Vanderbilt Journal of Entertainment & Technology Law

Volume 2
Issue 1 *Winter 2000*

Article 5

2000

Of Black Holes and Decentralized Law Making in Cyberspace

David G. Post

OF BLACK holes AND DECENTRALIZED LAW-MAKING IN CYBERSPACE

By **David G. Post**

There is, within the (rapidly-growing) community of people who spend their time thinking about law and policy in cyberspace, a rather interesting debate taking place. Though it is not always characterized in these terms, it reflects a conflict between competing visions of "order" and "disorder" in social systems. This is by no means a "new" debate, but it takes on a new shape in the rather special conditions of cyberspace—or so, at least, I hope to suggest in what follows.

The Incident

Last January, Professor Tom Field of the Franklin Pierce Law Center (FPLC), posted the following message to the Cyberprof listserve:[1]

To all:

Assuming that this message isn't screened out by the [the server at the University of Texas that hosts the Cyberprof discussion group], you might be interested in a "small" problem FPLC faces. A few weeks ago, someone "bounced" some spam off our server. It somehow corrupted our email system, and [now] I am beginning to get messages like this:

> *The message that you sent was undeliverable to the following: ipww@ljx.com Transcript of session follows: MAIL FROM: tfield@fplc.edu refused; see http://maps.vix.com/rbl/*

I hope it never happens to you. Meanwhile, any ideas about how to deal with it?[2]

The Explanation

There were, as it turned out, lots of ideas about how to deal with it — but that is getting ahead of myself. First, the facts, as best one can make them out here. Professor Field ("tfield@fplc.edu") had sent an e-mail message to an address at *ljx.com*. But the ljx.com e-mail server had refused to deliver the message to the intended recipient ("Mail From: tfield@fplc.edu refused") and returned it "undelivered" to Professor Field. What had happened? Why had it done so?

The explanation is provided—elliptically, to be sure—by the hyperlink reference ("see http://maps.vix.com/rbl") in the message that Professor Field had received. If you do indeed "see http://maps.vix.com/rbl" you are taken to the home page of something called the Mail Abuse Prevention System (MAPS). MAPS, the primary focus of this tale, is a California non-profit limited liability company.[3] It coordinates a kind of group boycott by Internet service providers (ISPs) for the purpose of reducing the flow of what is commonly called "spam"— unsolicited bulk e-mail. It operates, roughly, as follows.[4] The managers of MAPS create and maintain what they call the "Realtime Blackhole List" (RBL), which consists of a long list of Internet addresses.[5] They place on the RBL any Internet address from which, to their knowledge, spam has originated.[6] They also place on the RBL the address of any network that allows "open-mail relay"[7] or provides "spam support services."[8]

MAPS makes the RBL list available to ISPs and other network administrators on a subscription basis.[9] ISPs that subscribe to the RBL can, if they choose, set their mail handlers to delete all e-mail originating from, and/or going to, an address appearing on the list. That is, when an RBL-subscribing ISP receives a request to transmit e-mail to or from a subscriber, it checks the sender's numeric Internet address against the list of blackholed Internet addresses; if it finds a match, it deletes the message. The blackholed address thus, in a sense, disappears from the Internet as far as the subscribing ISP (and its customers) are concerned.

Apparently, Professor Field's network—*fplc.edu*—had been placed on the RBL—"blackholed —and *ljx.com*, the home server of the intended recipient of Professor Field's e-mail, was an RBL subscriber. When the *ljx.com* mail server received Professor Field's message, it recognized the e-mail as originating from a blackholed address and deleted it, helpfully sending back the message, reproduced above, to Professor Field to inform him what was going on.

The Question

What are we to make of things like the RBL? Here we have a problem—the proliferation of unsolicited mass e-mailing operations—that is, we might agree, a serious, or at least a non-trivial, one. At just the moment that e-mail has become an indispensable form of communication, of incalculable commercial and non-commercial importance for a substantial and ever-growing segment of the world community, its value is being undermined by a barrage of unwanted and unsolicited communications.[10] But is the RBL a reasonable means of addressing this problem? To what extent can we, and should we, rely on things like the RBL to devise a "solution" (however we might define a solution) to that problem?

