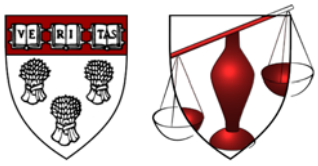

Submission to the Workshop on Internet Governance
February 26 – 27, 2004

John G. Palfrey, Jr.
Executive Director
Berkman Center for Internet and Society
Harvard Law School

This submission is based largely upon a co-authored working paper,
"The Accountable Net,"
by David R. Johnson, Susan P. Crawford, and John G. Palfrey, Jr.

International Telecommunications Union
Geneva, Switzerland

Summary and Background for "The Accountable Net"

This submission introduces the notion of peer production of governance, to which sovereigns ought to defer in instances where it can work. Only as a second option should we turn to a more centralized mode of governance, in which event meaningful public participation and the enfranchisement of individuals in developing countries ought to be first-order priorities.

We have been called, by the World Summit on the Information Society (WSIS) Action Plan, "to investigate and make proposals for action, as appropriate, on the governance of Internet by 2005." This submission addresses some of the public policy questions raised by this hard and, to date, intractable question.

Scope: Determine when (not if) Net governance is needed.

We have moved past the debate of the late 1990s about whether the Net can or should be governed. We acknowledge at the outset that traditional sovereigns can and should play an important role in regulating many actions and actors that affect the internet. There are collective action problems that arise on the global, unitary, public network of networks that we call the Internet that require some form of governance to resolve. Some problems that plainly call for some form of governance include, but are not necessarily limited to, spam, identity theft, network security, and certain aspects of technical coordination of the network. Our job – a hard one, to be sure – is to determine what the most pressing of problems are, and not to insist upon global governance schemes where they are not needed. We should not default to a single global Internet governance scheme. This scoping question is critical to get right as a threshold matter.[1]

Framework: Use the most wise, fair and effective form of governance for any given issue.

For those problems on the Net where some form of governance is required, we ought to test a series of possible schemes of governance to determine which scheme is the most wise, fair and effective. We are unlikely to conclude that a single mode of governance is the most wise, fair and effective means of resolving every difficult problem on the Net. Among others, Karl Auerbach has directed our attention to this issue in the second of his submissions[2] to this conference, in which he highlights the need for "Tailoring the Mode of Governance To The Matter Needing To Be Governed." We ought to be open to disaggregation of Net governance – the notion that certain problems will call for different forms of governance. We ought also to consider ways in which peers, or groups of peers, may be able to produce effective forms of governance for some problems that crop up on the Net.

Principle: Individual choice, participation, and diversity are paramount.

We should start with the premise that the individuals ought to have a reliable means of participation in any scheme of governance of the Internet that we develop or that otherwise emerges. If a governance scheme can drive choice to the individual level and if peers can produce their own system of governance, sovereigns ought to defer to this peer production of governance. Where peer production of governance is not the most wise, fair and effective mode of governance, any sovereign empowered to make and enforce rules must be accountable to those who defer to and grant that sovereign its authority.[3]

---

[1] Don MacLean's background paper for this workshop, "Herding Schrodinger's Cats: Some Conceptual Tools for Thinking about Internet Governance," provides some very helpful tools for this scoping exercise, grounded squarely in the discussion at the first WSIS meeting's documents.

[2] Karl Auerbach, "Governing the Internet: A Functional Approach." (Background paper to this workshop.)

[3] Consider, for instance, Vittorio Bertola, "End User Involvement in Internet Governance: Why and How." (Background paper to this workshop.)

Principle: Any governance scheme must enfranchise individuals in developing countries.

Our consideration of Internet governance schemes must build in from the start – not as a tack-on at the end of a long process – a conscious effort to give adequate voice (and, only if necessary, votes) to individuals in the developing world. We should learn from the abject failures of many of our early efforts to enfranchise developing countries in the Internet decision-making context. The empowerment of individuals in developing countries in a manner that corresponds to the empowerment of individuals in more developed countries should be a core tenet of any Net governance scheme.

Conclusion: Sovereigns should defer to peer production of governance where it can work.

In the context of an accountable internet – in which individuals connect only with those who have shown they are worthy of trust – the peer production of governance can address some of the toughest internet governance problem. This accountable internet is emerging through authentication and accreditation technologies and other phenomena of life on the Net. We should consciously build into the accountable internet the safeguards necessary to preserve the values that we hold dear.

Conclusion: Where a centralized group must be given the right to tell others what to do, meaningful public participation – in the form of votes or voice – and recourse against the decision-maker must be assured.

The accountable net means not only that peers are accountable to one another, but that any sovereign is accountable to those by whom it been granted power to make and enforce rules. Despite significant experimentation in this regard, no effective means of ensuring such accountability – and, correspondingly, legitimacy in the sovereign entity – has yet emerged in the Internet governance space.

THE ACCOUNTABLE NET:
PEER PRODUCTION OF INTERNET GOVERNANCE

By David R. Johnson,[4] Susan P. Crawford,[5] and John G. Palfrey, Jr.[6,7]

I. INTRODUCTION

At the first World Summit on the Information Society (WSIS) meeting, held in Geneva in December 2003, some countries called for the creation of an international government for the internet.[8] Others suggested that there is already a *de facto* online sovereign, the United States, and decried this state of affairs.[9] Even those developed countries that opposed the creation of new international institutions to govern the net seemed to agree that the days of a virtual "wild west" should be over. Some called for the creation of novel public-private partnerships -- new types of private sector institutions (like the Internet Corporation for Assigned Names and Numbers) with new powers to control online wrongdoing. Most at WSIS seemed to agree that some new sheriff is coming to cybertown and should be welcome.

We think the internet will become more orderly over time, but we do not agree that the internet needs, or will easily yield to, more centralized authority -- private or public. To the contrary, we believe a new kind of online social order will emerge as the result of new technologies that enable a more powerful form of decentralized decision-making. These technologies will give private actors greater control over their digital connections. They will enable both end users and access providers to establish connections based on trust, rather than connecting by default to every other network node and trying to filter out harmful messages after the connection has been made. Because of these new developments, participants on the internet will be more accountable to one another than they have been in the past.

Several years ago, there was much discussion about the question whether the internet, as a general rule, lends itself to regulation by traditional governments, or whether, in contrast, some aspects of the internet's architecture systematically resist such control or enable the development of new kinds of law.[10] We do not seek to reopen that debate, acknowledging at the outset that traditional sovereigns can and should play an important role in regulating many actions and actors that affect the internet. Rather, we seek to look more closely at a series of particularly thorny issues that have proven especially challenging for policy makers seeking to impose governance by local states on a new global medium.

---

[4] Distinguished Visiting Practitioner, New York Law School.
[5] Assistant Professor, Cardozo School of Law; Policy Fellow, Center for Democracy & Technology.
[6] Executive Director & Lecturer on Law, The Berkman Center for Internet & Society at Harvard Law School.
[7] This paper had its genesis at an Aspen Institute Internet Policy Project meeting in December 2003, and we are grateful to the organizers of and participants in that session. Thanks also to the Yale Information Society Project and the Berkman Center for Internet & Society for hosting us for discussion sessions. We are also particularly grateful to Esther Dyson, Lori Fena, Urs Gasser, Peter Harter, Spencer Reiss, and Donald Telage for their comments. Thanks also to Clifford Chen for his research assistance.
[8] *See* http://www.itu.int/wsis/ (accessed January 30, 2004); http://www.iccwbo.org/home/news_archives/2003/stories/icann.asp (accessed January 30, 2004). *See also* http://alac.icann.org/wsis/statement-wsis-20jan04.htm; http://www.theregister.co.uk/content/6/34163.html; and http://www.iccwbo.org/home/e_business/policy/ICC%20issues%20paper%20on%20Internet%20Governance.pdf (all documents accessed January 30, 2004).
[9] *See* IPS, *Who Should Master the Domains?* at http://www.ipsnews.net/focus/tv_society/viewstory.asp?idn=75 (accessed January 30, 2004).
[10] *See* David R. Johnson & David G. Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996). *Cf.* John T. Delacourt, *The International Impact of Internet Regulation*, 38 HARV. INT'L L.J. 207 (1997); Kenneth Neil Cukier, *Internet Governance and the Ancien Regime (A Reply to Larry Lessig)*, SWISS POLITICAL SCIENCE REVIEW (1999). *But see* Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998). *See generally* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE, 192-193 (1999).

Many of these new difficult online issues are caused by the ease with which antisocial individuals can take harmful action at a distance -- such as sending out bits that clog our electronic mailboxes, tricking us into downloading software that automatically collects and discloses detailed electronic records of our online activities, or disseminating malicious software code that erases hard disks or bombards servers with bogus traffic.

The internet also presents new opportunities for dealing with the problems it creates. Some such opportunities stem from the relatively equal capabilities of harmful and helpful software code and the ease with which individuals (and their employers and ISPs) can use helpful code to protect themselves. One man's fist (or club or rifle or bomb) may overwhelm another's defenses in the offline world of atoms. But incoming bits cannot overpower the defenses, also built with bits, that turn them away in cyberspace. If an ISP sets its routers and servers to reject traffic from a specified source, then that traffic cannot get through to that ISP's users. If an individual tells her email software to discard (or hide) all email that does not come from trusted sources, the desires of the recipient, not the sender, prevail.[11]

In the offline world, because we cannot easily protect ourselves against the threat of physical violence, the creation of a central state providing police protection and military defense seems a wise step. In contrast, any exchange of bits requires mutual consent. Your spam filter is completely effective against any particular source of email once you decide not to accept traffic identified as coming from that source.[12] Your individual decision to install a firewall and virus or spyware checking software (or to cooperate with or delegate to corporate actors who do this for you) can significantly increase internet security.[13] A new form of order is emerging based on this peculiarly digital balance of power. And we believe that any mechanism that can cope with spam, spyware, and electronic security issues would likely work well with respect to many other online problems.[14]

As long as ISPs, enterprises, and individuals use systems that require those who interact with them to authenticate themselves and/or provide acceptable reputational credentials -- using a contextually-appropriate mode of authentication -- then everyone can decide when to trust someone (some source of bits) and when to filter someone else out of their online world

[11] Of course, an arms race will ensue between those who want to refuse malicious bits and those who seek to get unwanted bits through, by means of trickery and misidentification. But the distinction between bits and atoms is still meaningful. Physical force can overwhelm physical defenses; digital "force" cannot.

