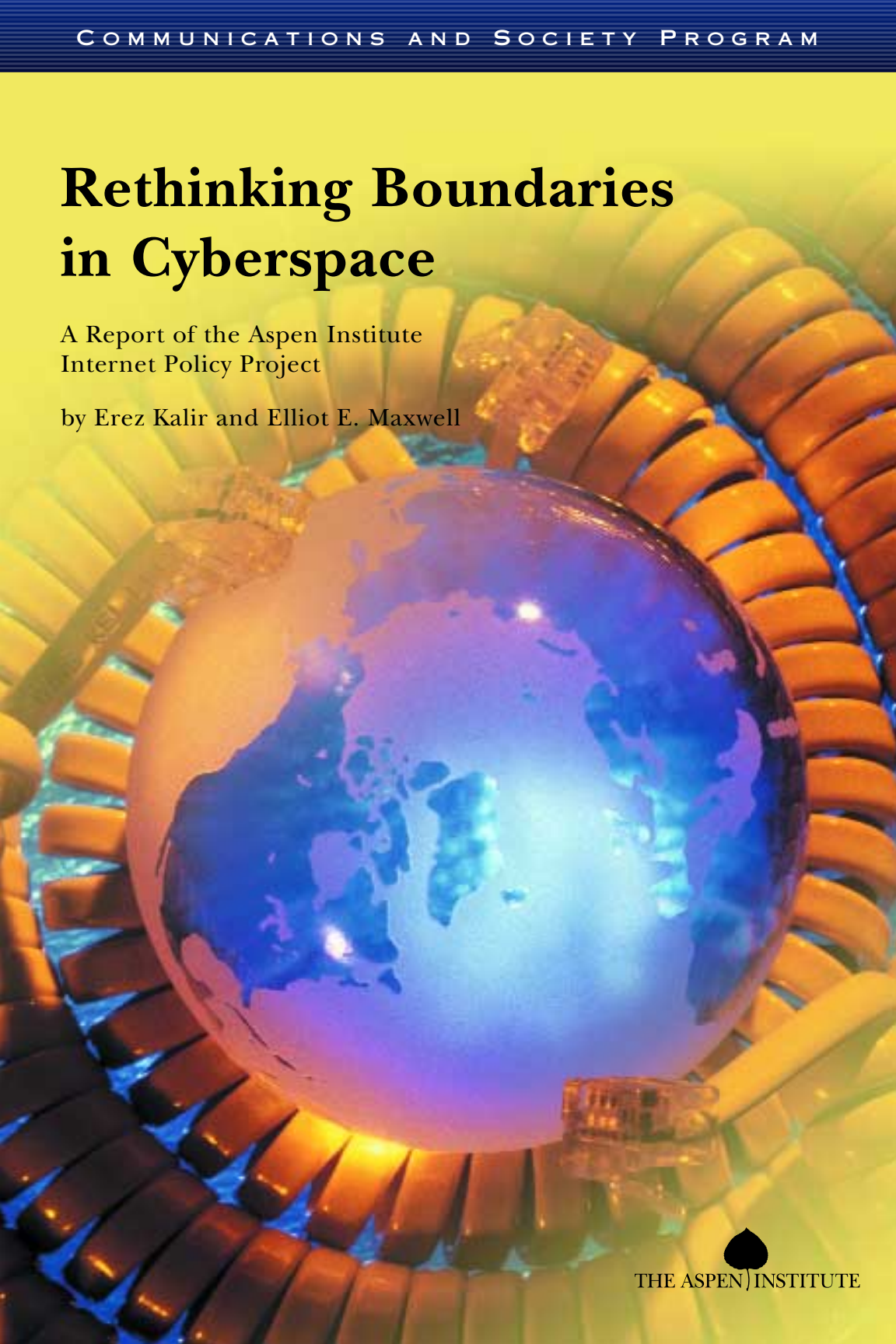


# Rethinking Boundaries in Cyberspace

A Report of the Aspen Institute  
Internet Policy Project

by Erez Kalir and Elliot E. Maxwell



# Rethinking Boundaries in Cyberspace

A Report of the Aspen Institute  
Internet Policy Project

by Erez Kalir and Elliot E. Maxwell



THE ASPEN INSTITUTE

*Communications and Society Program*

Charles M. Firestone

Executive Director

Washington, DC

2002

*To purchase additional copies of this report, please contact:*

The Aspen Institute  
Fulfillment Office  
P.O. Box 222  
109 Houghton Lab Lane  
Queenstown, Maryland 21658  
Phone: (410) 820-5338  
Fax: (410) 827-9174  
E-mail: [publications@aspeninstitute.org](mailto:publications@aspeninstitute.org)