The Debate

The question is, I think, both an interesting and an important one. Legal scholars have recently discovered—or re-discovered—the important role played by informal systems of decentralized, consensus-based social control in shaping human social behavior.[11] It is becoming increasingly clear that systems of rules and sanctions created and administered without reliance on State "authority," and outside of any formal State-managed process—"norms—are powerful determinants of behavior in many contexts. And what is the RBL if not a textbook example of an informal, decentralized, norm-

creation process? The MAPS operators propose a norm, a description of behavior that they consider, for whatever reason, unacceptable—allowing open mail relay systems, for example, or providing "spam support services."[12] They offer to serve as your agent—or, more accurately, as the agent for your network administrator or ISP—in identifying those who are violating this norm. They offer to keep you informed of those identifications (via the RBL). They propose to sanction norm-violators. The sanction they have in mind is the Ur-Sanction of informal social control processes: shunning. Those who choose to apply the sanction simply turn their backs on offenders, ceasing all (electronic) communication with them. MAPS helpfully provides you with the means to accomplish this sanction—software that will configure your system to delete e-mail to or from blackholed addresses.[13]

This is not, as it were, your father's norm-creation process; it has some unusual features missing from real-space norm-creation processes.[14] But it is norm-creation; whether or not it can helpfully be described as "bottom-up,"[15] it is surely both "informal" and "decentralized." Neither the decision to join (or not join) the group shunning exercise (i.e., to subscribe to the RBL in the first place), nor the shunning sanction imposed on violators of the norm, relies on access to (formal) State-supported enforcement devices or State-imposed legal sanctions,[16] and the decision whether to join that exercise is in the hands of a (relatively large) number of independently-acting agents.[17]

Conditions in cyberspace do seem to create, in Professor Elkin-Koren's words, "new opportunities for voluntary normative regimes" of this kind.[18] Not surprisingly, conflicts between formal and informal, centralized and decentralized, rule-making processes are at the heart of many of the important and challenging cyberspace policy debates. The extraordinary current turmoil in the domain name allocation system is one illustration. The story has been told in detail elsewhere.[19] Briefly, in the beginning—before the Internet became such a Big Deal—responsibility for operating the machines, and the databases on those machines, that correctly route Internet messages fell to the Internet Assigned Number Authority (IANA), an imposing-sounding entity that, in reality, consisted of a small number of dedicated volunteers in southern California. As the Internet began its explosive growth, IANA's ability to maintain the system became increasingly overloaded; beginning in 1993, responsibility for maintaining these databases –at least, for three of the increasingly popular "generic top-level" domains—*.com, *.net, *.org and the like—was handed over to a private firm, Network Solutions, Inc., under a contract—styled a "Cooperative Agreement"—funded by the U.S. government (first through the National Science Foundation, later through the Commerce Department's National Telecommunications and Information Administration).

When that cooperative agreement was due to expire in 1998, the Commerce Department had a decision to make. It could simply walk away from the relationship on the stated expiration date, which is ordinarily what happens when cooperative agreements (or any government contracts) expire. It rejected that option, however, taking the position that it would be "irresponsible to withdraw from its existing management role [in the domain name system] without taking steps to ensure the stability of the Internet."[20] The Internet naming system, it concluded, needed a "more formal and robust management structure," and it called for the creation of a new, not-for-profit corporation formed by the "Internet stakeholders" themselves to manage the domain name system.[21] Shortly thereafter, control of this system was placed in the hands of a single institution — now known as ICANN, the Internet Corporation for Assigned Names and Numbers—which would have overall responsibility for setting the rules under which the domain name system would henceforth operate. Putting aside whatever one might think of this decision (or the manner in which ICANN has fulfilled its responsibilities[22]), the decision to centralize authority over this system in a single, government-authorized entity will inevitably have deep implications for the Internet as a whole.

The debate over the normative implications of these informal processes has become a lively one indeed. In one corner are commentators, myself included, who find these systems normatively attractive, on both "legitimacy and "efficiency" grounds.[23] Legitimacy justifications rest on the view that informal private ordering schemes like the RBL are a "superior alternative to centralized government models in that [they are] the most consistent with autonomy and freedom."[24] By these lights, MAPS is normatively attractive inasmuch as it constrains individuals' behavior only to the extent, and precisely to the extent, that others share MAPS' views on the definition of wrongdoing, the choice of appropriate sanction, the identity of the wrongdoers, etc; the MAPS operators can persuade, cajole, and beg the thousands of ISPs to sub-

scribe to the RBL, but they cannot force them to do so in any meaningful sense of that term. Efficiency justifications rest on the extraordinary power of decentralized systems to generate, by means of repeated trial-and-error and the pull-and-tug of competing rules and counter-rules, solutions to complex problems that can be found no other way.[25]

Others disagree, both with particular reference to institutions like the RBL[26] and in general,[27] arguing both that the efficiency benefits of these cyberspace norm-creation processes are overblown and that such processes systematically exclude "public values" from being incorporated into the norms they generate.

It is a rich debate that will, I suspect, be one of the enduring legacies of the study of the law of cyberspace. I want to put aside, for purposes of this essay, the many difficult, even profound, substantive questions raised in this debate, in order to focus a little attention instead on the meta-debate, on questions about the ways in which the substantive questions themselves can be explored and evaluated.

> [C]onflicts between formal and informal, centralized and decentralized, rule-making processes are at the heart of many of the important and challenging cyberspace policy debates.