[12] As we will explain more fully below, spam has been a problem precisely because incoming email could identify itself as coming from a source different from the actual point of origination. The technology of the internet is now changing to allow such misidentification to be detected. For example, Project Lumos has proposed expanding email headers to include identity and other information required to securely distinguish the sender. And the Tripoli proposal envisions cryptographically linking a third-party certified, encrypted information and authentication token to every email message. *See* n. 39, *infra.*

[13] In some cases, delegation is necessary. Indeed, "transparency" may be counterproductive when it comes to security concerns. Because destructive code can propagate quickly, ISPs must be authorized to shut off sources of it without the permission of their users. Because filters can be worked around, it may be unwise for an ISP to disclose precisely what its filters check. And in the context of machine-to-machine communications, decisions regarding which sources and code/messages to "trust" will necessarily be automated. Despite these qualifications, we are suggesting that end users can and should remain ultimately in charge of the decisions made by online intermediaries regarding which types of connections and messages to accept.

[14] The ability of individual users to connect to others (to receive email or access web-based content), based on trust relationships and recommendations from trusted sources, plays a positive role. Such connections can lead users to valuable information and new trustworthy relationships. Thus, while we will look most intensely at exchanges of harmful messages, and at mechanisms that can filter out such exchanges, we are concentrating on these negative/filtering issues only because they are most pertinent to demonstrating that a better form of social order can be established online without resorting to centralized rulemaking and governmental enforcement powers. The emergent phenomena we describe in this essay involve not only avoiding harm but also finding benefit and forming new social organizations and roles. We mean to include these positive connections in our overall description of the "peer production of governance."

altogether.[15] Using such systems, we can collectively hold those with whom we interact online accountable for their antisocial actions (and for their failures to hold others accountable).

This approach reverses the presumption that we have had on the internet so far. The old default was that you accepted communications unless you had some particular reason to reject (or discard) messages from your correspondent. New technologies will make it possible to adopt a new default: to connect only with those who have shown they are worthy of your trust. Because antisocial individuals cannot override these decisions by sheer electronic force, there is reason to expect that concerted action by responsible cybercitizens (and by the ISPs and enterprises to which they delegate power) will greatly improve most online neighborhoods. Engaging in internet connectivity "by invitation only" represents a radical departure from prior online social convention. But it will radically affect the flow of wrongful or malicious packets.

We acknowledge that there is an inherent conflict between (1) the internet's original goal of assuring unfettered global communications and (2) limiting connectivity based on trust relationships. As we will explain in this essay, we are confident that any possibly negative effects of this presumption shift will be greatly mitigated by human needs to connect to others -- and will be outweighed by substantial long-term benefits. The internet is becoming a major city, in which it no longer makes sense to leave one's door unlocked. But it can become an orderly city in which it is easy to form new, valuable relationships and to find a rich array of competing ideas. It is time we recognized the end user's right to decide with whom to communicate. It is time we insisted that our employers and ISPs connect only to other network "peers" that take responsible security measures. If users (and their ISPs) do not take steps to constrain antisocial action, governments will feel compelled to take on that role. Governments may not do as good a job as can be done, in a decentralized fashion, by the online community itself.

As in the offline world, the question of online "governance" is all about allocation of control over the available means of making and enforcing rules. History presents us with three basic alternatives to choose from: benevolent dictatorship (centralized control, without accountability), representative democracy (centralized control, with formal accountability to a citizenry), and decentralized decision-making (everyone makes their own rules and enforces them as best they can). In the real (offline) world, western democracies have rejected dictatorship -- no matter how benevolent it may claim to be -- as tyranny. We have also dismissed decentralized decision-making, on the Hobbesian ground that decentralized control over physical force would lead to chaos. Accordingly, we have settled, offline, on theories of governance that accept the need for centralized power and top-down rules. We seek to preserve our freedoms by using elections to select representatives empowered to establish and enforce these rules. And, as a counterweight to the powers we have created in our offline governments to make rules and use physical force to enforce them, we articulate legal rights that constrain governmental actions -- and we hope the courts can persuade the sheriff to support their decisions.

We do not quarrel with those choices in matters that primarily affect or occur in the offline world. We accept that there is a need to create a monopoly in the sovereign on the legitimate use of physical force. And we respect and appreciate the practices of representative democracy. But the world of bits is not the same as the world of atoms. The two worlds are closely connected, yet some problems exist solely in or primarily concern one sphere or the other. And the methods used to solve bit-based problems should reflect the way bits behave. Specifically, because the internet involves a much more equal distribution of "force" than does the offline world, it may not be necessary to create a centralized monopoly over the use of digital force. As authenticated persistent identifiers proliferate, it will become increasingly easy to avoid or neutralize antisocial activity. When we can choose with whom to connect, the online society we encounter will reflect

[15] We are drawing a distinction here between "identification" and "authentication." We do not think that a certified connection to a real-world, flesh-and-blood person would be necessary for this system to work. But authentication will be necessary. For more on the distinction between "identification" and "authentication," see NIST publication at http://csrc.nist.gov/publications/nistpubs/800-11/node26.html: "Identification is the process whereby a network element recognizes a valid user's identity. Authentication is the process of verifying the claimed identity of a user."

our own willingness to take risks, and the extent of the threat we face from wrongdoers will diminish in proportion to our ability to act on recommendations from trusted sources. The growing effectiveness of decentralized action will require us to rethink our received theories of governmental legitimacy in the online context.

Rather than electing representatives, or hoping that some unaccountable online sovereign will do the right thing, we can collectively assume the task of making and implementing the rules that govern online activity -- holding each other directly accountable for our respective actions and establishing levels of connectivity tied to context, personal knowledge, contractual undertakings, and reputation. We may not need to give a central government the power to use the electronic equivalent of force in order to assure adequate online order. The aggregation of numerous individual decisions about who to trust and who to avoid will create a diverse set of rules that most accurately and fairly serves the interests of those who use the online world.[16] In other words, we can use "peer production of governance" to address the collective action problems that arise in the online context.[17]

We first discuss several contexts in which some form of internet governance can be said to be needed. We then discuss three alternative models of governance. We reach the conclusion that, of the available alternatives, decentralized decision-making to establish trust-based connections is most likely to provide an effective, wise, and just form of governance for the online world. This form of governance is newly enabled by tools that allow accurate identification of the sources of messages/packets and enhanced management of the interconnections between networks and among end users. It will require more widespread adoption of the practice of deciding which sources and connections to trust. It will require a growing understanding that establishing a connection with others across the internet represents a social contract, breach of which should lead to ostracism. We will call the desirable end result of such changes "the accountable internet." We predict that governments will defer to such decentralized governance, to the extent that it proves able to protect people from major online problems.

II. WHY MUST WE GOVERN THE NET?

Early net theorists proclaimed that the affordances and architecture of the net made ungoverned (or ungovernable) liberty inevitable online.[18] We are not seeking to turn the clock on this discussion back to 1996. It has become clear that unconstrained online interactions can lead to highly undesirable results.

---

[16] We are specifically not referring to "trusted systems" here. That term is used to refer to centralized means of administering permissions for access to particular documents. To the extent that some systems establish rights to access online materials by means of algorithms, they are not what we have in mind. Moreover, we are not talking about technical mechanisms that govern connections between machines (for example, the rules that govern ATMs). Nor are we talking about technical filters that inspect the characteristics of particular packets of bits or collections of code, without looking for first for their source. Such technical filters have been important to create some order on the internet in the past, just as has been the ability of individuals to decide affirmatively what links to click on. But both such mechanisms are susceptible to fraud and subject to technological arms races. We are talking about the likely emergence of a quite different phenomenon: the ability, at both the individual user level and that of the ISP, to decide with whom to communicate.

[17] Yochai Benkler defines peer production as a new mode of collaboration in which individuals contribute to the construction of some valuable work product, in exchange for recognition or reputational gain rather than as part of an employment relationship or in the course of a market-based transaction. We use "peer production" to describe decentralized governance because the processes we describe end up creating a valuable work product – increased online social order – even though the many individuals taking the necessary actions are not paid to do so, select themselves for this task, and operate as equals. Yochai Benkler, *Coase's Penguin, or Linux and the Nature of the Firm,* 112 YALE L.J. 369, 375 (December 2002).

[18] John Perry Barlow, *A Declaration of Independence of Cyberspace*, February 8, 1996, at http://www.eff.org/~barlow/Declaration-Final.html (accessed December 18, 2003).

There are bad guys out there online who do not care what effects their actions have on others. Right now, the costs of being and staying bad online are very low.[19] These bad actors can have disproportionately harmful effects on others. The fact that electronic messages can easily cross territorial boundaries makes it harder, although not impossible, for traditional government structures to control the resulting problems. Even if some local legal controls are possible, conflicts between local standards inevitably arise.[20] This can lead to a "race to the bottom" -- the creation of havens for actions (like sending spam) that some affected countries consider wrongful but that other countries decline to prosecute.[21]

Accordingly, various serious problems cannot readily be solved by local sovereigns. Yet the internet will also continue to become more and more important to global business and communication of all types.[22] We are building it into the very fabric of our lives.[23] So we need to find some means of keeping bad actors under control. And we need to think outside the box of traditional, localized, legal solutions.

We describe below three examples of online collective action problems that we will use to test the relative efficacy of three alternative modes of online governance.

A. Spam

The central vice of spam (generally defined as the bulk sending of unwanted commercial email messages) is that it wastes the world's collective attention. Unlike intrusions in the real world, sending massive amounts of spam is virtually free to the sender.[24] Spam presents a classic tragedy of the commons, arising because individual actors lack an adequate incentive to avoid overusing and abusing valuable resources: our time, the processing power of our mail servers, and our ability to find things of interest in our electronic mailboxes. Spam is a problem that does not exist in the same way or to the same degree in the offline world. It is also a problem to which traditional legal responses may not provide an adequate solution.[25]

---

[19] A few of the so-called "spam kingpins" have been caught, but prosecutions have been infrequent. See Brad Wright, Virginia Indicts Two on Felony Spam Charges, www.cnn.com, December 12, 2003, at http://www.cnn.com/2003/TECH/internet/12/12/spam.charges/ (accessed February 12, 2004)

[20] *See* Jonathan Zittrain, *Be Careful What You Ask For: Reconciling a Global Internet and Local Law*, *in* WHO RULES THE NET? INTERNET GOVERNANCE AND JURISDICTION 13 (Adam Thierer et al. eds., 2003).

[21] Many countries already have varying reputations for their willingness to condone activity online that other countries would not abide. Nigeria, for instance, is thought to be a place from which a disproportionate percentage of the world's spam, in particular certain frauds, originates. *See* Joanna Glasner, *Nigeria Hoax Spawns Copycats*, Wired, June 2002 at http://www.wired.com/news/business/0,1367,53115,00.html. In some extreme cases, such as the creation of HavenCo on the self-declared island "nation" of Sealand in the North Atlantic, entrepreneurs have sought to make data havens possible. *See* Simson Garfinkel, *Welcome to Sealand. Now Bugger Off*, Wired, July 2000 at http://www.wired.com/wired/archive/8.07/haven.html (accessed January 14, 2004). *See also* Zittrain, *Be Careful What You Ask For*, *supra* note 17, at 17 – 18.