*For all other inquiries, please contact:*

The Aspen Institute  
Communications and Society Program  
One Dupont Circle, N.W.  
Suite 700  
Washington, DC 20036  
Phone: (202) 736-5818  
Fax: (202) 467-0790  
Web address: [www.aspeninstitute.org/c&s](http://www.aspeninstitute.org/c&s)

Charles M. Firestone  
*Executive Director*

Patricia K. Kelly  
*Assistant Director*

---

Copyright © 2002 by the Aspen Institute

**The Aspen Institute**  
One Dupont Circle, NW  
Suite 700  
Washington, DC 20036

Published in the United States of America in 2002  
by the Aspen Institute

*All rights reserved*

Printed in the United States of America

ISBN #0-89843-336-3

02-007

1142/CSP/02-BK

# Contents

**FOREWORD, *Elliot E. Maxwell***.....v

**RETHINKING BOUNDARIES IN CYBERSPACE,**

*Erez Kalir and Elliot E. Maxwell* .....1

    Prologue: Why a Conference on *Internet Governance*? .....3

    Trends and Challenges: Where We Are Now .....7

    Guiding Principles .....13

    Roles of Different Actors (I):

        Traditional Governments .....21

    Roles of Different Actors (II):

        Alternative Governance Organizations .....26

    Roles of Different Actors (III):

        Corporations, Traditional NGOs, and Users .....30

    Coming Full Circle: Three Specific Governance Challenges .....35

    Conclusion.....41

**APPENDIX**

    List of Conference Participants .....49

    About the Authors.....51

    The Aspen Institute Communications and Society Program.....53



# Foreword

The Aspen Institute's Internet Policy Project has never lacked ambition. Under the leadership of David Johnson, one of the pioneers of cyberlaw, and then Andrew Shapiro, an influential commentator on Internet issues, the Project sponsored a series of small group meetings and workshops aimed at helping to create an intellectual framework for Internet policy. These meetings focused on the privatization of the domain name system, Internet privacy, the impact of the Internet on intellectual property rules, jurisdiction in cyberspace, the legal nature of e-commerce transactions, and the applicability of self-regulation and self-ordering to the resolution of Internet-related issues. It was an agenda fitting the fulsome ambitions for this new medium. The meetings resulted in significant contributions to the development of new approaches to Internet governance and policymaking.

During the past year, the Project has focused on the next generation of Internet issues. In the early days of the Internet, many commentators saw it as a special place, "borderless" and free from government intervention, a locale run by and for its participants. Even in the first major Internet policy statement by the U.S. government in 1997—The Framework for Global Electronic Commerce—the emphasis was on private-sector leadership regarding Internet policy. But as the Internet has grown in visibility and importance—economically, socially, politically, and culturally—and as the number of international transactions utilizing the medium has exploded, it is no surprise that governments around the world have begun to give it greater scrutiny. In many cases governments have begun to pass laws and regulations seeking to control conduct and content on the Internet, within and beyond their borders.

In the summer of 2001, 24 participants—leading entrepreneurs, technologists, academics, and policy advisors—took part in a three-day conference convened by the Project titled "Rethinking Boundaries in Cyberspace." The conference agenda focused on the growth of government involvement in the Internet and, in particular, the implications of the exercise of extraterritorial reach by

governments in areas such as privacy, taxation, content regulation, and the sales of goods or services. A central question, given the global nature of the Internet, is who will make the rules governing these and other issues, and what values will underlie these rules. Will rules be made by local, national, or international authorities, by governmental bodies or by private-sector actors? Will the rules encourage or discourage the continued growth and development of the Internet? These questions have even greater resonance in the post–September 11th environment as governments focus on security issues and seek to extend their jurisdiction worldwide in order to battle terrorism.