We like to think, at least at a conceptual level, that we conduct this debate by placing decentralized rule-making processes (like the RBL) on the table, dissecting their features, and comparing them, on whatever normative or descriptive criteria we choose, with alternative processes. But there are serious impediments to our ability to do that, impediments that skew the inquiry into the virtues (or lack thereof) of decentralized processes. Let me try to explain the sorts of things I have in mind.

First, I would suggest that *we understand little—far less than we need to—about the processes of self-ordering and informal coordination.* The rise of the Internet itself shows us, I think, how little we know about the ways that decentralized, trial-and-error, consensual processes can build stable structures of literally unimaginable complexity and power. If cyberspace did not exist, we would all probably agree that it could not exist. How, after all, would we go about building something as ridiculously complex as a single interconnected global communications network? Who would we place in charge of such a project? How would we solve the seemingly impossible coordination problem facing anyone trying to construct that global network—constructing, and getting large numbers of people to adopt, what amounts to a single global language?[28]

Of course, we did, somehow, solve it, without any "authority" in charge of bringing it into being, in a remarkably short period of time, and to the surprise of virtually everyone.[29] A decentralized process of developing consensus among larger and larger numbers of geographically-dispersed individuals somehow managed to get us here. Emergent institutions like the Internet Engineering Task Force[30] (whose motto, "We reject Kings, Presidents, and voting; we seek rough consensus and working code," aptly captures its decentralized orientation), the World Wide Web Consortium[31], the Internet Assigned Numbering Authority[32], and the like—institutions with *no authority whatsoever* to act on anyone's behalf, no fixed address or membership, no formal legal existence—somehow got hundreds of millions of individuals across the globe to agree on a common syntax for their electronic conversations. The protocols of the global network, like the natural languages they so closely resemble, emerged from a process that was at its core unplanned and undirected. Though we can certainly point *ex post* to many individuals and institutions who played particularly important roles in its emergence, *ex ante* there was no one we could have pointed to as charged with "creating" the set of rules we now know as the Internet, any more than we can point to any one individual or institution charged with creating the set of rules for English syntax.

Could it have been built any other way? My instinct is that it could not have, that only an "authority-free"

process of this kind could have constructed this system, that *no one with the authority to build the Internet could have done so.*[33] If I'm right, this is of considerable importance to the normative debate, for it obliterates the distinction between the normative and the descriptive aspects of the debate; if we were trying, circa 1965, to find the "best" way of constructing the protocols for the Internet, we would not lay alternative centralized and decentralized decision-making models side-by-side for comparison, for there would be no centralized model to examine that could accomplish the task. But this is, I admit, just instinct; I do not know of any analytic vocabulary or framework within which I could make that argument. Even if my instinct is correct, how would we have known that in 1965? How would we know it now?

Second, and relatedly, I believe that *conditions in cyberspace make it difficult to specify the alternative processes with which decentralized processes are to be compared as part of this policy calculus.* No one, of course, suggests that decentralized processes like the one of which the RBL is a part constitute rule-making Nirvana. The relevant normative question is always whether processes of this kind are better—*however* one chooses to define "better"—than available alternatives.[34]

> The decentralized process that built the Internet protocols and the domain name system cannot, *ex ante*, "ensur[e] the stability of the Internet."

We need, in other words, to be debating whether the process of which RBL is a part is better than—than what? As I look over the contributions to this debate I'm not always sure I can fill in that blank. Some of this is mere rhetorical device; it is always tempting to seize the rhetorical high ground by demonstrating the substantial distance between an opponent's position and perfection itself.[35] But there is a deeper problem here. Cyberspace is particularly, and genuinely, tricky on this score. What *are* the alternative rule-making processes or institutions that should be placed on the analytic table alongside the RBL? The problems posed by the borderless features of this new medium for traditional rule-making institutions, faced with the problem of mapping territorially-based legal regimes onto a medium in which physical location is of little significance, have long since passed into cliche; but that doesn't mean that they are not real problems. Whose rules regarding spam should we be comparing to MAPS'? The Virginia legislature's[36]? The United States Congress'[37]? The International Telecommunications Union's? UNESCO's? ICANN's?

The task of identifying the alternative rule-makers for purposes of normative comparison is made even more difficult than this because cyberspace, having emerged from decentralized disorder—from the primordial ooze of the Internet Engineering Task Force — may well create conditions that favor the growth of powerful *centralizing* forces.[38] The State of Virginia will soon discover that its anti-spam statute has little effect on the amount of spam that its citizens receive, because while spam originating anywhere on the network can easily make its way into Virginia, spam originating elsewhere—i.e., outside of Virginia's borders—is largely immune to Virginia's control.[39] The same will be true in regard to a federal anti-spam statute (if such a statute is enacted), just on a grander scale. We can already write the headline: "Use of Offshore E-Mail Servers Hinders Enforcement of Federal Spam Statute; Government Calls for International Cooperation to Solve 'Serious Problem.'" We will, inevitably (and, since we're on Internet Time, sooner than we think), hear calls for "international harmonization" of spam regulation, replicating the pattern currently spreading across the cyberspace legal spectrum. How can we factor *this* into the normative comparisons we are trying to make?