[22] Roger Alcahy, THE NEW ECONOMY: WHAT IT IS, HOW IT HAPPENED, AND WHY IT IS LIKELY TO LAST (2003) (comparing rise of internet economy to rise of economy powered by electricity).

[23] Internet World Stats reports internet usage by 201 million people in North America (62.2% penetration rate); worldwide, 682 million people were using the internet as of November 2003, a 90% growth since 2000 (10% penetration), at www.internetworldstats.com (accessed January 30, 2004). Likewise, there has been a continuing increase in the penetration of faster broadband connections, which in turn drive more useful applications and reasons to work online. *See* http://www.websiteoptimization.com/bw/0312/ and http://www.urlwire.com/news/010204.html (accessed February 11, 2004).

[24] As Lawrence Lessig put it, "The guy who sends out 10 billion emails just to get 100 orders has no incentive to behave well." At http://beta.kpix.com/news/local/2004/01/22/There's_More_Spam_Out_There_Than_Ever.html (accessed February 12, 2004).

[25] Even the recent US federal law (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, the "CAN-SPAM Act of 2003") recognizes that local legal prohibition of spam may be ineffective. And, indeed, the Act may have had little impact on spam. *See* BBCNews, "*US anti-spam law fails to bite*," February 9, 2004 at http://news.bbc.co.uk/2/hi/technology/3465307.stm (accessed February 9, 2004).

Many fixes to the spam crisis have been proposed.[26] For example, some have suggested imposing an economic cost on the spammer.[27] But the online medium, as currently configured, allows numerous ways to defeat any effort to impose a postage fee or other economic solutions.[28] Spammers can easily move "offshore" with respect to the jurisdictions in which the effects of their messages are felt. Some have suggested making the sending of spam a crime, and the US recently passed a law to this effect.[29] But other governments could view spam sent to the US as a means of enhancing economic development.[30] Even if we could find the spammers, we might not be able to extradite them.

In short, even though there is widespread (but not total) agreement that we should somehow govern activity on the net to reduce the impact of spam, we will probably not be able to rely on existing legal institutions to accomplish this result.

B. Spyware

Informational privacy is another issue that arises in a very different form online than offline, because information collection is more easily accomplished online, because collection and storage of online data is so inexpensive, and because the creation and dissemination of a detailed personal electronic dossier is so easily automated.

In the real world, it is difficult and costly for someone to follow us around and make a record of everything we do. For that reason, we generally do not expect that every moment of our lives will be remembered and recorded, much less publicized. Online, the credentials and identifiers we use to engage in transactions automatically create a detailed record of our activity that can be stored at very little cost. Even worse, software code can be installed by third parties on our computers, with little opportunity for us to notice or object to this practice, and that software can then automatically record and disclose everything we do online. The resulting fine-grained profile, if published, could be extremely invasive of our privacy interests. No reasonable person would actually agree to be followed around all day. Yet many legal systems make the inscrutable clickwrap licenses that purport to allow installation of spyware enforceable.

---

[26] Earthlink Inc., the third largest US internet service provider, has developed a system to screen out unwanted spammers by requesting a return form from the sender, a process the spammers' automated systems cannot handle. Stephen Baker, *The Taming of the Internet*, *BusinessWeek*, December 15, 2003. Sales of anti-spam software alone in 2003 amounted to $653 million dollars and are projected to double within two years. Companies such as AOL and Microsoft are pouring research dollars into state of the art filters, while venture capitalists in Silicon Valley are beginning to invest in new startup companies intent on building the perfect fortresses for their customers. *Id.* at 31. None of these proposed solutions has yet been tried on a large scale. The problem has gotten progressively worse. Microsoft reports that 83% of the messages received by Hotmail accounts, or between 2.5 and 3.0 billion messages per day, are spam, a dramatic increase over previous years. *Caller-ID for E-mail*, Microsoft Corporation, January 13, 2004. *See also* Sebastian Rupley, "Congress, Yahoo! Slam Spam," PC Magazine, December 12, 2003, at http://www.pcmag.com/article2/0,4149,1411813,00.asp (accessed January 31, 2004) ("The anti-spam war is gathering momentum. Hardly a week goes by without a major technology company or various arms of the government creating a new way to attack unsolicited e-mail."). Other proposals include the "bounty hunter" solution and a "do not e-mail" list, similar to the US federal "do not call" list proposal to stop abusive telemarketers.

[27] *See e.g.*, Ed Bride, "Stamping Out SPAM With E-Mail Postage," EnterpriseInnovator, Sept. 29, 2003. *See also,* Sonia Arrison, *Canning Spam: An Economic Solution to Unwanted E-mail*, Pacific Research Institute, February 2004.

[28] There are several additional arguments why "epostage" is a bad idea. To be effective, such a system would have to impose minimum and uniform standards on email clients, reducing diversity and competition. It would be difficult to distinguish between email and other forms of messaging. Administration of micropayments has been notoriously difficult and cost-ineffective.

[29] CAN-SPAM Act, *supra* note 22.

[30] On the other hand, even the Chinese government seems to be cracking down on spam in response to international pressure. The Internet Society of China is using selective disconnection from ISPs that originate spam, a tactic analyzed in this essay, to address the issue. *See* "China joins global fight against spam," Computer Weekly.com, September 11, 2003, at http://www.computerweekly.com/Article124772.htm (accessed February 21, 2004).

Because the electronic records that give rise to these problems are owned or controlled by private actors, we cannot rely on traditional legal doctrines limiting government searches to protect us. Even if we passed new laws against unduly intrusive spyware practices, key actors may, again, be offshore and effectively beyond the reach of such regulation. In short, most people would agree that we should govern the net to reduce the threat of spyware, but existing legal regimes are unlikely to be able to solve the problem.

C. Security

More and more of our time is spent in online communications and collaborations that create organizations and markets. Accordingly, the newfound ability of individuals to send disruptive bits into these complex social contexts creates a security threat that is as severe as any we have experienced offline. The deranged individual who wants to attack our infrastructure can deploy weapons of mass electronic destruction -- such as denial of service attacks against predetermined targets, using execution of code on many vulnerable hosts.

Events online that seriously threaten our collective security -- from distribution of viruses to intrusions into corporate servers -- may have to be countered with the use of force. But traditional governmental reactions to employ physical force may prove insufficient. Bullets do not stop destructive bits. Moreover, even if we could identify the person who is originating destructive code, it may be difficult to coordinate the governments that have to act together to bring physical force to bear on that person. We need to use electronic/digital force. It seems that only meta-information (information about information) can effectively govern harmful information.

Online, the equivalent of force is the use of a software filter or firewall, which can render a security threat harmless by refusing to accept packets with specified characteristics.[31] This is a type of force over which governments do not have a monopoly, legitimate or otherwise. Our challenge is to come up with a way to use the dispersed, private-sector control over such electronic force to reduce online threats to our collective security. This can take two somewhat different forms: (1) decisions to inspect and reject packets of data after they have been received or (2) affirmative decisions to connect to (receive packets from) identified others. We are at a moment in time when it may be possible and advisable to shift from the former mode to the latter, radical as such a "connect only with whom you trust" model may seem.[32]

III. How We Could Govern the Net

This section explores the nature and effectiveness of three distinct models of internet governance (dictatorship, representative democracy, and decentralized decision-making) with respect to the collective action problems described above.

A. Benevolent Dictatorship

In the online world, a benevolent dictator would be the equivalent of a global, mandatory AOL. Within its own walled garden, AOL can dictate terms of service to which all users have to adhere in order to retain the right to enter. (The same is true of the network run by your employer.)

---

[31] A filter does need to know which source to filter out, but does not need to know where the human being behind the bits is to be found, or who has legal jurisdiction over him.

[32] Of course, the net provides many new opportunities to create (rather than destroy) social value. Every useful hyperlink adds to our collective knowledge. It is the relatively unbounded connectedness of the net that has led to its enthusiastic adoption worldwide. On the other hand, the creation of social value online depends critically on prevention of the disruptions that only a few bad actors can cause. An email box becomes much less attractive once it is smothered in spam. Many potential online applications go unused, or even undeveloped, because of fears of letting in destructive code. We focus on wrongdoers, and on the inadequacies of current filters, and on the problems posed by centralized governmental approaches to prevention of wrongdoing, because we think a net that is reconnected on the basis of affirmative trust among identifiable parties may be a better net. We are optimistic about the future of life online.

Moreover, users of AOL are not able to take actions that AOL's software code does not allow. AOL can install a spam filter by fiat.[33] It can collect a great deal of detailed information about its users' online actions, but retain the ability to protect these data from disclosure. It can decide when identities should be taken away from bad actors. It can install firewalls and virus checkers. In theory, it could refuse to connect to customers' systems unless they were configured in an appropriately secure manner.

It might be possible, in theory, to turn the entire online world into one managed online space. The Chinese government, with the help of that country's ISP community, is attempting exactly this with respect to its own population.[34] All that is required is the use of a government's control over physical force to compel all the owners of online servers to comply with a single set of rules.

But the end result of such careful management would not be the internet we know and love. It would be a single network, with a single network administrator, not a "network of networks" that have voluntarily agreed to interconnect. We would have destroyed the online village in order to save it. And, even if efficient, such a regime would suffer from all the deficiencies of authoritarian rule.

If there were a benevolent dictator for the internet, it might make rules that ban the simultaneous sending of similar messages to more than a specified number of subscribers. Such a dictator, as hypothesized, would even be able to install software that made such actions impossible. Just as no one user of AOL can use AOL's mail system to fire off 10,000 unsolicited messages to AOL members, some centralized governance structure with the power to make and enforce rules applicable to all the servers connected to the internet could directly prevent spam. But how would those subject to such rules ever be able to change them? One could not leave the internet as a whole to seek better policies in some other equivalent online space. Would the dictator decide that unsolicited non-commercial messages, or messages critical of the global system operator, should also be banned? How could we be sure that the actions against which this postulated internet dictator could wield such impressive electronic powers were really evils that most people would condemn?

Similarly, an internet dictator could seek to protect informational privacy by establishing rules about what information could be collected, aggregated, and/or published by those engaged in electronic communications. Just as any ISP can make rules about when to publish its users' personal information, or what due process is required before a user's online identity is removed, some centralized authority could (with the aid of traditional sovereigns) do so for the internet as a whole. But, here again, what would prevent this global system operator from abusing its own access to detailed information about every online actor? What would prevent it from arbitrarily banning an online user?