This question of who will make the rules is not new: It has been addressed in the context of the privatization of the domain name system. But the broad range of issues of interest to governments dramatically raises the stakes. The exercise of sovereignty by physically based states could result in new borders on the “borderless” Internet, policed using rapidly developing location-identifying technologies. Imposition of national policies, based on values that vary from country to country or locality to locality, raises the possibility of segmenting the global Internet into a series of regional, national, or even local data networks.

But control of the Internet by governments was not the only issue of control raised at the meeting. The conference also recognized the rise in “private governance.” As Larry Lessig and others have pointed out, more and more “policy” decisions are being made by private players and are being embodied in the hardware and software that allow access to the Internet and provide its myriad applications. These policies found in “code” are part of a larger trend whereby private actors make decisions that in the “physical world” would be the province of governments. In some cases, governments have delegated responsibilities to private firms (as in the most recent Council of Europe Treaty), deferred to industry self-regulation, or allowed firms to exercise control based on the firms’ own view of competitive advantage. If private firms are going to be the ones who make the rules for the Internet, it is important to understand the values and criteria they will employ.

At the same time, there is a technological arms race between those who seek to expand control and those who seek to minimize or

escape it. Technologies to provide anonymity or promote privacy continue to develop. They offer mixed blessings: protecting private information or shielding dissidents from oppressive regimes and at the same time allowing bad actors to escape their just rewards. The conference examined one of these technologies—peer-to-peer computing—which undermines control because of the absence of any central point of authority. These technologies, coupled with the rise of new communities such as those of the instant messaging world, are simultaneously being praised for their ability to support collaboration and resource sharing and condemned for facilitating massive violations of copyright law.

The debates over control will surely continue. They must, because the stakes are so high. They involve the central characteristics of the Internet: the ability to communicate and collaborate with anyone online; to access staggering amounts of information hosted around the world; and to choose content, services, and features on the Net free from constraints built into the network itself. The consequences of choosing the wrong path are a dramatic decline in the political, social, and economic innovation made possible by the Internet.

The conversations at the meeting were exceedingly rich. The following report is not a simple summary but an attempt to extract the most salient themes, provide a useful context in which to view them, and identify issues worthy of future dialogue. The rules under which these Aspen meetings take place encourage wide-ranging dialogue that focuses on underlying values—in this case those of communications, collaboration, and community. The Internet has broadened our sense of the possibilities in all of these areas. This publication reflects the general sense of the meeting, though each participant may not agree with every statement. Further, the opinions expressed are those of the authors and not of any current or former employer. By this report's dissemination, we seek to engage a wider group in discussing how to ensure that the medium grows and flourishes.

## **Acknowledgments**


I am pleased to acknowledge and thank our sponsors for their generous contributions to the success of the conference. The



following entities sponsored the 2001 conference: Catenas, Citigroup, the Markle Foundation, McKinsey & Company, Nokia, Nortel Networks, Pitney Bowes, RealNames Corporation, VeriSign, Verizon Communications, and VISA U.S.A. I would like to thank all of the participants—all expert, all enormously busy, all willing partners in our dialogue. I would particularly like to thank our international participants for coming such long distances (proving that distance is not dead yet) and for bringing important insights about this truly global medium that is too often viewed simply from a U.S. perspective. Charlie Firestone, executive director of the Aspen Institute’s Communications and Society Program, has given the Internet Policy Project a home at the Aspen Institute and always provided support and wise counsel; Lisa Dauernheim, Tricia Kelly, and Sunny Sumter-Sana of the Communications and Society Program have helpfully and cheerfully provided for the myriad of details necessary for this publication and for the operation of the Project as a whole. Amanda Mills of Yale Law School assisted us in shaping the agenda and identifying the issues to be addressed. Lastly, I would like to express my deep appreciation for the work of Erez Kalir, the meeting’s rapporteur, whose dedication to searching for the core of meaning in the swirling conversations at Aspen was the foundation for this report.