Third and finally, if all this weren't confusing enough, *decentralized processes are fundamentally, and irreducibly, unpredictable.* No one can say *ex ante* what kind of anti-spam rules will emerge from the RBL process, or how the domain name allocation system would today be operating had the Commerce Department chosen to step aside in 1998, because *that information does not exist unless and until the process itself generates it.* No one can say whether MAPS' initiative will, or will not, cause open

mail relay systems to disappear, because that depends upon the response of thousands of individual system administrators; no one can say whether alternative and as yet untried and perhaps unthought-of means of deterring spammers will prove more popular than MAPS; no one can say how spammers will react to the absence of open-mail relay (or to these other alternatives) or how the anti-spammers will react to those reactions, etc.

Because we can not see, or imagine, where the RBL might take us—the rule(s) of spamming that the RBL and its variants could produce—we cannot lay these rules side-by-side with their centralized alternatives for purposes of analysis, deliberation, and debate. Our analytic table contains only, as it were, the bad news: the inherently disordered and aggravating messiness of decentralized processes, mail that doesn't reach its intended destination, disruptions of service, and the like.

It all makes for an apparently simple policy choice: order versus chaos. During all of the discussions—which can only be described as "frenzied"—leading up to the decision to grant ICANN the authority to manage the domain name system, I was continually struck by the impossibility of discussing rationally the course of action whereby the government would just walk away from the entire thing. The Commerce Department set forth a number of principles to guide its decision; the domain name system should "support competition and consumer choice," "reflect, as far as possible, the bottom-up governance that has characterized development of the Internet to date," and "reflect the diversity of [the Internet's] users and their needs" by "ensur[ing] international input in decision making."[40] But one principle was *primus inter pares*:

> The U.S. government should end its role in the Internet number and name address systems in a responsible manner. This means, *above all else, ensuring the stability of the Internet.* The Internet functions well today, but its current technical management is probably not viable over the long term. We should not wait for it to break down before acting. Yet, we should not move so quickly, or depart so radically from the existing structures, that we disrupt the functioning of the Internet. The introduction of a new system should not disrupt current operations, or create competing root systems.[41]

The decentralized process that built the Internet protocols and the domain name system cannot, *ex ante*, "ensur[e] the stability of the Internet." If that is indeed the goal, that option is off the table. Because there is no way to answer the question "What kind of domain name system would we have today had the Commerce Department stepped aside in 1998?," that course of action could not be taken seriously.

My fear is that this leads to a policy-making catastrophe of significant proportions. A "stable" Internet is one locked in place, incapable of generating innovative responses to the very problems that it is itself bringing into existence. The very existence of the Internet should caution us against dismissing too quickly the notion that there are some problems that are best solved by these messy, disordered, semi-chaotic, unplanned, decentralized systems, and that the costs that necessarily accompany such unplanned disorder may sometimes be worth bearing.[42] But which problems? How can we know? ◆

Postd@erols.com: An earlier version of this paper was originally presented at the Yale Information Society Project Conference on "Private Censorship/Perfect Choice," April 9, 1999. Thanks to Bill Scheinler for research assistance, and to the Temple Law School summer research grant fund for support in completing this paper.

---

1 Cyberprof is a listserve discussion group moderated by Professor Mark Lemley of the University of California-Berkeley.

2 E-mail from Tom Field, Professor, Franklin Pierce Law Center, to Cyberprof Discussion Group, Jan. 28, 1999 (thanks to Professor Field for his permission to quote the message here) (copy on file with the author).

3 See Robert McMillan, *What Will Stop Spam?* (last modified Nov. 20, 1999) <http://www.sunworld.com/sunworldonline/swol-12-1997/swol-12-vixie.html>. See generally *Mail Abuse Prevention System* (visited Nov. 19, 1999) <http://mail-abuse.org>; *Maps Realtime Blackhole List* (visited Nov. 19, 1999) <http://maps.vix.com/rbl>.

4 See generally, *Mail Abuse, supra* note 3.

5 The RBL currently has approximately 1,400 entries. E-mail from Nick Nicholas, Executive Director, Mail Abuse Prevention System, to David G. Post (Oct. 6, 1999) (on file with author). Most of these entries consist of only a single numeric Internet address; some, however, consist of the address of what is commonly called a "Class C" network, which itself contains 255 individual addresses. See Paul Vixie, *MAPS RBL Candidacy* (visited Nov. 19, 1999) <http://maps.vix.com/rbl/candidacy.html>.

6 See Vixie, *supra* note 5. Removal from the list requires a showing by the blackholed address, or the appropriate network administrator, that the spammer is no longer at the address in question and/or that a stronger "Terms of Use" agreement has been put in place for the network on which the spammer was located. Id.