An online dictator could also require as a condition of connection that each subsidiary network install suitable security software and follow specified practices. Just as any walled-garden administrator can now do, a dictator of the internet could log all traffic, watch the information associated with IP blocks, and generally get to "know its customers/citizens" well enough to prevent most security threats. But such security practices would entail serious downsides as well. Would the dictator decide that only "approved" executable applications could be sent within its world? Preventing all risky communications would inevitably prevent many valuable ones. One would never know the costs to innovation of such a policy. Allowing a central authority to "know its customer" too well carries all the privacy risks outlined above. A dictator that could

---

[33] Many of the largest ISPs do filter some email messages by fiat.

[34] *See* the work of the Open Net Initiative, a joint project of the Citizen Lab at the at the Munk Centre, University of Toronto (Prof. Ronald Deibert), the University of Cambridge (Rafal Rohozinski), and the Berkman Center for Internet & Society at Harvard Law School (Prof. Jonathan Zittrain) at http://www.opennetinitiative.net/ (accessed February 24, 2004). *See also* Jonathan Zittrain and Benjamin Edelman, *Documentation of Filtering Worldwide*, at http://cyber.law.harvard.edu/filtering/ (accessed February 24, 2004).

effectively respond to all security threats could also eliminate any users or communications that made the electronic powers that be uncomfortable.

In general, the problem with using an unaccountable central authority to govern the internet is less that such an authority could not take effective action and more that its actions would be unconstrained and that its goals might diverge from those widely supported by those it governs. To handle that kind of problem in the offline world, we have developed various means of making government accountable to the governed.

B. Representative Democracy

There is no theoretical reason why well-known institutions of representative democracy could not be applied to the online world. Electronic voting is feasible, if imperfect in its incarnations to date.[35] Indeed, properly deployed, electronic identifiers might make such voting systems quite secure. We might, in theory, decide that rules relating to spam, spyware, and security practices could be made by a legislature elected by the world's cybercitizens.[36] Any such body could wield electronic force -- to the extent that ISPs looked to its rulings -- and thus might have greater enforcement power in the online context than does any local "real world" sovereign. An elected online authority might have the power to unplug any portions of the internet that refused to obey its laws. Such electronic enforcement powers are already familiar to us. Direct revocation of domain name registrations -- the equivalent of pulling the plug at the level of an authoritative domain name server -- is now used to enforce arbitration decisions finding a party guilty of cybersquatting. Why not create a democratic government that can use the revocation of online identifiers (or mandatory denial of interconnections among service providers) to control whatever it considers to be online wrongdoing?

There are some obvious problems with porting the democratic model to the internet. Successful democratic institutions require a rich backdrop of shared values and civic interaction, factors that are not yet present online in a global context.[37] Moreover, local "real world" sovereigns are very unlikely to cede power to an online legislature, no matter how democratically elected.[38] Even if a democratic, centralized internet governance institution could demand deference, it would likely produce uniform rules that did not adequately reflect the diversity of local values. In the US, we have dealt with this problem by means of federalism, allocating various issues to local control. But a very large portion of internet traffic is non-local commerce that crosses both virtual and real-space boundaries.[39] So almost any local rule would unduly burden such commerce (and undue local permissiveness would create havens for those whom others consider wrongdoers). We would need a global dormant commerce clause -- and, if we had one, it would, in the context of

---

[35] There is a long, fraught debate as to the security of online voting systems and the problems of online authentication and auditing. Several of these problems garnered widespread attention after the leak of numerous internal documents written by employees of Diebold, a large American corporation that makes, among other things, electronic voting machines. *See* Mary Bridges, *Diebold v. the Bloggers*, Berkman Briefings series, January, 2004, at http://cyber.law.harvard.edu/briefings/dvb (accessed January 30, 2004). The Electronic Frontier Foundation posts an archive of information on e-voting and related issues at http://www.eff.org/Activism/E-voting/ (accessed January 30, 2004). *See also* Kim Zetter, *Aussies do it right: E-voting*, WIRED.COM, November 3, 2003 at http://www.wired.com/news/ebiz/0,1272,61045,00.html (accessed January 30, 2004).

[36] Though not precisely analogous, consider the aspirations of e-Parliament, at http://www.e-parl.net/ ("The e-Parliament is the first world institution whose members are elected by the people.")

[37] Hans Klein, *The Feasibility of Global Democracy*, August, 2001, at http://www.prism.gatech.edu/~hk28/klein-democracy.pdf (accessed January 30, 2004).

[38] WSIS suggested the creation of a global authority by governments. Most of the governments that participated in the creation of a global operator might well be expected to defer to it. But democratic elections would place most control over a centralized online authority in the hands of people outside of any particular state. If a central authority not created by a particular nation were to take action adverse to the interests of its citizens, the nation might be expected to resist such assertions of authority even if its citizens were in theory allowed to participate in an election used to select that authority's officials.

[39] One proxy for this point is the increase in the Internet-related cross-border consumer fraud reports received by the FTC. *See* http://www.ftc.gov/opa/2003/02/cbfrpt.htm (accessed February 12, 2004).

the internet, forbid most local regulation of traffic originating from foreign sources. To avoid that result, we would need a doctrine of sovereignty for local networks. If we had a strong version of such a "state's rights" doctrine, it would reflect the real diversity in our values and foster exactly those problems the central authority had been created to address.

The key problem with creating any centralized authority over the internet is not just the need to assure the accountability of such an authority but also the reality that the values of the population to be controlled are so diverse that no single set of rules will enjoy the widespread support necessary for legitimacy. And any explicit devolution by that central authority of the power to create local rules would necessarily create havens for activity that impose on other users what those users consider to be unjustified harm. We will not soon be a global nation, democratic or otherwise -- certainly not one with a constitution that includes a supremacy clause.

The collective action problems we are addressing arise because some individuals seek to impose costs on others who do not share their values. It is one thing for a citizenry confined to a single geographic location to govern (or expel) a small minority of bad actors. It is quite another thing to create rules on a global scale, in which context there are much starker disagreements about what is right or wrongful and no option to leave the territory. We clearly need some mechanism to prevent the imposition of harm by some individuals or small groups on others, globally. But the creation of any centralized authority will necessarily involve delegation of the power to decide what is "harmful." Because there would be no way to leave the global online world for an alternative regime (aside from withdrawing entirely from electronic interaction with the rest of humanity), the enforcement powers of a centralized internet government would be, in effect, too great. Once such a government strayed beyond condemning actions that virtually everyone considers to be crimes, the consensus underlying its claim to legitimacy would collapse. The world is too diverse to allow any central authority to mandate, in effect, allegiance to a single set of values -- even with respect to what should be permitted or punished in the realm of bits.

C. Decentralized Action: The Peer Production of Governance

This leaves the third alternative of not creating any centralized government for the internet. In this model, no one is in charge. But that is not to say that no one has any power to exercise control over online events. The control necessary to protect the attention commons and the many valuable systems connected to the internet would rest with individual end users and the employers and internet service providers who run the networks they use.

The "peer production" alternative involves allowing each individual to make his/her own decisions (or to require/empower his/her ISP or employer to make decisions) regarding when and with whom to connect. Even if there is no central internet governance authority, individuals can still decide which informational flows they will accept, based on verifiable tags or labels that identify messages as coming from other people they know or from those recommended to them by others they know and trust.[40] Such decentralized decisions reflect each individual's views as to which communications are valued, not a collective agreement regarding what is right or wrong. The absence of a centralized authority does not lead to inaction. Instead, such a power vacuum allows highly effective action by private parties to protect themselves against whatever they consider to be antisocial activity. If you trust the other person or entity, their bits will get through. If you do not, that other person will not exist for you.

Individuals will, of course, seek and sometimes defer to recommendations by others. Many may in effect delegate almost all control of their online connectivity to their ISP or their employer. But individuals nevertheless can remain the ultimate source of authority regarding what rules will be made and enforced, provided they can choose among ISPs or access providers (or among

[40] *But see* Lawrence Lessig, *Tyranny in the Infrastructure*, Wired.com, July 1997, at http://www.wired.com/wired/5.07/cyber_rights_pr.html (accessed January 31, 2004) ("Blocking software is bad enough – but in my view, PICS is the devil.") We are not suggesting that a single, standardized set of labels or authenticating credentials should be identified. We envision multiple, contextually-appropriate sets of labels or tags that will emerge from various communities.

outsourced sets of rules made available to individuals). We will discuss below the important questions of how best to keep these intermediaries accountable to end-users.

We are suggesting that, at the individual level, tools will be created that allow end users to more affirmatively manage their connections, particularly with respect to email. At the ISP level, we are suggesting a very slight change in the practices that already exist: the conditioning of connectivity among networks on continued compliance with security measures that make the entire online world safer. There was never a right on the part of any network to connect to an unwilling neighbor.[41]

Using this multilayer system, we will end up with an internet that indirectly connects everyone to everyone else but that only provides direct, unfiltered connections to the degree that the private parties concerned in any given exchange consider the relationship desirable. The online world created by this form of governance is built both on trust and on the right to distrust. In its pure form, it is a world in which every online actor could be held accountable, by every other online actor, for his actions. There would be no one government that could grant or repeal your authentication for all purposes. But there would be many peers whose willingness to accept your packets would determine how easy it would be to get your message through. If you were new to some section of this cybertown, you might need a letter of introduction.

IV. IMPLICATIONS OF PEER PRODUCTION OF GOVERNANCE

This section discusses the implications of the accountable internet for the particular online problems we have identified.

It is clear that decentralized decision-making can control or sharply curtail the spam problem, as long as sources of email can either be accurately identified (authenticated as actually coming from the source listed in the headers) or known to be incapable of authentication.[42] Some people may decide to continue to accept mail from any source, whether or not known or recommended. But others will regain control over their email boxes. It will be impossible for anyone to force a message through against the will of the recipient. The spam game will no longer be an arms race involving attempts to detect or disguise particular mutable characteristics of the message's payload. Instead, it will be a matter of who the user wants to hear from, and which introductions from friends to new persons the user wants to heed. The new world of email will consist of messages you are very likely to want to receive -- because sending a message to you that you do not want might get the sender taken off the list of those you invite to communicate.