Elliot E. Maxwell  
Senior Fellow for the Digital Economy, 2001  
and  
Director, Internet Policy Project, 2001  
Communications and Society Program  
The Aspen Institute  
Washington, DC  
February, 2002

**RETHINKING  
BOUNDARIES IN  
CYBERSPACE**





# Rethinking Boundaries in Cyberspace

The Internet's explosion into the public consciousness in the 1990s was marked by a heady rhetoric about its uniqueness. Unlike previous technologies, the Internet would render geography obsolete, allowing anyone, anywhere, to access a limitless fund of digitized information and to share such information with anyone else, free from control or regulation. Territorially based laws were said to have little or no effect in cyberspace—a global, “borderless” place beyond the sovereignty of any existing jurisdiction. The Net would be governed, if at all, through the self-initiated efforts of its constituent communities: the dream of the Declaration of Independence made real, virtually.

As the Internet has matured, however, traditional governments and private actors have increasingly sought to assert control over conduct and content in cyberspace. Governments, responding to the geographic dispersal of Internet users and the Net itself, have directed their regulatory efforts not only at people and entities within their territorial borders but also at those beyond them. And private actors—service providers, applications vendors, and industry consortia (among others)—have played a growing role in drawing new and different kinds of borders on the Net, such as borders around namespaces.<sup>1</sup> To bolster their efforts to assert control, governments and private actors alike have enlisted various new technologies that did not exist in the Internet's early days. Not surprisingly, users have countered with other innovations designed to “route around” the borders that constrain their freedom. The result is an evolving game of technological cat-and-mouse.

How will—and how should—governance in cyberspace evolve now that the utopian vision of the Net as a perfectly self-governing realm has been dispelled? This report takes up that question, not in the hope of offering a blueprint but in the spirit of sketching some useful (if still provisional) answers. The focus is on four key areas:

- 1) **Where we are now.** What are the trends and challenges that comprise today's Internet policy agenda and will help shape tomorrow's? Are there troubling aspects about the direction

in which governance on the Net is evolving? What trends in particular deserve the scarce attention of public policymakers and the public?

- 2) **Guiding principles for good governance.** Algorithms for good governance do not exist. But based on what we have learned about the nature of the Internet since its inception and on relevant historical antecedents in other areas, can we arrive at principles to guide governance decisions for the Net toward successful outcomes and away from dangerous pitfalls?
- 3) **Proper roles for different actors.** Governance on the Internet is not the exclusive province of traditional governments. On the contrary: A proliferating array of other actors—corporations, multinational rule-making, standard-setting, and advisory bodies, nongovernmental organizations (NGOs), and new kinds of organizations that do not fit neatly into any existing categories—play increasingly significant roles in Net governance decisions. What are the proper roles for these actors? For traditional governments? Can complex relationships among diverse decision makers be structured to prevent rivalry and chaos?
- 4) **Specific governance challenges.** Governance challenges for the Internet exist in myriad subject areas. Three areas of importance to the future of cyberspace are extraterritoriality, confidence issues (e.g., promoting privacy, security, and trust on the Net), and namespace management. Drawing on the insights developed in earlier parts of the report, can we begin to map the right direction for public policy in these areas—or at least identify some of the right questions on which public deliberation should center?

To probe these and related topics, the Aspen Institute's Internet Policy Project convened 24 leading entrepreneurs, technologists, academics, executives, and policy advisors for its 2001 conference. The conference, moderated by the Project's director, Elliot Maxwell, took place July 22–25, 2001, in Aspen, Colorado. This report is a synthesis and interpretation of the conference discussions.

## **Prologue: Why a Conference on *Internet Governance*?**

As a few conference participants observed, much conversation about Internet governance proceeds as if the problem were new, and thousands of years of political and legal thought simply irrelevant in light of the Net's uniqueness. This notion is manifestly false: Many of the governance questions that apply to the Internet today arose in similar form during the popularization of other technologies, such as modern shipping, aviation, and telecommunications (to name only a few). The answers that human societies forged to those questions then can help us answer analogous questions today. Yet recognizing that the Internet lies on a historical continuum of transformative technologies led conference participants to ask two interrelated questions that merit attention before delving into others: What characteristics mark the Internet as a novel and genuinely disruptive technology? And what about the Net poses new challenges for governance?

