

## Trusting the Net in Developing Countries: Peer Production of Governance

*David Johnson, Susan Crawford, and John G. Palfrey*

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. Others, particularly those representing countries in the developing world, suggested that there is already a *de facto* online sovereign, the United States, and decried this state of affairs. 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 (such as the Internet Corporation for Assigned Names and Numbers, or ICANN) with new powers to control online wrongdoing. Most at WSIS seemed to agree that some new sheriff is coming to cybertown and should be welcomed.

We predict that the Internet will become more orderly over time, as new technologies emerge that permit greater levels of authentication and that rely increasingly on trust between parties. But we do not agree that the Internet needs, or will easily yield to, more centralized authority—private or public. Contrary to conventional wisdom, we are unconvinced that greater centralized control is necessarily better for people accessing the Internet from developing countries. Instead, 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 in developing and developed countries alike greater control over their digital connections. They will enable both end users and access providers to establish affirmative 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. They will help empower Internet users to do right by one another and to avoid, more easily, those who would do harm. These technologies will help to keep decisions closer to the user—more local, closer to the edge, with less interference from the hub.

For example, GoodMail is a company with a plat-

form that aims to restore trust in e-mail and in messaging generally by creating trusted class e-mail. Goodmail’s goals are to improve the consumer e-mail experience while shifting the economic burden from the recipients to the senders. The system achieves trusted intermediation and messaging by accrediting senders and authenticating and labeling messages. The second goal is met by employing a per message fee on the sender. The sender’s behavior is controlled by the number of complaints registered with GoodMail against that sender.

Yahoo! gives users installing their instant messenger platform the option of preventing people not on their buddy list from contacting them. Yahoo!’s solutions attempt to empower users to make decisions about trade-offs. Yahoo! is also developing DomainKeys, an e-mail solution that allows for domain authentication. Yahoo! does not necessarily bounce incoming e-mail that fails authentication, but routes it to a bulk mail folder. Yahoo! is also using SquareTrade to verify particular categories of online merchants—for example, to verify that a particular company is authorized to sell regulated items. Yahoo! sees this as a way to provide a trust label for a transaction.

These new technical developments will render participants on the Internet more accountable to one another than they have been in the past. By creating a greater degree of accountability among participants on the Internet, these systems give rise to the possibility of peer production of governance, a mode of governance to which governmental sovereigns ought to defer in those areas where it works. Peer production of governance will serve those in both developed and developing countries better than a heavily centralized model, dominated either by the strongest actors in the political process (in a UN-centric model) or the most powerful technology companies (in a centralized private-sector model). Problems such as spam and spyware, which have to date resisted a broad array of ordinary legislative fixes, will be more easily tackled by peers putting trust to work online.

The conventional wisdom suggests that people from developing countries would be best served by a centralized body, such as one under the rubric of the United Nations, taking control of the governance of many Internet-related functions. Even the harshest critics of UN involvement in Internet governance must acknowledge that there are some good

## FORUM

reasons to concur with this line of reasoning. The UN system has a series of safeguards for all participants built in, whereas *ad hoc* organizations, such as ICANN or standards bodies, rarely have such reliable safeguards in place. Where *ad hoc* organizations have these safeguards in place, they are inconsistent and it is often hard to ascertain exactly how best to participate, despite protestations to the contrary. By contrast, most countries already pay to send qualified permanent representatives to UN sites such as Geneva and New York. The mode of participation is clear. Developing countries know they will have something of a voice and that, by banding together, they can at least make a forceful argument in favor of their collective interests. But we fear that a decision to create an international "Internet governance" body would not serve developing countries well in the long run.

The decision with respect to Internet governance for those in developing countries is not between a United Nations model, an ICANN model, or complete anarchy. None of those choices is ideal for dealing with most problems on the Net. The decision is rather between, on the one hand, a centralized control system and, on the other, an environment in which we rely upon the emergence of trust-based networks among peers to solve some of the most persistent, distributed problems online. And the decision ought to be made not wholesale, but rather by looking hard at which problems require centralized authority and which can be solved in a peer production mode.

We acknowledge that there are collective action problems that arise on the Internet that require some other form of "governance" to resolve. Online problems that plainly call for some form of governance include, but are not limited to, spam, identity theft, and network security. Many of these problems have been created by the ease with which antisocial individuals can take harmful action at a distance in this new global medium. Traditional models of governance may not be as effective in regulating problems that exist solely in the online world. The job of those thinking about Internet governance—a hard one, to be sure—is to identify the most pressing problems, and not to insist on global governance schemes where they are not needed. For those in developing countries in particular, as connectivity and access spread slowly but surely, the choices

made now could have ramifications far into the future.

For any given online collective action problem, we ought to consider three alternative models of governance: 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). The first two models, when extrapolated to global problems, present the very real risk that the relatively low market and political power of developing countries will result in decisions made by those in the most powerful countries that do not necessarily map to the interests of those in less powerful regions. By contrast, a decentralized model offers the possibility of keeping decision making on most Internet issues local. Of these options, sovereignty resides closest to the user in the peer production model.

The Internet presents new opportunities for dealing with the problems it creates, stemming 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. A new form of order is emerging based on this peculiarly digital balance of power. 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. The basis of these mechanisms is an infrastructure that provides contextually appropriate authentication or accreditation, allowing individual parties to decide whom to trust and whom to filter out entirely. This approach creates a new presumption that we connect only with those who are worthy of our trust. The goal is an Internet where good behavior is fostered locally, and our firm belief is that trust-based networks will yield valuable connections between would-be collaborators. We are confident that any 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.