Similarly, appropriate levels of protection against spyware can arise from a system in which individuals (and ISPs) decide whom to trust with access to the detailed electronic information

---

[41] A peer production of governance system works slightly differently at different levels. To the extent that an individual end user controls access to a particular portion of his system (e.g., an electronic mailbox), the rules applicable to connectivity can be set directly. For example, given persistent authenticated identifiers, it is feasible for an individual to decide to receive email only from people that individual knows and trusts. You can set your email box only to accept mail from those on your address list, absent a manual override that you enter when you receive a recommendation of a new contact from someone you already know. In contrast, at the level of the ISP (and the other networks that engage in "peering" to exchange messages across the internet), the mechanisms of trust-based connectivity differ. As an ISP, you know who you are connected to, because your routers can accept or reject packets from identified sources. You either connect directly to another ISP, or to a backbone that has policies about who it will connect with and on what terms, or to a peering point at which identifiable networks mutually connect on specified terms. Right now, when a particular network (or server) is identified as the source of a security problem, those who connect with it (receive bits from it) can cut it off.

[42] Many of the leading technologists working on solutions to the spam problem believe that we can solve the authentication problem with existing technology. *See* Tim Weber, *Gates Forecasts Victory over Spam*, BBC Online, January 24, 2004, at http://news.bbc.co.uk/2/hi/business/3426367.stm (accessed January 30, 2004). *See also* TRIPOLI: An Empowered E-mail Environment, at http://www.pfir.org/tripoli-overview (accessed January 30, 2004).

created by online actions. Connections will be based on a verifiable pattern of reputation-enhancing behavior. This pattern of behavior will become a credential that may be demanded in advance of any interaction. Whether a third party will be in a position to install surreptitious software that collects detailed information about your online actions will depend on who you or your ISP choose to deal with. Such parties will have reputations and you or your ISP will know whether or not your friends (or friendly ISPs) trust them.[43] Those who can gain information about us will become more accountable to us, and will lose access to our information if they betray our trust.

We may need new tools that will tell us to whom our local computers are sending information regarding our online actions. When we have those tools, the question who can track (and disclose) our online activities will become a matter of who we allow our computers to communicate with, rather than what kinds of information and information uses are described in a privacy policy. This shift from (1) trying to govern what data is collected or disclosed to (2) controlling with whom we connect makes possible governance by decentralized decision-making.

Peer governance systems are also well suited for dealing with most security risks. Destructive code will propagate less freely if many users decline to deal with others whose identity is not verified and whom they do not have reason to trust (or who do not follow acceptable security practices).[44] A traditional legal approach to security might involve trying to deter wrongful action (e.g., launching destructive code or a denial of service attack) by making it illegal and using the physical force deployed by police to enforce such rules. In contrast, the peer production of security takes the form of making access to the right to send packets (or executable code) dependent on (1) a demonstration of verifiable identity, and (2) the establishment of a basis on which the recipient should take the risk of allowing packets from the source onto his systems.

Trust will sometimes be betrayed. And some people will fail to participate, or to act rationally, exposing themselves and others to harm. But those who do not join the collective action to filter out destructive code can themselves, ultimately, be banished by the networks they use.[45] Thus, decentralizing decisions about when to trust and when to disconnect can dramatically increase overall security. This requires a reversal in the previous presumption that all should connect to all. But we are approaching a level of threat that justifies such a reversal.

It is worth observing that we have always had various weak forms of decentralized decision-making regarding online connections. Individuals have always been able to decide not to go to particular web sites. A link is, after all, a form of "recommendation" from a source -- a source that we may not trust or be able to identify. Individuals already can decide not to open email they do not expect. Blogs work well because they give us reasons to go to particular online sources, based on pointers from people we already consider reliable judges of value.[46] ISPs have always had the ability to connect to (or, more formally, "peer with") only those other ISPs they believe follow responsible security practices, although most have not attempted to apply such rules downstream. Most companies set their routers and domain name servers to filter out some identifiable sources of spam, some types of executable downloads, and some web pages with offensive material. Some ISPs routinely filter out email coming from locations that the Realtime

---

[43] To the extent the data you provide to third parties can itself be tagged, you may be able to find out whether or not such parties have disclosed such information into public channels.

[44] It is essential to distinguish the transmission of destructive code, such as viruses and worms, from malicious hacking or "cracking," wherein a third-party gains unauthorized access to your computer or network. The peer production of governance will work well to reduce the risk of harm from the former, but is less well-equipped to handle the latter. Indeed, increased use of trust-based connectivity may increase the risks that wrong-doers will exploit the trust relationships that have been established. No system can entirely eliminate fraud or betrayals of trust. It is in these latter cases that the backstop of sovereign involvement may be needed.

[45] Provided adequate choices of network connections exist, those who are ostracized should be able to start again with building a reputation. There will be many second chances in the peer-governed internet.

[46] Web logs, or blogs, are roughly thought of as "the unedited voice of a person" writing to a web page, much like an online journal. For one definition, *see* Dave Winer, *What Makes a Weblog a Weblog?*, at http://blogs.law.harvard.edu/whatMakesAWeblogAWeblog (accessed February 11, 2004).

Black Hole group says encourage spam by running open relays. Some end users can set their browsers to take them only to approved locations (e.g., .kids.us) or never to allow them to visit the wrong part of cybertown (e.g., a new .xxx domain or any web site not labeled with an appropriate ICRA rating). We have all come to appreciate the reputational feedback loops on eBay that help us decide which vendors are most likely to be honest and to treat us well if there are problems with a transaction.

What is different now, and what accounts for our prediction that social order will increase online, is that new technologies will make it increasingly easy to be sure that messages are in fact coming from identified sources, that the web pages reached by clicking on a url really are the ones you intend to go to,[47] and that hosts that do not follow the security precautions a particular ISP finds adequate cannot send any packets to that ISP's servers. We are about to develop more new tools that make it much easier to decide to accept communications only from trusted sources.

For example, Yahoo! has announced a new public key encryption system to authenticate email coming from its servers. This is valuable to the extent that we trust that Yahoo! will itself eliminate users who send spam. Others have proposed standards for federated or decentralized authentication of packet sources.[48] Social software programs are making it easier for large groups to exchange valuable reputational information.[49] We will soon find it relatively easy to determine (or have our ISPs or computers determine, in the background) whether the source of an email (or other form of message) has been determined by one of our trusted friends to be a spammer or to present a spyware or security problem. There will not be only one form of authentication, much less only one global system of establishing trust. To the contrary, many different systems will compete to demonstrate that they are reliable. But the unifying, and new, factor will be that end-users (and their ISPs, if users insist on this) will be in charge of the decision whether to accept communications from another party.

These new systems should not be thought of only in terms of their increased ability to limit or condition connectivity. They will also increase the value of the connections we do decide to make. We will find out which sources of content are viewed by our friends as particularly valuable. Indeed, the ability of trust relationships to control the distribution of digital media of all types may well be what leads to rapid adoption of these new tools. Sending a new song into a network of friends, who trust each other's taste in music, may be the very best way to reach the market. In short, we will be able to leverage our collective efforts to evaluate both what is wrongful and what is valuable, while remaining in control of where we go online and who (and what) we allow to become part of the online space we personally encounter.

None of this will happen automatically. If we are going to clean up the internet neighborhood by collectively deciding to shun bad actors, then we actually have to take the decentralized actions

---

[47] Recently, Microsoft fixed a problem with the Internet Explorer browser that had allowed a particular form of "phishing" – the display of an apparently legitimate url while the browser is instead taking the user to another, illegitimate site (typically a bogus copy of the apparently accessed site, designed to elicit disclosure of user passwords or credit card or account information).

[48] There are several different ideas for authentication. One is based on authenticating the identity of the server originating the message. *See* Larry Seltzer, *Yahoo! Proposes Anti-Spam Standard for Internet*, EWEEK, January 12, 2004, at http://www.eweek.com/article2/0,4149,1430976,00.asp (accessed February 11, 2004). Another is based on providing a separate, secure description of the source and nature of a potentially deliverable message. *See* Lauren Weinstein, *Tripoli: An Empowered E-mail Environment*, at http://www.pfir.org/tripoli-overview (accessed February 11, 2004). *See also* Hans Peter Brondmo *et al.* Project Lumos http://www.networkadvertising.org/espc/Project_Lumos_White_Paper.pdf (accessed February 11, 2004) (proposing "a federated Registry model for registering and certifying volume e-mail senders.") MailKey and SenderID.org have floated a confidential proposal along similar lines, based on the currently functional SML Protocol (proposal draft of January 14, 2003, on file with authors). Both the Yahoo! Domain Keys and Microsoft Caller-ID for E-mail would rely upon methods of authentication.

[49] The social software movement is demonstrating the power of personal recommendations and networks, although the links reflected in such networks are currently insufficiently nuanced. *See generally* LinkedIn, at https://www.linkedin.com/, and Orkut, at http://www.orkut.com/ (accessed January 30, 2004).

that add up to this new form of social control. End users will have to decide to take control of their own email boxes. Individuals with servers will have to either install firewalls or insist on dealing only with ISPs who do so.[50] ISPs have to compete against one another on the ground that their connectivity and security practices better serve the needs of particular customers. A market for wise connectivity rulesets will emerge, but only if we participate in that market. And, finally, if we are going to avoid the problems associated with creating a more centralized authority to govern the internet, we must collectively make the decision that we do not need to elect an online sheriff -- or tolerate an unelected rulemaker.

V. How Should We Evaluate Alternative Forms of Internet Governance?

Each form of online governance outlined above would address the collective action problems posed by cyberspace in a different way. They are not mutually compatible. We either cede power to a single benevolent online despot, or we do not. If we do not cede such power, we can seek some form of accountability, either by democratic election of some group authorized to make and enforce rules on our behalf or by allowing individuals to choose and enforce their own rules. We can either attempt to make a centralized online authority accountable, or we can decide that it is possible, at least in the online world and with respect to certain problems, to do without any central authority at all. How should we go about deciding which of these forms of social order will be best?

To determine which kind of social order to prefer, we must first define "best." We have adopted the following definition:

- We consider an online governance regime "wise" if it accurately identifies those rules that will, over time, best serve to the greatest possible degree the interests of the largest number of affected people.

- We consider an online governance regime "just" if it does not systematically disregard or ignore the interests of classes of individuals, even if by doing so it could optimize the welfare of most.

- We consider an online governance regime "effective" if it successfully protects the valuable social order we collectively create online, by preventing the unreasonably destructive acts of antisocial individuals.

This is not a theoretical exercise. We need to choose between real-world alternatives for addressing the three concrete collective action problems of spam, spyware and security.

- To reduce spam, should we allow some centralized filtering authority to decide which messages may be delivered, pass legislation in some newly-minted international legislature, or simply allow everyone who wants to decline to take email other than from trusted persons to do so?