Begin with the first of these questions. While early accounts may have overstated the Internet's uniqueness, conference participants generally agreed that the Net has changed social, economic, and political relationships around the globe in several significant ways. To begin with, by dramatically lowering transaction costs, the Internet has facilitated a vast increase in the volume of economic transactions.<sup>2</sup> Net-based transactions that cross national borders are growing at a particularly impressive rate, in absolute terms and as a percentage of overall Internet traffic. The Internet is hardly the first technological innovation to boost cross-border exchange; many others did so in their day as well (the telegraph, railroad, and telephone, to name just a few). Yet the sheer magnitude of the increase in cross-border transactions attributable to the Net, participants suggested, is unprecedented and consequential.

Second, the Internet has also revolutionized the economy of information. On the production side, it has radically decentralized—and democratized—the power to distribute information to the public. Traditional media conduits such as print, radio, broadcast television, and cable have long been controlled by relatively few large corporations. Ordinary individuals and groups cannot easily gain access to these conduits to broadly disseminate their ideas and opinions. The Internet provides users with a means

to do so; to paraphrase one conference participant, it turns freedom of speech into freedom of the press. This transformation equates, on the consumption side, to a massive increase in the quantity of information available to the public. But the consumption-side change isn't only a matter of quantity: The Net also renders information easily accessible over a far wider geographical scope (as dramatized in Yahoo!'s advertisements depicting a denizen of the arctic shopping on the Net in his igloo). The Net's impact on the economy of information, too, distinguishes it from prior technological innovations.

Third, the Internet disrupts existing relationships between individuals, businesses, and states, spawning new intermediaries between these entities and eliminating old ones. Because the Net significantly increases the liquidity of information, for example, it creates opportunities for new information hubs to connect buyers and sellers on an international scale—hence EBay, Priceline, and business-to-business exchanges. Of course, the emergence of these new intermediaries has threatened the livelihood of others, such as local pawn shops, travel agents, and wholesalers. Nor is this process of dis- and re-intermediation limited to the private sector. In the sphere of policy and politics, the Internet has given rise to new entities mediating relationships between individuals and their governments. Some of these new entities, such as the vote-trading sites that sprung up during the 2000 American presidential election, are grassroots organizations that seek to facilitate broad-based political action. Others, such as the Internet Corporation for Assigned Names and Numbers (ICANN), are decision-making bodies with narrower missions and a narrower membership consisting of technical experts. Yet both of these types of Net-centered entities—the grassroots and the technical—have redistributed political and policymaking power away from traditional actors. They have also made it more difficult to surveil the regulatory landscape and locate all the points of decision-making authority.

These three phenomena—the growth in the volume of cross-border transactions, transformation in the economy of information, and reordering of societal intermediaries—raise a host of new governance challenges. Much of the commercial law that undergirds

international business transactions, for example, has been designed to facilitate exchange among businesses, “repeat players” with the experience and resources to fend for their interests effectively. What adaptations should be made to this law when individuals (e.g., the man in the igloo) become transactors in the global economy? Or consider another challenge that follows from the Net’s empowerment of individuals. Nation-states differ widely in their laws and norms regarding freedom of speech and press. In the past, territorial borders prevented their differences in this sphere from breaking into open conflict save in rare cases. But cyberspace introduces porousness into those borders, enabling individuals to circumvent domestic laws and norms and to seek information in jurisdictions where they’re most likely to find it. Thus, Americans constrained by U.S. obscenity laws can shop for pornography on websites based in Holland, and French citizens governed by France’s regulations on the display of Nazi regalia can view it on websites based in the United States. How should nation-states resolve the inevitable legal and normative disputes that ensue?