As in the offline world, the question of online "governance" is about allocation of control over the available means of making and enforcing rules. Offline, we have settled on theories of governance that accept the need for centralized power and top-down rules. 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. It's a distinction that makes a big difference in the governance debate.

Because the Internet involves a 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, like spamming. When we can choose with whom to connect, the online society we encounter will reflect 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.

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 in the long run. This form of governance is newly enabled by tools that allow accurate identification of the sources of messages 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, and it will require a growing understanding that establishing a connection with others across the Internet represents a social contract, a breach of which should lead to ostracism. As these tools are just now emerging—though not yet in widespread use—now is precisely the wrong time to give up on peer production governance mechanisms and devolve power to a more centralized force. This strategy is most compelling for developing countries whose Internet environment is beginning to take shape, and for whom the decision to devolve power away from the user might be the most costly.

There are deep reasons why peer production will work once the right tools are in place, and provided we collectively decide to use them, and provided further that governments encourage effective competition among intermediaries and constructive action by online civic organizations. Order emerges from decentralized action, when many individual de-

isions to control online environments result in beneficially stable states. Humans naturally trust and form networks, social and otherwise, creating constant pressure to establish societal links. Peer production of governance is inherently congruent, creating 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. And peer production of governance is inherently flexible, similar to complex systems in nature that "self-regulate" and evolve by means of feedback loops generated by autonomous elements and implemented by decentralized decision makers.

Peer production of governance does not simply mean to accept whichever technical or economic solution is proffered by the leading technology companies. For example, some of the proposed technical solutions to problems that an accountable Net seeks to address—like spam—are not particularly good ideas from the perspective of developing countries. For instance, the series of ePostage proposals to address the spam problem—charging a small amount to senders of e-mail in order to change the financial dynamic of spam—would require a huge investment in infrastructure to participate. For a developing country in which fewer people have access to credit or bank accounts, such a scheme could dramatically undercut the growth of the Internet at a critical moment. To rely on peer production of governance means to choose from among technical and service offerings those that make the most sense for users in a given part of the network.

Developing countries—or any country for that matter—need not give a central government or private sector players from afar the power to use the electronic equivalent of force in order to assure adequate online order. The aggregation of numerous individual decisions about whom to trust and whom to avoid will create a diverse set of rules that most accurately and fairly serves the local interest and diverse values of all of those who use the online world. The local sovereign, with the collaboration of sovereigns in other parts of the world, should be there at the ready to prosecute extreme cases, like fraud, misrepresentation, and malicious security breaches. Developing countries should seek to build local trust in the Net and develop the capacity to use "peer production of governance" to address some of the thorniest collective action problems that arise in the online context. Through social ordering

## FORUM

and use of the right tools, peers can get much of the online governance job done together. This ordering may be as simple as configuring Eudora e-mail clients more effectively, choosing with greater care ISPs based on their service offerings, or building forms of greater accountability into peer-to-peer networks through Creative Commons licenses and similar, nontraditional governance approaches.

The point is neither that those representing developing countries ought to ignore the WSIS process, nor that no form of government involvement in Internet-related affairs is ever warranted. Governments in developing countries can and should build enforcement capacity, as well as strong bridges with law enforcement officials in other parts of the world, to crack down on the worst crimes that occur online. But there are also great benefits to people in developing countries in relying on the peer production of governance to reduce the impact of certain problems—like spam, identity theft, and certain security issues—and to take advantage of the private ordering that can stem from increased trust-based communications. It would be a mistake to give up on localized decision making on the Net just as peer production of governance is emerging as a feasible alternative. ■

© 2005 The Massachusetts Institute of Technology  
Information Technologies and International Development  
Volume 1, Number 3–4, Spring–Summer 2004, 73–76

## Universal Access and the Rural Challenge

*Pierre Guislain*

The exclusion of part of the world's population from access to information and communication technologies (ICTs) was rightfully a major concern at the World Summit on the Information Society (WSIS) held in Geneva in December 2003. By the time world leaders reconvene in Tunis in November 2005, countries are expected to have adopted and started implementing strategies to bridge what is often called the domestic digital divide, which separates the urban classes who have access to ICTs from the rural and poor who do not.

Access to ICTs is defined in different ways, including geographic proximity, affordability, content relevance, and people's capacity to effectively use technology. Fundamentally, however, access depends on information and communication infrastructure. The goal is to use the terms of the WSIS Plan of Action, access that is "universal, sustainable, ubiquitous, and affordable."

The universal access challenge may not be as big as some may think. According to ITU data for 2002, over half the world's households (more precisely 57%) already have fixed-line telephone service. The mobile picture is better still, with mobile phone signal available to over 80% of the world's population, exceeding 60% even in low-income countries. Extending access to universal levels will require servicing the most hard-to-reach in low-income countries, the majority of whom live in rural areas.

Creating an environment that encourages private firms to provide service is the first and most important step in expanding access. This means abolishing barriers to new entry, fostering competition, and establishing a level playing field for all players to reduce costs and enable new solutions for rural and remote areas. Currently about half of low-income countries have opened their mobile telephony markets to full competition; but only 15% have done so for their fixed-line local loop. This represents a considerable lost opportunity. To illustrate the potential of effective competition, consider Morocco. The Moroccan mobile market had 116,000 subscribers in 1998 when it was opened to competition. By 2002, the number of subscribers had exploded to 6.2 million, representing a year-on-year growth rate of