7 "Open-mail relay" refers to a practice whereby Internet mail servers process and transmit e-mail messages in circumstances in which neither the sender nor the recipient is an authenticated local user; that is, it allows "strangers" to access its mail handling facilities. Spammers, apparently, utilize open-mail relay sites to "launder" their e-mail; by using an open relay, their e-mail will appear to have originated from a source other than the true source, thereby making it difficult to trace or filter the messages. See *Better Network Security Through Peer Pressure: Stopping Smurf and Spam* (visited May 31, 1999) <http://securityportal.com/cover/coverstory19990531.html>; Paul Hoffman, *Allowing Relaying in SMTP: A Series of Surveys* (visited Nov. 19, 1999) <http://www.imc.org/ube-relay.html>; Chip Rosenthal, *MAPS TSI: Anti-Relay: What is Third-Party Mail Relay?* (visited July 31, 1999) <http://maps.vix.com/tsi/ar-what.html>; Vixie, *supra* note 5.

8 MAPS includes in this category such activities as hosting web pages that are listed as destination addresses in bulk e-mail, or providing e-mail forwarders or auto-responders that can be used by bulk e-mailers. See Vixie, *supra* note 5.

9 There is currently no charge to subscribe to the RBL. See Nick Nicholas & Chip Rosenthal, *MAPS RBL Participants* (visited Nov. 19, 1999) <http://maps.vix.com/rbl/participants.html>. The RBL currently has over 180 registered subscribers who receive full, frequently updated copies of the RBL for storage and use on their own routers and servers. These subscribers are required to execute a license agreement with MAPS, the terms of which are not publicly available. Id. In addition, there are "several thousand" other users who either receive the RBL via "EBGP4 Multi-Hop," a protocol used by routers on the Internet, or through direct queries on specific numeric Internet address to MAPS' RBL servers. Id.

10 Some have suggested — plausibly — that the explosion of mass e-mail is undermining the viability and even the existence of many open discussion forums (in particular, many Usenet newsgroups) — one of the Internet's earliest and most remarkable innovations. See Paul K. Ohm, Comment, *On Regulating the Internet: Usenet, A Case Study*, 46 UCLA L. REV. 1941, 1951 (1999) (noting that spam causes a dramatic decrease in Usenet's "signal-to-noise" ratio and is therefore considered a "major threat" to [Usenet's] continued popularity).

11 See generally, ROBERT ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES (1991) (arguably the start of the rejuvenation of the study of norms within legal scholarship.) The Symposium on *Law, Economics, and Norms,* 144 U. PA. L. REV. 1643 (1996), maps out much of the recent terrain.

12 MAPS provides an extensive rationale for its proposed norms. See Paul Vixie, *Our Rationale for the MAPS RBL* (last modified July 12, 1999) <http://maps.vix.com/rbl/rationale.html>.

13 The RBL has apparently become popular enough that many of the vendors of the most popular mail server configuration software provide support for RBL implementation in their products. See Paul Vixie, (visited Jan. 5, 2000) <http://maps.vix.com/rbl/usage.html>.

14 The implementation *in software* of this particular norm is surely an unusual feature of this process that has no clear analogue in real-space norm-creation schemes. Enforcement of norms by code is, as Professor Lessig has demonstrated, a large, and a most fundamental change. See LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999). Cyberspace, in Lessig's words,

> . . . demands a new understanding of how regulation works and of what regulates life there. It compels us to look beyond the traditional lawyer's scope — beyond laws, regulations, and norms. . . . In cyberspace we must understand how code regulates — how the software and hardware that make cyberspace what it is *regulate* cyberspace as it is. As William Mitchell puts it, this code is cyberspace's "law." *Code is law.*

Id. at 6 (emphasis in original).

15 Margaret Radin and R. Polk Wagner criticize what they describe as a "false dichotomy" between characterizations of "top-down" and "bottom-up" ordering. See Margaret Radin & R. Polk Wagner, *The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace*, 73 CHI.-KENT L. REV. 1295, 1297 (1998). Any rule-making regime, they suggest, "can be characterized as either [top-down or bottom-up], depending upon how you look at it." Id. at 1298. The point is an important one; rule-making processes are always top-down when seen from one level of the hierarchy of social institutions and bottom-up when seen from a different level. MAPS's decision-making process is top-down from the perspective of, say, the MAPS webmaster, who receives from " higher up" a list of sites to put on, or take off, the RBL each morning. This top-down process is simultaneously a component of a bottom-up process from the perspective of someone looking at the responses of the Internet community as a whole to the proliferation of commercial e-mail. This is a feature of all networks (including social networks) consisting of embedded hierarchies; any element in the network is simultaneously at the top of some hierarchy(ies) and at the bottom of others. See David G. Post & Michael B. Eisen, *How Long is the Coastline of the Law? Thoughts on the Fractal Nature of Legal Systems*, 29 J.L.S. 545 (2000) (describing this "dizzying" characteristic of embedded hierarchies as a consequence of their fractal structure).