Yet the challenges that the Internet poses for governance go beyond practical problems of the kind discussed above. At a deeper level, the Net challenges familiar notions of “government” and “governance” themselves, inviting us to rethink what a government is and what governance entails. For the past two centuries, the dominant governmental actor has been the nation-state. On the Net, however, other decision makers—particularly leading corporations (such as AOL, EBay, and Microsoft) and private multinational forums (such as ICANN, the Internet Engineering Task Force [IETF], and the World Wide Web Consortium [W3C])—are increasingly as important if not more so. These other actors are likely to make a greater number of governance decisions than nation-states, which are hampered by the slowness of legislatures, courts, and agencies. And their governance decisions are likely to have at least as much impact because they are often closer to users and to the Net’s infrastructure than are traditional governments. A shift in governance instruments accompanies this shift in governance actors. The dominant regulatory instrument of traditional governments has been law. But as Mitch Kapor, William Mitchell, and Larry Lessig have taught us, on the Net the dominant



instrument of governance is “code”: the combination of software, hardware, and network design that substantially defines the nature of cyberspace.<sup>3</sup>

As the earlier free speech example tacitly suggests, the Internet also challenges traditional assumptions about sovereignty. Sovereignty in the physical world is, for the most part, clearly delimited. Multiple sovereigns may assert power to regulate conduct in the same territorial space, but their relations to one another are either plain from the outset or resolvable through time-honored legal devices (such as treaties, choice of law rules, and the doctrine of comity). Thus, the U.S. federal government, the state of California, and the city of Berkeley all claim authority to set rules for behavior in Berkeley, California, but all three understand that the U.S. Constitution’s supremacy clause resolves whose laws have primacy.<sup>4</sup> And if a catastrophic industrial accident occurs in India at the local plant of an American firm using defective machinery manufactured in France, longstanding doctrines will enable courts to determine with relative ease the proper forum for the ensuing mass torts litigation.

In cyberspace, in contrast, sovereignty is interpenetrated and ambiguous. Consider the question of sovereignty over the Internet’s core code. The Net is defined by a set of protocols collectively known as Transmission Control Protocol/Internet Protocol (TCP/IP). The design of these protocols—and, in particular, the overarching “end-to-end” principle that funnels control to users at the network’s “edges” and allows all forms of communication to travel across the network without central control—has a profound effect on the range of conduct that can occur in cyberspace.<sup>5</sup> Who has sovereignty to direct the evolution of this set of protocols and to decide whether and how the “end-to-end” principle changes? Private companies that own the physical infrastructure underlying the Net? Private companies offering applications and services that use the infrastructure? Governments that traditionally regulate the conduct of inhabitants within their territorial borders? There are no obvious answers to this question.

The foregoing discussion reflects the view—shared by most conference participants, though not all—that the governance challenges the Internet poses are in some ways new, and defy simple

analogies to the challenges that followed previous technological innovations. But there is an important caveat. Virtually all participants agreed that the Net's impact on human affairs is best understood within a broader context. The growth in the volume of cross-border transactions, increase in the liquidity of information, and advent of new social intermediaries, as well as the rise of competitors to the nation-state and the complication of traditional notions of sovereignty are not attributable to the Internet alone. They should be viewed as part of a larger phenomenon of globalization—which fuels, and is fueled by, the Internet's popularity.

The conference that spawned this report took place before the catastrophic events of September 11, 2001. It goes almost without saying that those events have changed the way Americans and others think and talk about many issues, including Internet governance. In the United States, security is now at the forefront of public consciousness, and other values (such as privacy) have receded. What the long-term effects of September 11 will be—and whether the new emphasis on security becomes a permanent feature of public policy in the United States and elsewhere in the West—remains unclear. Whatever the long-term repercussions of September 11, however, it has already underscored that Internet governance is inextricably tied to broader questions of governance and globalization.

### **Trends and Challenges: Where We Are Now**

What are the trends and challenges that define today's Internet policy agenda and that will help shape tomorrow's? Three key themes emerged from the conference discussions: first, the disappearance of the "borderless" Internet, as states and private actors alike seek to assert control over cyberspace by transforming it into an increasingly regulated space; second, the efforts of users to escape these controls by using new technologies, and the "arms race" that ensues as public and private actors respond; and third, the growing trend to resolve the contest for control on the Net by resort to private governance—governance by private entities which, unlike many traditional governments, afford the public little or no representation in decisions that affect it.

