockroach design are implemented"—is satisfactorily answered. To explain why cockroaches are the way they are, or to predict what they will look like in the future, evolutionary biologists must begin with a theory of how evolution proceeds, and then ask "Can we explain the features of the cockroach by reference to the working of those evolutionary forces?" (and, if not, does our theory of the way evolution proceeds, or our understanding of the problems faced by the cockroach, or both, need to be revised?). Identification of the optimum is still of interest, to be sure, but only in the context of asking whether these forces are likely to produce a system at or close to this optimum. For a discussion of these issues, see Post, Is the Optimization Approach the Optimal Approach to Primate Foraging? in ADAPTATIONS FOR FORAGING IN NONHUMAN PRIMATES, (P. Rodman & J. Cant, eds.) (1984).

**NOTE 4**: I do not mean to suggest that I am the first person to look at this meta-question of law-making in cyberspace. See, e.g., I. Trotter Hardy, The Proper Legal Regime for Cyberspace, 55 U. PIT. L. REV. 993 (1994); David R. Johnson and Kevin A. Marks, Mapping Electronic Data Communications onto Existing Legal Metaphors: Should We Let Our Conscience (and our Contracts) be our Guide?, 38 VILL. L. REV. 487 (1993).

**NOTE 5**: ELLICKSON, supra note 2, at 123-36.


**NOTE 7**: I use the example of the Georgetown University local area network throughout this paper purely, it should be stressed, for illustrative purposes.

**NOTE 8**: In Ellickson's words, "In a society replete with governments, private organizations, social forces, contractual arrangements, and individuals potentially capable of self-control, there must be rules that decide, for each domain of human activity, the division of social-control labor among the various controllers. Controller-selecting rules perform this function."
NOTE 9: The Communications Decency Act of 1995, S. 314, was introduced on February 1, 1995 by Senator Exon and would subject to criminal and civil liability anyone who "transmits or otherwise makes available" by means of a "telephone or telecommunications device" any "obscene, lewd, lascivious, filthy, or indecent" comment. This has occasioned much controversy; relevant materials can be located at the Electronic Frontier Foundation World Wide Web site. Return to Text

NOTE 10: To take another example, the design of the next generation of the hypertext transfer protocol-HTTP, the set of specifications permitting transmission of World Wide Web documents is currently being considered by the Internet Engineering Task Force. See <http://www.w3.org>. One of the design goals under consideration for implementation within this new version of HTTP would optimize the "caching" of World Wide Web pages; caching involves downloading and copying Web pages off of their host machines and onto intermediate servers (a LAN server, for example, or some other individual network host), which enables those users with direct connections to that intermediate host to access those pages without the need to wait for files to be transferred over the Internet. Caching, of course, raises difficult questions under U.S. copyright law; if storing a Web page in a cache constitutes the making of a "copy" — as it well might under the view of such cases as MAI Systems Corp. v. Peak Computer, Inc., 991 F.2d 511 (9th Cir. 1993) and Advanced Computer Services v. MA Systems Corp., 845 F.Supp. 356 (E.D. Va. 1994), holding that transitory fixation in RAM constitutes copying for purposes of the Copyright Act — then each instance of caching constitutes prima facie copyright infringement. My point here is not to debate whether or not copyright law should be interpreted in this manner, but rather that anyone interested in that question must take a long look at the new HTTP standards, for any view of the copyright rules that will govern on the Internet that does not take these technical rules regarding permissible copying into account will necessarily be sorely deficient. Return to Text

NOTE 11: One is reminded of the report that Prodigy examines all electronic mail transmissions for the purpose of identifying those that contain any of the FCC's "seven dirty words," an activity made possible by the centralized architecture of the Prodigy network. Return to Text

NOTE 12: The general notion of "exit" derives from Hirschman, EXIT, VOICE AND LOYALTY (1970). Return to Text

NOTE 13: I believe that the controversy spawned by recent attempts to define the liability standards that will be applicable to network administrators and system operators in regard to individual instances of defamation, libel, copyright infringement, and the transmission of obscene material, reflects this phenomenon. The few recent court cases that have addressed this issue, e.g., Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y 1991) (holding that a computer service providing subscribers access to an electronic library of news publications independently managed for the service was not liable for defamatory statements made in those publications), and Playboy Enterprises v. Frena, 839 F. Supp. 1552 (M. D. Fl. 1993) (holding that the operator of a computer bulletin board was liable for copyright infringement of magazine photographs uploaded by bulletin board users) have engendered mountains of commentary. See, e.g., Henry H. Perritt, Jr., Tort Liability, the First Amendment, and Equal Access to Electronic Networks, 5 HARV. J. L. &AMP; TECH. 65 (1992); Eric Schclacter, Cyberspace, the Free Market and the Free Marketplace of Ideas: Recognizing Legal Differences in Computer Bulletin Board Functions, 16 HASTINGS COMM/ENT L.J. 87 (1993); Henry H. Perritt, Jr., Metaphors for Understanding Rights and Responsibilities in Network Communities: Print Shops, Barons, Sheriffs, and Bureaucracies

NOTE 14: The literature on the Internet, and specifically Internet architecture, is vast. I have found the following particularly helpful. Henry H. Perritt, Jr., What is the Internet (available at <http://ming.law.vill.edu>); John S. QUARTERMAN, THE MATRIX: COMPUTER NETWORKS AND CONFERENCING SYSTEMS WORLDWIDE (1990); Krol & Hoffman, What is the Internet, Internet Engineering Task Force RFC 1462 (available at <http://ds.internic.org>); Johnson-Laird, The Internet: The Good, the Bad, and the Ugly, Paper presented at the Computer Law Association Annual Meeting, September 29, 1994 (available from the author at andy@jli.portland.or.us; Reinhardt, Building the Data Highway, 19 BYTE 46 (1994). Return to Text

NOTE 15: The development of the medieval law merchant may represent a close historical analogue to the market for rules in cyberspace, inasmuch as it represents an example of unregulated and unconstrained rule-making in the absence of State control. See Hardy, supra note 4, at 1019-1021; Paul R. Milgrom, Douglas C. North, & Barry R. Weingast, The Role of Institutions in the Revival of Trade: The Law Merchant, Private Judges, and the Champagne Fairs, 2 ECON. &amp; POLITICS 1 (1990); Bruce L. Benson, Customary Law as Social Contract, 3 CONST. POL. ECON. 1 (1992). Return to Text

NOTE 16: Imagine, for example, a network in which a "no copyrights will be recognized" rule is declared. Such a rule may be beneficial to all network participants, but may impose costs on non-participants (i.e., individuals who hold intellectual property that has value under other rule-sets but whose value is diminished because of the free copying available to the network participants). Return to Text