- To protect our privacy against the threat of spyware, should we keep all our data in a central "passport" database, access to which is allowed only on the terms set by the monopoly supplier of that service, or should some democratically elected body (or international tribunal selected by our governments) seek to establish new substantive rules about the use of personally identifiable information, or should we all (individually, or

[50] There have been recent articles decrying the cluelessness of end-users and despairing of any strategy that requires knowledge by end-users of what their computers are doing, much less decisions on the part of end-users to change defaults. As more fully discussed below, we think much of the work required to be done to build an accountable internet can be accomplished by means of individuals' demands that their access providers take the steps necessary to protect them. But we also think that individuals are on track to learn more about the devices they use.

in groups through our ISPs) decide who to tell about ourselves, and what software to use and what online connections to make, in light of the likely consequences of doing so?

- To protect the security of our way of life (more and more of which is happening online every day), should we defer to some self-appointed global systems operator, elect an online sheriff, or lock our own electronic doors and issue digital invitations sparingly?

In the offline world, the primary argument for democratic election of representatives is that voting is the best way to determine the will of the people, and that giving people a vote assures the legitimacy of the regime and the willingness of the people to abide by its laws. That argument does not work as well in the online environment, as currently constructed. The very best way to find out what rules people want to have applied online is to let individuals set and enforce the rules that control the actual operation of their own machines. The internet is not television. What is available on your screen is not necessarily a function of the decisions of some remote authority. Individuals now have routers and firewalls in their own homes. These devices can be set, often with the help of the user's ISP, to refuse all packets not originating from trusted and adequately identified sources. On average, any centralized authority (even if democratically elected) is more likely to be wrong about the real desires of individuals than are those individuals themselves.

Offline, no individual can meaningfully make (or lawfully enforce) a "law" against another's acts. Online, you can decide whom you are willing to trust, and you can make everyone else disappear entirely from your own version of the internet. This sounds like a drastic measure, and it is. But we believe the reversal of the connectivity presumption will lead, over time, to re-growth of a much more valuable, and still very diverse, internet.

Because only the peer production model distributes the selection of rules to the end points of the system, it is inherently "wiser" about which outcomes should be sought. We recognize that people can be irrational or can misperceive their own values or goals. But so, too, can governments. We also recognize that ISPs may over- or under-link or filter. Provided those decisions are adequately visible, and an individual can choose to go to another ISP on the basis of these filtering or linking decisions, we believe ISPs will be driven to adoption of optimal rulesets for the groups they serve.[51]

Only peer production of governance can claim systematically to serve every individual equally, and, thus, not systematically to disserve any individual in order to increase the welfare of the larger group. Even without a written constitution, the peer production of governance (by means of trust-based connectivity) is inherently "just," in our sense of this term. It is also effective, because the software code barriers on which it relies are more likely to be obeyed than any set of laws that must be enforced by means of physical force wielded by the police of local sovereigns.

VI. OBJECTIONS TO THE PEER PRODUCTION OF INTERNET GOVERNANCE

Our preliminary look suggests that the accountable internet will produce an optimal kind of social order, provided we all make the choices required to filter out bad actors and share the work of attaching good reputations to those who deserve them. But there will be those who argue strongly that good governance can only come from governments. We attempt in this section to deal with some of the many flavors of that argument.

A. Decentralized Decision-Making Does Not Produce Social Order.

Some might say that the rules developed by decentralized actions do not constitute a form of social order at all, because they are not embodied in any single authoritative text or even in

[51] In contrast, when governments order ISPs to filter, but do not then make transparent to users (or, citizens, for that matter) what sort of filtering is occurring, their decisions are not checked by the independent decisions of individuals. *See* Zittrain & Edelman, *supra* note 19

widely-shared norms formulated with the well-being of the group in view. Our answer to that objection is that the social order resulting from individual decisions (about who to trust and with whom to connect) is an emergent kind of order. Even though each individual's action is taken merely to establish and enforce rules that the individual finds satisfying, the combined impact of such individual decisions creates something very much like a societal rule, albeit one that can be much less uniform in application than authoritative texts usually purport to be. If most people decline to accept your email, your messages may or may not get through to your intended recipients, depending on (1) the degree to which those who accept your communications decide to pass them along, and (2) the degree to which these intermediaries are trusted by those you are attempting to reach.

In the world of peer production of governance, reputation is everything.[52] Reputation is decidedly not equally distributed. Everyone's bits are both equally powerful and equally powerless against an emergent consensus (among a network of peers) that someone is or is not to be trusted. The social order created by decentralized decision-making is strong enough to create outcasts. These outcasts will not be able to communicate freely with those who do not trust them. The resulting pattern of connectivity (and disconnectivity), and its substantive impact at the informational level, is a form of social order.[53] The real question is whether it is likely to be a better order than that created by traditional governmental means.

B. The Accountable Internet Will Not Work Without Mandated Labeling Standards and Centralized "Trusted Computing" Systems.

A second objection is that decentralized decision-making cannot work unless some centralized authority can (1) require all parties to label their electronic communications accurately and (2) administer the "permissions" that have been granted. How can your system filter out a message from an distrusted other if you cannot tell who it is coming from? The surprisingly easy answer to this objection is that, once persistent authenticated identifiers become widely available, you can set your defaults to filter out anyone you do not have an affirmative reason to trust. This does not require any mandatory use of a particular type of identifier or any centralized system for administering permissions.

As discussed above, there are many good reasons not to create a centralized authority. And centralized rules are not required to mandate accurate labeling as long as (1) you can tell when something does not have a trustworthy (secure, authenticated) identifier, and (2) you can reasonably decide to filter out communications from those who have not yet proved themselves. Once it becomes easier to authenticate oneself, many people will do so and it will become reasonable to reject unauthenticated traffic. Once some critical mass of users adopt authenticated identifiers, we will not need a global authority to establish the conditions for this new form of social order to emerge.

C. Unaccountable, Private, Non-State Actors Will Set All the Rules.

A third variation of the objection that only governments can create good governance takes the following form: individuals will inevitably delegate power to groups to make filtering/connecting decisions for them, and these groups will be corporations and private parties likely to act irresponsibly, making choices for private gain rather than in the individual's best interests. It is true that, for whatever reason, most people do not adjust the defaults for computer systems or software, much less carefully review in advance the policies of the ISPs they use to connect to

---

[52] Reputation in the ecommerce world has been shown to be extremely important. *See* Paul Resnick, Richard Zeckhauser, John Swanson and Kate Lockwood, *The Value of Reputation on Ebay: A Controlled Experiment,* at http://ksgnotes1.harvard.edu/research/wpaper.nsf/rwp/RWP03-007?OpenDocument (accessed January 15, 2004).

[53] Those who are cast out will need to rebuild relationships, one connection at a time, in order to communicate. Provided competition for access providers remains strong, there will always be a place to start again.

the internet. There is every reason to expect that online spaces will set the policy defaults for individuals. But if those defaults and policies have an impact, such as allowing too much spam or permitting privacy violations or security breaches, users notice. As long as there is some reasonable level of competition among ISPs, and some awareness on the part of individuals that they can mold the contours of the internet to which they choose to connect, such actions by corporate agents are part of the reason why decentralized governance can be so effective.

The key difference between peer governance and centralized forms of governance is that, in the context of decentralized governance, individuals are free to choose which sources of defaults (or of reputational advice) to defer to. Competition among such sources for increased adherence will lead to more and more effective systems.[54] As long as no such system can claim anything approaching a monopoly, much less sovereignty, all such systems will compete for new users at the margin and, therefore, will tend to remain accountable to the individuals who adopt them. No majority group can enforce their adoption on any minority that finds some other source of reputational information, or policy defaults, more attractive. Thus, the formation of intermediary groups is a feature, not a bug, of peer governance, provided that any such intermediary must compete for new customers.

To be sure, there are some countries in which the only ISP is, in effect, the government. And failures to enforce the antitrust laws could lead to situations in which particular corporations can dominate part of the technical infrastructure. But even such concentrations of power only produce a threat of overblocking. If an ISP or corporation underblocks, it will still be possible for the individual to override that decision by installing an additional set of filters on her local machine. Better variations of filters are likely to evolve if there is some market demand for them. Thus, even if some online intermediaries fail to provide the kind of filtering that individual users want, individuals may well be in a position to provide it for themselves. We acknowledge the threat of overblocking, and our hope is that adequate competition and the world's diversity will mitigate this threat.

D. Peer Governance Will Squelch Free Speech.

Some will protest that any such system will prevent anonymous speech and, thereby, harm political freedoms.[55] Our answer to that objection is that anonymity does not need to be prohibited to allow accountability. There is no particular reason why a receiver needs a real-world identification of the source in order to make decisions about whether to accept a packet or not. We see a key difference between authentication, on the one hand, and identification, on the other. All we need is to be able to tell the difference between the case in which a speaker (packet sender) stands by a verifiable reputation (including the reputation of a pseudonym) and the case in which there is no way to tell anything with confidence about the source of the communication. Under the emerging system of trust-based communications, we can certainly allow anonymous communications. Indeed, nothing in the system that is emerging prevents a decision to send or receive messages that lack any authenticated identifiers.[56]

We understand the need to assure that there is some way for unpopular points of view to be heard. But one person's right to distribute a political flyer without source identification is not the

[54] Some systems may compete by disclosing their policies, but some might compete solely on the basis of results. We believe that online email hosts that limit spam will attract more customers, regardless of whether they explain in public exactly how they do so. Obviously insecure systems, which expose users to unnecessary virus risks, will be shunned.

[55] In addition to the concerns about squelching speech, some scholars have considered, from a positive rather than normative viewpoint, the social effects of anonymity on online behavior. *See e.g.,* Michael Tresca, *The Impact of Anonymity on Disinhibitive Behavior Through Computer-Mediated Communication*, at http://www.msu.edu/user/trescami/thesis.htm (accessed January 15, 2004). Such studies tend to find that anonymity encourages antisocial action.

[56] An interesting question that emerges from this analysis: should we treat a sender who has no reputation and history associated with his or her identity differently from someone with a long and checkered history? Done right, that choice would be up to the end-user, or the recipient of the communication. Different rulesets will deal with this question differently.

same as another person's duty to read that flyer.[57] Moreover, we do not accept the suggestion that trust-based connections will confine most people to hearing only ideas they already believe.[58] Almost any point of view is popular with some people, and some of those people are trusted by others. The relatively few people who are most densely connected to others will have the power to push a new or unpopular idea into widespread distribution.[59] We admit that the new trust-based system may affect the speed with which unpopular views propagate. But it certainly does not eliminate them.[60] It may assure that the surprising/unpopular messages that get through receive greater attention, because they will, when received, have been recommended by a trusted source.