*The Disappearance of the Borderless Internet and the Quest for Control*

The quest of public and private actors to assert control over conduct in cyberspace results from, and accelerates, the erosion of the boundary between cyberspace and the physical world. As the Net mediates a growing proportion of human interactions, states find that they must regulate it in order to maintain the force of their laws within their physical borders. Thus, the attorney general of Minnesota sued gambling sites outside his state not because he wished to suppress the activity throughout cyberspace but because he sought to enforce his state's own law that forbids Minnesotans from gambling.<sup>6</sup> The Council of Europe backed the "cybercrime" treaty for similar reasons. The treaty, which has yet to take effect in the United States, would require Internet service providers (ISPs) to maintain logs of users' activities for up to seven years and to keep their networks tapable by law enforcement agencies.<sup>7</sup> These measures spring not from any desire by European governments to assert Orwellian control over the Internet but from their accurate recognition that effective crime control "on the street" now requires interdicting criminal activity online. As the foregoing examples indicate, erosion of the boundary between cyberspace and the physical world renders cyberspace itself a more regulated, bordered place—a place that more closely resembles the world outside.

A similar dynamic is at work with private actors such as ISPs, software vendors, and content distributors. The blurring of boundaries between the "virtual" and the "real" world manifests itself in the private sector as a blurring of the boundary between e-commerce and "physical" commerce: A growing proportion of all commerce is transacted at least in part online. In their efforts to capture and cordon off a share of this commerce, private actors are building new kinds of borders in cyberspace that often reinforce states' attempts to superimpose territorial borders there. Thus, AOL, the owner of a massive "names and presences" database associated with its AIM instant messenger service, has bordered this namespace in the name of "security" and thereby prevented other instant messenger services from interoperating with AIM. Microsoft has unveiled an initiative to issue all Netizens with digital certificates or "passports" that would contain authenticated identifying information about them—encoded in software controlled by Microsoft and its partners,

and not presently interoperable with other identification systems. Numerous firms are at work developing rights-management systems that would enable fine-grained monitoring and control of what users do with intellectual property on the Net: software that reports not just whether you downloaded the MP3 file but how many times you've played it, how many times you've copied it, where you've stored it, and who you've shared it with. Still other firms are marketing "mapping" software that can pinpoint an Internet user's geographical location with a high degree of certainty. This software allows advertisers to target consumers with greater refinement, yet it's likely to find another customer base as well: sovereign states looking for efficient ways to map their laws onto the Net.

### *The Unfolding Arms Race: Technologies of Freedom and Technologies of Control*

Not surprisingly, many users have responded to the zoning efforts of public and private actors by turning to technologies that restore (and in some cases enhance) elements of their freedom. Perhaps the most common example: anonymizing technologies aimed at empowering users to communicate in and move about cyberspace free from surveillance by governments or corporations. These technologies range from "first generation" websites that serve as protective "shells" for surfers seeking privacy to more sophisticated software enabling users to join a network of computers that serve as shells for one another. Needless to say, such technologies are locked in a fierce battle with the new mapping technologies. But the battle isn't purely technological. While it plays out through a rivalry of technologies, it reflects two broad groups of antagonists. On one side are states and corporations that correctly understand that user anonymity deprives them of control. On the other are users and code-writers (many academic, but some entrepreneurial) who resist the control that states and corporations would wield. Each side in this battle has resources beyond technology at its disposal. States and corporations can leverage the power of laws and markets; users and code-writers can leverage their quickness and relative anonymity. Which side will ultimately prevail? Conference participants did not address that question at length, but they agreed that the answer will have a vast impact on the future of the Net.