16 You are not, in other words, subject to any sanction enforced through the formal State-created processes if you choose to join, or not to join, the MAPS exercise. If for any reason you do not approve of MAPS' particular definition of unacceptable behavior, their choice of sanction, the means they have chosen to implement that sanction, or their method of detecting violators subject to the sanction, you can ignore them (or, if you'd like, to propose your own). MAPS can persuade, cajole, and beg the thousands of ISPs out there to join the group of RBL subscribers, but it cannot use State-sanctioned force to get them to do so.

17 Professor Elkin-Koren defines "decentralized" norm-creation processes as those in which the "power to create and shape . . . rules is not concentrated in the hands of any individual group, or institution [and which is] spread among various social agents." Niva Elkin-Koren, *Copyrights in Cyberspace – Rights Without Laws?*, 73 CHI.-KENT L. REV. 1155, 1161 (1998). As of June, 1999, there were over 6,000 ISPs in the United States alone offering Internet connectivity, See Jason Oxman, *The FCC and the Unregulation of the Internet*, FCC Office of Plans and Policy Working Paper No. 31 (last modified July, 1999) <http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp31.pdf>, and countless other network administrators in a position to subscribe (or not) to the RBL.

18 Elkin-Koren, *supra* note 17, at 1161-62 (Cyberspace "significantly reduces the costs of communicating and collecting information regarding individuals' preferences. It also facilitates fast and cost-effective information processing that allows real-time feedback on public preferences and choices. Cyberspace, thus, opens up opportunities for effective participation of individuals in defining the rules.").

19 See A. Michael Froomkin, *Of Governments and Governance*, 14 BERKELEY TECH. L.J. 617 (1999); Milton L. Mueller, *Internet Domain Names: Privatization, Competition, and Freedom of Expression*, Cato

Briefing Paper No. 33 (last modified October 16, 1997) <http://www.cato.org/pubs/briefs/bp-033.html>; Jon Weinberg, *Testimony of Jon Weinberg, Professor of Law, Wayne State University before the U.S. House of Representatives Commerce Committee, Subcommittee on Oversight and Investigations, "Domain Name System Privatization: Is ICANN Out of Control?"* (last modified July 22, 1999) <http://www.law.wayne.edu/weinberg/testimony.pdf>. The Department of Commerce's "White Paper," *Management of Internet Names and Addresses* (visited January 24, 2000) <http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm>, has a comprehensive summary of the history of domain name and number administration on the Internet.

20 See Department of Commerce, *supra* note 19.

21 Id.

22 My own views have been set forth at length elsewhere. See David G. Post, *Governing Cyberspace: Where is James Madison when we need him?*(last modified June 6, 1999) <http://www.icannwatch.org/archives/essays/930604982.shtml>; David G. Post, *Elusive Consensus* (last modified July 21, 1999) <http://www.icannwatch.org/archives/essays/932565188.shtml>; David G. Post, *ICANN and Independent Review* (last modified Aug. 1999) <http://www.icannwatch.org/reviewpanel/index.shtml>; David G. Post, *Cyberspace's Constitutional Moment*, THE AMERICAN LAWYER, Nov. 1998, at 117.

23 See, e.g., Tom W. Bell, *Fair Use v. Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine*, 76 N.C. L. REV. 557 (1998); Llewellyn Joseph Gibbons, *No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace*, 6 CORNELL J. L. & PUB. POL'Y 475 (1997); I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. PITT. L. REV. 993, 995-96 (1994); Maureen A. O'Rourke, *Copyright Preemption After the ProCD Case: A Market-Based Approach*, 12 BERKELEY TECH. L. J. 53, 80 (1997); David Post & David R. Johnson, *And How Shall the Net Be Governed? A Meditation on the Relative Virtues of Decentralized, Emergent Law, in* COORDINATING THE INTERNET, (Brian Kahin & James Keller eds., 1997); David G. Post & David R. Johnson, *"Chaos Prevailing on Every Continent:" Towards a New Theory of Decentralized Decision-Making in Complex Systems*, 73 CHI.-KENT. L. REV. 1055 (1998); David R. Johnson & David G. Post, *The New Civic Virtue of the Internet: Lessons from a Model of Complex Systems for the Governance of Cyberspace, in* THE EMERGING INTERNET (1998 Annual Review of the Institute for InformationStudies) (C. Firestone ed., 1998). The distinction between the "legitimacy" and "efficiency" justifications for decentralized Internet rule-making comes from Elkin-Koren, *supra* note 17, at 1166-79.