Even if the initial state of your online communications is set to "only talk to people I know," this does not create a world in which you cannot be reached. To the contrary, one by one, indirect communications that are based on actual trust and the recommendations of friends will begin. We are all only a few links away from everyone else. Most valuable messages will get through, if only because a sender of a valuable message can route it indirectly through others who are trusted by the intended recipient and who (if the message really is valuable) can and will add their recommendation. There is nothing "rigid" about the resulting pattern of connections. This new social top layer of the internet protocol stack will evolve flexibly in response to actual relationships among people, rather than as a result of updates to automated code-based embodiments of security algorithms that can easily fall out of date. And it will preserve both the freedom to speak and the freedom to decide when to listen – both of which are prerequisites to personal autonomy.

E. Self-Contained Communities of Wrongdoers Will Flourish.

Some may object that decentralized decision-making cannot effectively prohibit the actions of small groups of wrongdoers who agree to connect to one another. Even if virtually everyone acts to cut off any connection to those who distribute child pornography or facilitate gambling, for example, a group of child porn or gambling enthusiasts could still remain online connected to one another. To the extent that child pornography involves the exploitation or abuse of children, the local sovereign where such acts occur would still surely have the ability and duty to take appropriate legal action to prevent and punish such action. Similarly, to the extent that online gambling requires the use of payment mechanisms that are regulated by local authorities, it has been shown that this local connection provides the ability to regulate such activities to a substantial extent.

More importantly, what makes most wrongful actions wrongful is their impact on unwilling victims. If everyone who wanted to avoid any particular content was able effectively to eliminate it from view, by declining to connect to others who sponsor or support such content, then the amount of harm that can be done by any set of bits, considered only as bits, is quite low.

F. Decisions to Disconnect/Connect Will Be Inaccurate.

---

[57] McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995); *see also* 10th circuit opinion, confirming, with respect to the national do-not-call-registry, that "the ancient concept that 'a man's home is his castle' into which 'not even the king may enter' has lost none of its vitality," and asserting that the First Amendment does not prevent the government from giving consumers the option to avoid unwanted sales pitches: "Just as a consumer can avoid door-to-door peddlers by placing a "No Solicitation" sign in his or her front yard, the do-not-call registry lets consumers avoid unwanted sales pitches that invade the home via telephone, if they choose to do so."

[58] We do not agree, in general, with those who suggest that the internet encourages people to listen only to others with whom they agree. The accountable net would surely result in people being exposed to less unwanted information than under the current model. However, we trust individuals enough to seek out diversity of information and viewpoints, trusted not simply because the individual agrees with the viewpoint, but because it is worth hearing and considering and is not likely to be laden with viruses or worms. *See, e.g.,* CASS SUNSTEIN, REPUBLIC.COM (2001).

[59] Consider the online version of six degrees of separation.

[60] We disagree with those who suggest that there is a right to spoof. That is like claiming a right to commit fraud. Spoofing cannot be considered harmless from the point of view of those who want to know the identity of those with whom they are communicating.

In a world in which one must gain trust in order to be connected, and in which wrongdoing is punished by banishment, there is a risk of overreaction and collateral damage.[61] Some ISPs may refuse to take traffic from IP numbers or domains that contain, or serve, many entirely innocent parties.

It is true that life in our projected online world may not be fair. We must admit that, at least on paper, many traditional governmental processes are better able to assure that punishment is not meted out until someone is proven guilty. There is little use of guilt by association in the laws of western democracies. On the other hand, the peer production of governance does not put the power of banishment in any one entity's hands. Losing the ability to communicate directly with the users of one ISP does not mean you are off the net. It simply means you may need to get a recommendation from someone who does not use that ISP, and who is trusted by those who do, in order to get your message through. True, filters can be overly blunt instruments. But the accountable internet provides multiple second chances. To the extent we fear that the membranes of the accountable internet will start out with too few holes, we should remember that the net was originally designed to "route around" barriers. Our digital membranes will become more permeable over time -- without posing unacceptable risks to those who connect.

Moreover, we all have incentives to use the most precise and accurate filters available. Once we can decide to connect only based on trust, we will create many new ways to establish trust and we will insist that our ISPs not use filters that block large amounts of desirable traffic. Right now, most users experience an internet that seemingly has no effective barriers against wrongdoers. Most users cannot see where any such barriers are or judge how effective they might be. Once we reverse the presumption of connectivity, and demand authenticated identity and a reason to trust as the condition for accepting others' bits, we will also demand better and better ways of seeing the impact of those actions. If your ISP cuts off all of Germany, you will want to know that (and will likely be able to find it out, whether or not your ISP decides to tell you it has done so). How you react to such decisions will increasingly be up to you.

G. Decentralized Decisions Undermine the Values Underlying "Common Carriage" Obligations.

Trust-based connectivity depends on the right of each individual actor (end user or ISP) to decide not to connect. In a world in which phone calls are routed over the internet, the idea of allowing a refusal to connect may seem troubling. We think of physical telephones as lifelines, and we do not take them away, even from convicted criminals. Yet ISPs have never had a duty to take all comers, must less to peer with other networks whose practices are unacceptable. The net may be becoming a vital utility. But we may not be able to preserve it as an orderly, socially valuable network if we give everyone an unqualified right to connect to everyone else. Society can help to establish the conditions for trust, but it cannot and should not mandate trust any more than it can compel communication. We need trust-based relationships to create an accountable social order online, and we may have to give up ideals of universal connectivity along the way.

Perhaps the greatest state change required to allow trust-based connectivity is the change in our assumptions about the social nature of the net at the level of shared metaphor. The net is persistent, and therefore "place-like," but it has never been a single "place."[62] We can now recognize that going "there" does not have to mean exposing ourselves to relationships with those who want to impose costs or harm on us. We can go "there" by increments, deciding for ourselves who else will be able to send us messages, and empowering our ISPs to filter out wrongdoers in various ways.

The prerogative not to connect is vital to our ability to bring order to the online space. This is in part because bits, while equal in force, can be distributed very fast. Some of the packets of bits that wrongdoers want to send us destroy our very ability to communicate with others. There is a

[61] It should be noted that governments are also capable of imposing sanctions in an overbroad way.
[62] Consider the work of Dan Hunter and many others on the notion of cyberspace as place.

clear need to preempt wrongful traffic, once a potential source of it has been identified.[63] It follows that the idea of an inherent right to connect would amount to a right to be trusted for no good reason -- a right the original architecture of the net grants implicitly but that we can and should now decide to revoke. We can now reasonably shift the burden of proof, the burden of persuading a recipient to risk betrayal, to the sender.

VII. WHAT IS REQUIRED TO MAKE THE ACCOUNTABLE INTERNET WORK?

If decentralized decision-making is this good at creating social order online, why has it not already done so? Does our experience with the deterioration of the internet over the last few years show that government intervention is necessary? Even if the peer production of governance will work in theory, is reliance on the sheriff (whether or not elected) necessary as a practical matter? What is required to make the peer production of governance work?

Part of the answer to the first question lies in the novelty of emerging tools and applications allowing us (and our agents) to identify with some certainty who we are communicating with. The internet was created by the decentralized decisions of particular networks to connect with one another. For various reasons, it was originally designed so that the act of interconnection allowed anyone with even one link to the internet to send packets directly to anyone else, without even providing any means for the recipient to verify that the originator of the packets really was the person the bits held him or her out to be. Perhaps because the early engineers already knew and trusted each other, they did not build in any means to make sure that the header information in an electronic packet was correct.

That design was unnecessary and runs counter to the most fundamental needs of our social systems. We cannot trust each other unless we know whom we are trusting. We need to be able to threaten to disconnect in the event of a betrayal. This inherently requires that we connect only to those we trust.

At the least, we can now know when a proffered communication is coming from someone whose identity we cannot be sure about. We will be able to decline to accept such messages, as a practical matter, once most of the messages we want will come from those whose identity will be able to be authenticated.

But the technical tools to provide authenticated identity and to insist upon it are not enough. We also need to establish some baseline conditions that are necessary to the success of this new decentralized means of producing social order online.

- First, we must prevent the acquisition of monopoly power by any internet service provider. If there were only one way to get onto the net, then users would not be able to choose among differing policies regarding which connections to risk and which filters to deploy. Where some natural monopoly limits our choices among transport providers, we may need to insist that transport be separated from the provision of filtering options, in order to preserve the needed competition among rulesets.[64] Perhaps increasing abilities to create wireless networks with our neighbors -- networks that are not necessarily owned or controlled by any central authority -- may help to solve this problem. It may be that the very category of "internet service provider" as a business will be rendered obsolete by the emergence of these *ad hoc* networks.

[63] The internet is not like print publication, with respect to which we may well want to discourage any prior restraint.

[64] An interesting issue arises here about portability of user identifiers. Once transport is separated from the filtering layer, it may be easier for users to move from one transport provider to another while still retaining their identities and reputations. Some form of portability of identifiers may be needed in order for user choices among providers to be affordable as well as real.

- Second, we may need to insist that any intermediary that imposes filters disclose what it is doing.[65] There cannot be a marketplace among alternative filtering solutions without disclosures that allow users to make meaningful choices among alternatives. Senders of messages must be able to determine when they will have to take extra steps (e.g., seeking a recommendation) in order to assure that their message gets through. In the context of overblocking, we agree that "PICs is the devil."[66] But overblocking by system operators will become less likely as effective controls over connectivity by end users become possible.

- Third, we will need better tools that do more than connect and/or filter. We should call for the development of tools to allow us to visualize which other sets of users and which parts of the internet are accessible from any particular location. We need to develop and deploy more capable software allowing users to compensate, at their own machines, for underblocking by intermediaries.

Admittedly, there is a major state change required to make trust-based connectivity feasible. There have to be enough people and networks using authenticated identifiers so that it becomes reasonable to refuse messages/packets from those who are not doing so.[67] We believe that this state change will occur over the next several years, pushed along by several different forces -- including work by internet standards bodies and the commercial needs of businesses and ISPs. It will happen both in stages and in parallel. It may be that all those served by a particular ISP, for example, will begin demanding authentication of emails. Once two or three large ISPs join in, many individual users will see the benefits of adopting a trust-based connection approach to "their" internet, and the system will begin to change quite quickly. This new internet (or, initially, collection of internets) will evolve towards a better state because it will create trust-based connections that are likely to be positive (rather than merely filtering out random negative events). This new internet may initially be made up of virtual networks that do not connect to one another. When a single trust-based connection is made between two such networks, however, they will be reconnected, with all nodes at least indirectly (by recommendation) accessible to each other.