24 Elkin-Koren, *supra* note 17, at 1172.

25 Decentralized decision-making processes, in the language of complexity theory, are powerful algorithms for finding "high points on the fitness landscape" (i.e., solutions to problems defined over complex, interdependent spaces). See Post, *Chaos Prevailing on Every Continent, supra* note 23, at 1081-86. The problem-solving power of decentralized systems is well-documented and reasonably non-controversial in mathematical, physical, and biological systems, underlying phenomena as diverse as parallel processing algorithms in computational mathematics and natural selection in the design of living things. See id. at 1083-1093.

26 Professor Lessig has written, in discussing the "spam wars," that:

> . . . these battles [between spammers and anti-spammers] will not go away. The power of the vigilantes will no doubt increase, as they hold out the ever-more-appealing promise of a world without spam. But the conflicts with these vigilantes will increase as well. Network service providers will struggle with antispam activists even as activists struggle with spam.
>
> There's something wrong with this picture. This policy question will fundamentally affect the architecture of e-mail. The ideal solution would involve a mix of rules about spam and code to implement the rules. . . .
>
> Certainly, spam is an issue. But the real problem is that vigilantes and network service providers are deciding fundamental policy questions about how the Net will work — each group from its own perspective.
>
> This is policy-making by the "invisible hand." It's not that policy is not being made, but that those making the policy are unaccountable. . . . Is this how network policy should be made?
>
> *The answer is obvious, even if the solution is not.*

Lawrence Lessig, *The Spam Wars* (last modified Dec. 31, 1998) <http://www.thestandard.com/articles/display/0,1449,3006,00.html> (emphasis added). This view — not only that we should not rely on the interplay [a misnomer, perhaps] between spammers and anti-spammers to make "network policy," but that it is "obvious" that we should not do so — seems to be widely shared. In the course of the most enlightening discussion of these questions on the Cyberprof listserve, skepticism about bottom-up processes in general, and certainly about the RBL, was widespread. *Cyberprof Listserve* (selected postings Jan. 29-30, 1999) (copies on file with author). For example:

> These private blacklists — however virtuous the maintainers might be — are a perfect example, in my humble opinion, of where bottom up doesn't work. The externality from this boycott is huge. Yet there is no body that can reckon that externality.
>
> [My company] fell victim to [the RBL] during last summer. Given the nature of our proprietary architecture, making the fixes they wanted wasn't an option. While they eventually were forced to acknowledge this, we were blackholed for an unacceptable period of time while we tried to make them understand why we couldn't comply. The lack of formal process on their end seriously hampered our ability to get them to understand. Many of our customers had major problems arise during that time period because they couldn't use our service to get mail out to users on ISP who subscribed to the Vixie list.
>
> The average RBL'd site with an open mail relay is like a neighbor who allows members of the public open access to his yard, whence they deposit all sorts of trash into *my* yard. . . . Why can't I allow access to my yard without fear that some members of the public will abuse it to litter both mine and my neighbors' yards? Moreover, I wonder how many generations of locks and lock pickers we have yet to endure. Something is amiss in this let-it-all-hang-out picture.

Professor Field himself, it might be noted, shared this skepticism:

> I regard email as a tool, not a career. I appreciate that some are otherwise inclined, but neither I nor many other people are interested in its history and arcana. My point was and remains: Public policy should not require them to delve deeply to send a simple message and avoid

what amounts to vandalism and vigilante responses thereto.

See also Jon Swartz, *Anti-Spam Service or McCarthyism? Internet Group Puts Some ISPs on a Blacklist* (last modified May 10, 1999) <http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/1999/05/10/BU76824.DTL> (describing MAPS' activities as a sort of "Cyber-McCarthyism").

27 Three of the contributions to the recent symposium on "The Internet and Legal Theory" focused on the deficiencies of informal Internet rule-making systems. See Elkin-Koren, *supra* note 17; Mark. A. Lemley, *The Law and Economics of Internet Norms*, 73 CHI.-KENT L. REV. 1257 (1998); Margaret Radin & R. Polk Wagner, *supra* note 15. See also LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

28 The Internet is, at bottom, that language, the set of grammatical rules (the "Internet protocols" and related transmission and communication standards) that allow machines to exchange information with one another. Lawrence Lessig, *Open Code and Open Societies: Values of Internet Governance* (last modified May 11, 1999) <http://cyber.law.harvard.edu/works/lessig/kent.pdf>; David G. Post, *What Larry Doesn't Get: A Libertarian Response to Lessig's "Code and Other Laws of Cyberspace,"* STAN. L. REV. (forthcoming).

29 See "The Death of Distance," THE ECONOMIST, Sept. 30, 1995, at 35 (probably the best general description of the striking inability of politicians, social theorists, and even some very savvy players within the computer industry itself to predict *ex ante* the emergence and growth of this medium).

30 *Internet Engineering Task Force* (visited Nov. 18, 1999) <http://www.ietf.org>.

31 *World Wide Web Consortium* (visited Nov. 18, 1999) <http://www.w3.org>.

32 *Internet Assigned Number Authority* (visited Nov. 18, 1999) <http://www.iana.org>.

33 The failure of the "official" standard-setting bodies – the International Organization for Standardization (ISO) and the International Telegraph and Telephone Consultative Committee (CCITT) (now the International Telecommunications Union (ITU)) — to gain acceptance for their OSI internet working protocols is a nice case in point. See KATIE HAFNER & MICHAEL LYON, WHERE WIZARDS STAY UP LATE: THE ORIGINS OF THE INTERNET 246 - 251 (1996) (describing the battle between the OSI protocols and the ultimately-triumphant-and-dare-I-call-it-bottom-up TCP/IP protocols); Peter Salus, *Protocol Wars: Is OSI Finally Dead?*, 6 Connexions 16 (1995). See also John Lamouth, *Understanding OSI* (last modified Nov. 11, 1997) <http://www.salford.ac.uk/iti/books/osi/osi.html>; *OSI* (last modified May 16, 1998) <http://webopedia.internet.com/Standards/Networking_Standards/OSI.html>. But one data point does not a theory make.

34 See Elkin-Koren, *supra* note 17, at 1188 ("private ordering should not be examined in the abstract, but rather in comparison to its alternatives"); Lemley, *supra* note 27, at 1261 (noting, by implication, the difficulties of analyzing questions of "comparative institutional governance").

35 This is a common enough technique to have its own name: the "Nirvana Fallacy." See, e.g., Harold Demsetz, *Information and Efficiency: Another Viewpoint*, 12 J. L. & ECON. 1 (1969).

36 The John Marshall Law School maintains a useful database of state efforts to curb unsolicited bulk e-mail. See (last modified Mar. 5, 1999) <http://www.jmls.edu/cyber/statutes/email/state.html>. In 1998, for example, Virginia amended its computer trespass statute to provide that it is unlawful to "[f]alsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk electronic mail through or into the computer network of an electronic mail service provider or its subscribers." VA. CODE ANN.§ 18.2-152.4 (Michie 1999).

37 Numerous bills to regulate or proscribe certain types of e-mail were introduced in the 106th Congress alone, including: *Unsolicited Mail Act of 1999*, H.R. 3113, 106th Cong. (1999); *Can Spam Act*, H.R. 2162, 106th Cong. (1999); *E-Mail User Protection Act*, H.R. 1910, 106th Cong. (1999); *Inbox Privacy Act of 1999*, S. 759, 106th Cong. (1999); and *Telemarketing Fraud and Seniors Protection Act*, S. 699, 106th Cong. (1999) and its House counterpart, *Protection Against Scams on Seniors Act of 1999*, H.R. 612, 106th Cong. (1999).

38 See LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 206 (1999):

> Just as there was a push toward convergence on a simple set of network protocols, there will be a push toward convergence on a uniform set of rules to govern network transactions. This set of rules will include not the law of trademark that many nations have, but a unified system of trademark, enforced by a single committee [citation omitted]; not a diverse set of policies governing privacy, but a single set of rules, implicit in the architecture of Internet protocols; not a range of contract law policies, implemented in different ways according to the values of different states, but a single, implicit set of rules decided through click-wrap agreements and enforced where the agreement says.

See also David G. Post, *Governing Cyberspace*, 43 WAYNE L. REV. 155, 163-64 (1997).

39 That is, I realize, a somewhat controversial claim. See A. Michael Froomkin, *The Internet as a Source of Regulatory Arbitrage, in* BORDERS IN CYBERSPACE: INFORMATION POLICY AND THE GLOBAL INFORMATION INFRASTRUCTURE (Brian Kahin & Charles Nesson eds., 1997) (available at <http://www.law.miami.edu/~froomkin/articles/arbitr.htm>); Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998). Doctrinal impediments to Virginia's assertion of extraterritorial jurisdiction over out-of-boundary spammers includes the Commerce Clause, see American Library Ass'n v. Pataki, 969 F. Supp. 160, 161 (S.D.N.Y. 1997), and limitations on Virginia's "jurisdiction to prescribe" extraterritorially and limitations on the Virginia courts' ability to exercise personal jurisdiction over persons and entities residing elsewhere; even Professor Goldsmith, the most forceful critic of the notion that there are such impediments, agrees that in both the domestic and international arenas the "enforceable scope" of any jurisdiction's laws is "relatively narrow," extending "only to individual users or system operators with presence or assets in the enforcement jurisdiction." Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1220 (1998).

40 Department of Commerce, *supra* note 19.

41 Id.

42 Virginia Postrel captures an important dimension of this battle between those of different faiths regarding these matters in her discussion of the difference between "dynamists" and "stasists." See VIRGINIA I. POSTREL, THE FUTURE AND ITS ENEMIES: THE GROWING CONFLICT OVER CREATIVITY, ENTERPRISE, AND PROGRESS (1998).