There may additionally be steps that local sovereigns could take to facilitate the development of decentralized governance. Offline, many towns take the initiative to encourage a neighborhood watch. The neighbors actually do the watching, but governments recognize that their law enforcement burdens will be minimized to the extent that they can encourage individuals to take responsibility to protect themselves. The online world is just as amenable to the creation of civic improvement organizations. Such private sector collective action can create real communities, voluntarily chosen by participants. So perhaps the most important thing for governments to remember is that an orderly online society will depend less on traditional law enforcement (with the default of the government trusting no one and seeking to control the actions of all) and more on the success of private actors in collaborating to build expanding circles of trust and clean up the neighborhood they have chosen to inhabit.

What we are positing is a state change that will amount to the addition of a new social layer to the internet protocol stack. It may be that the old internet cannot survive this change entirely intact.

---

[65] See n.11 regarding potential counter-productivity of a transparency requirement. Effective competition among those who provide access to the internet can dramatically increase the leverage of any system that uses decisions about connectivity/banishment to control wrongdoers.

[66] *See* n. 38, *supra*.

[67] We are suggesting that individuals should demand that their ISPs (and other networks that provide them with access) not agree to connect with others who, directly or indirectly, connect to still other networks that are not worthy of trust. And all networks should be obliged to banish those who betray our collective trust. Both levels of this system require the availability of authenticated (non-spoofable) identifiers -- because you cannot condition connectivity on trust unless you know who you are or are not connected with. It is just such identifiers that are now becoming available, which is why we now will have the option of building a personalized internet based on established trust and recommendations from those we trust.

But we think the new society of the internet these changes allow us to build will be better than the likely alternatives.

VIII. WHY PEER PRODUCTION OF GOVERNANCE WILL WORK

We think there are very deep reasons why, once the right tools are in place, and provided we collectively decide to use them, and also provided that governments encourage effective competition among intermediaries and constructive action by online civic organizations, peer production of governance will work.

A. Beneficial States Are Stable.

Order emerges naturally from decentralized action because, in general, beneficial states are stable and non-beneficial states are not. Good connections persist, and bad ones, those that produce negative effects, tend to be severed. We know this intuitively. Our circles of friends and colleagues constantly change to allow us to give more attention to those who are "good for us" in various ways. We do not need laws or kings or Congressmen to tell us what social networks to join.

B. Humans Are Wired To Trust and Form Networks.

As biologists and economists are now beginning to realize, we are wired for trust. Contrary to the Hobbesian view, human nature is designed to create relationships, not to seek selfish advantage. We all do better by cooperation. We are the children of ancestors who benefited from belonging to a tribe. Using a filtering/trusting mechanism will not result in the creation of disconnected electronic islands, because humans want very badly to be part of the social fabric. Even if we start by excluding all messages from strangers, complex social molecules will still form online.

The special evils introduced by the internet have resulted from the elimination of costs and friction that make entry into relationships in the real world more deliberate. Offline, we constrain wrongdoing by threatening loss of access to society. We have spam because it is easy for a stranger, without any invitation, to send a message we cannot entirely ignore. We have privacy problems because it is easy for someone you do not know to sneak a piece of spyware onto your machine and then tell the whole world all about you. We have security problems because our machines were initially set up to be open to management from afar. In retrospect, it is the peculiarly unconstrained connectivity of the internet that should surprise us, not the rise of online wrongdoing in that environment.

We can solve these "harmful bit" problems by making our systems condition connection on the establishment of trust or the provision of acceptable reputational credentials. Even if our ISPs and employers do most of this work for us, we have the ability to constrain their actions. If we take appropriate action, we will get the online social order we naturally desire.

C. Peer Production of Governance is Inherently Congruent.

Peer production naturally creates an optimal degree of mapping between the set of people affected by any given rule and the set of people for whose benefit the rule is made. We will call this "congruence." There is reason to think at least substantial congruence is necessary to allow a complex system to find an optimal state.[68] Indeed, congruence may be the only stable state, in the long term, because a lack of congruence incites revolutions. If you make your own rules, and they primarily affect you (because you do not force others to adopt them), neither you nor anyone else is likely to challenge those rules as illegitimate.

---

[68] David R. Johnson and David G. Post, *The New Civic Virtue of the Internet*, at http://www.cli.org/paper4.htm (accessed January 30, 2004). This article appeared in The Emerging Internet (February, 1998), the Annual Review of the Institute for Information Studies, a joint program of Nortel and the Aspen Institute.

As long as members of online groups can set their own filters on top of those set by the group, then rules that allow messages that particular individuals find harmful will simply cease, over time, to affect those individuals. Obviously, no set of filters can be perfect. Indeed it is vital that some leakage occur to allow the overall system to explore new territory.[69] But, at least as compared with even the best alternatives, decentralized decision-making is more optimally congruent than any form of centralized rulemaking. Any king is more likely to make mistakes about what his subjects want than are those subjects themselves, and even an idealized democratic system involves a lag time between changes in the citizenry's desires and the ability of representatives to act on those desires. If one takes into account the non-benevolence of most kings, and the self-interested actions of most elected officials, there is no question that delegating power to the edge is most likely to ensure a fit between the group whose welfare is sought by the governance regime and the group that feels the actual impact of the rules the system establishes and enforces.

Indeed, peer production of governance works, in part, because it provides no excuse for anyone who might take constructive action to enhance the social order to refrain from doing so. Once you accept the idea that local action can create social order, there is no plausible way to pass the buck to Washington or claim that you need not do your part to protect your online neighborhood. We set up governments for the real world because people were powerless to defend themselves against a ruthless neighboring tribe. That is not the case, in the same way, online. And explicit recognition of the ability of end users to control the flow of messages on their own version of the internet will help to make sure that they do so.

D. Peer Production of Governance Is Inherently Flexible.

Finally, peer production of governance works better than any centralized internet governance system because decentralized decision-making is inherently able more rapidly and flexibly to react to changes in external conditions. All complex systems in nature that "self-regulate" and evolve do so by means of feedback loops, generated by autonomous elements and implemented by decentralized decision-makers. The reputational feedback loops that we see emerging on the internet can constantly adjust to the changing nature of threats to the social order. By contrast, any reasonable process for making or enforcing traditional law is relatively unresponsive.

Indeed, there is reason to think that peer production of governance can work to solve many other online problems. Filters have always been the most useful way of dealing with offensive content. Even fraud becomes harder to perpetrate as reputational feedback loops get better. We have focused on decentralized decision-making to filter out harmful messages/packets. But the other side of peer production of governance is the increasingly effective use of recommendations and reputations to help us find valuable content, find groups with which we can effectively collaborate, and engage in trustworthy commerce.[70] Decisions to trust need not be taken in a binary way. The meta-information that identifies the source of a potentially harmful/valuable packet will be complex, allowing each of us to make increasingly nuanced and context-sensitive decisions about where to direct our attention, when to release our information, and when to engage in risky interactions.

IX. CONCLUSION

[69] 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); Susan P. Crawford, *The Biology of the Broadcast Flag*, 25 HASTINGS COMM/ENT 599 (2003).

[70] We are clearly beginning to see developments along these lines -- e.g., the formation of "guilds" in the context of online games, which serve both to constrain wrongful actions and to encourage new kinds of cooperation. Susan P. Crawford, *"Who's In Charge of Who I Am: Identity and Law Online,"* http://www.nyls.edu/docs/crawford(2.0).pdf; David R. Johnson, *"How Online Games Will Shape the Law,"* http://www.nyls.edu/docs/johnson.pdf.

The key question raised by governments at the December 2003 WSIS was how to create social order, and prevent the harmful effects of antisocial action, online. We do not take it as a given that rules designed primarily to govern online interactions can only be made by national sovereigns. We also do not think that the internet will be best left ungoverned, even if there were any chance of that happening. So we, like everyone seeking to benefit from a valuable social order for the internet, are compelled to ask what form of governance might be best for the online world, given its attributes.

What we think we have shown is that, notwithstanding the famous remark about it being "the worst, except for all the alternatives," even representative democracy is not the best available form of governance for the internet. Decentralized decisions regarding what to filter and who to trust can produce social order more reliably and fairly than even our "best" (most democratic and participatory) means of creating centralized authority and enforcing authoritative legal texts.

If software code is the law of the net, as Larry Lessig has suggested,[71] then, in certain instances, we must take that law into our own hands. The only way to make sure we select code that reliably serves our social values, and that does so effectively when needed, is to insist on delegating the decisions to use such code to the edge of the network. We must therefore become more accountable to one another, as peers (at both the level of the individual end user and the level of the ISP/local network), if the internet is to serve our collective goals. As we make this transition, we ought to do so consciously, recognizing that our joint efforts represent a form of governance. And we ought to seek to mitigate the most troubling of the new paradigm's prospective effects. We may lose some of what we have come to love about the net in the process, but in so doing we will save far more.

We have called this method of social ordering the peer production of governance.[72] It is not entirely new. Online spaces have been governing themselves for some time, and individuals make choices every day about where to go online, what messages to accept, and what to filter out. But new tools that make a robust form of decentralized order possible on the internet are just now being developed and gaining acceptance -- and a recognition of the power of this distinct form of governance is thus newly urgently needed. The sooner we decide to accept individual responsibility to make the choices that help create social order online, the less time we will spend pursuing ineffective alternatives.

We have no doubt that the accountable internet will create new problems and risks of its own. The list of "who you trust" could become a valuable piece of information about you, vulnerable to invasion by the government or others who may not respect your privacy. Whenever we form trust relationships, we make ourselves more vulnerable to betrayal, because those who would defraud or harm us will attempt to ride on top of those trusted connections. Nevertheless, we think an online world in which we are accountable to one another will be a better place than one in which our communications are governed by inflexible, centralized rules.

There is only one internet but there is no global system operator.[73] Even if there were, such an authority would not be accountable to those it ruled. And even if we could elect an online government, it could not make uniform laws without systematically disserving the interests of minorities in a heterogeneous world. But we do not have to cede power over the internet to a central authority. We can rely on the aggregated power of all online actors to decide for themselves who to trust, and with whom to connect and interact. As the internet continues to evolve, new tools that make such choices even easier and more effective will become available. We will be able to begin to insist on authenticated identity (and some reason to trust) as a pre-condition for any communications. And we will be able to banish those who abuse our trust. Our virtual neighborhoods will improve as we all become more accountable to one another, online.

---

[71] LESSIG, CODE, *supra* note 4, at 6.
[72] *See* Benkler, *supra* note 7.
[73] *See generally* Jonathan Zittrain, *The Rise and Fall of Sysopdom*, 10 HARV. J.L. & TECH. 495 (Summer 1997).

28