Anonymizing and mapping software comprise only one facet of the technological arms race. Peer-to-peer computing (P2P) represents another, one which may prove at least as important in determining the balance of power between users and entities that would govern them. P2P, made famous by Napster, refers to a class of applications that seek to take advantage of the immense computing resources latent in devices at the “edge” of the Internet—such as PCs, personal data assistants (PDAs), and web phones—by connecting them directly to one another. To access these decentralized resources in a manner that maintains their autonomy from centralized servers, P2P applications bypass the Internet’s domain name system and rely instead on alternative addressing architectures. P2P applications thereby liberate users in two interrelated ways. First, they enable users to transform their devices into “peers” that can interact with one another and form impromptu networks while relying minimally (if at all) on centralized intermediaries. Second, they empower users to unbundle, share, and aggregate any resource contained in their individual devices: storage capacity, processing power, communications capability, content, or whatever else. This leveraging effect is what transformed the modest, isolated music collections of individuals into the mega music library of Napster.

Both of P2P’s liberating effects—the ability to connect “edge” devices directly to one another and the ability to share the resources in these devices—make it much easier for users to form autonomous communities in cyberspace. Indeed, numerous P2P-based communities already exist: Witness the immense followings garnered by Napster and its progeny or by instant messaging systems such as AIM and ICQ. Of course, the very characteristics that give P2P its breathtaking community-building potential also render the communities it spawns very difficult to police because of an absence of centralized control. P2P thus creates serious challenges for governments and service providers. Exhibit A: Napster. As everyone knows, Napster was ultimately ordered to shut down because public and private authorities could not devise a less draconian remedy to prevent the copyright infringement that it facilitated. Yet the legal injunction against the company has been far from foolproof: Other P2P applications such as Gnutella and Morpheus have sprung up as substitutes (albeit with smaller user bases so far). In a future in

which P2P communities are rife, it seems unlikely that litigation alone will succeed in regulating them. A more plausible scenario envisions traditional governments enlisting private-service providers to help restore a measure of centralized control through tools such as terms-of-service agreements and monitoring technologies. The effectiveness of that approach remains an open question.<sup>8</sup>

The Napster case raises an important, broader point that several conference participants took pains to emphasize: namely, the normative ambiguity of the emerging arms race between technologies of freedom and technologies of control. This battle, participants agreed, does not pit “good” versus “evil.” P2P applications, for instance, lend themselves just as easily to positive ends (e.g., communities engaged in grassroots sharing of ideas and inventions) as they do to destructive ones (e.g., networks of lawbreakers aggregating computing resources to destabilize society). The point applies to mapping and anonymizing technologies as well. In the hands of authoritarian governments, mapping technologies can facilitate repression, while anonymizing technologies can allow users to escape it. Conversely, in the hands of wrongdoers, anonymizing technologies can facilitate fraud, defamation, piracy of intellectual property, and cyberterrorism, while mapping technologies can allow governments to police such violations. Whether these technologies promote the public good depends entirely on who is using them and how. This reality suggests that society may do well to strive for balance between the powers of users and those of governance actors—a theme we revisit below.

### *The Rise of Private Governance Arrangements*

If the contest for control between decentralized users and centralized authorities is a defining part of the present moment in the Internet’s history, so too is the rise of private governance arrangements that increasingly mediate that contest. “Private governance” refers to governance by private actors that affects the public but affords it little or no representation in decision making. Such governance exerts influence over the Net in several different forms. Private, multinational entities such as ICANN, IETF, and W3C, which are not directly accountable to the public, leverage

technical expertise to play growing rulemaking, standard-setting, and advisory roles in shaping the changing architecture of cyberspace. Private corporations such as AOL and Microsoft, whose first mission is to maximize shareholder value, control borders on the Net (such as borders around namespaces) that concern not only their own customers but also millions of other users. And governments themselves increasingly seek to “deputize” private actors such as ISPs and portals in order to regain traditional powers that have ebbed in cyberspace—as illustrated by developments such as the European cybercrime treaty and the French judiciary’s ongoing conflict with Yahoo! This “deputizing” trend—which enables governments to regulate with far less transparency than many ordinarily do—is likely to become more important in the future as P2P applications blossom.

The rise of private governance arrangements on the Net intersects in important ways with the rise of code (software, hardware, and network design) as the dominant instrument of regulation in cyberspace: The trends are mutually reinforcing. Greater reliance on code as a regulatory instrument further “privatizes” decision making for several reasons. First, code is less transparent than law and therefore less susceptible to democratic scrutiny. The popular press and the public can readily grasp the import of most laws enacted in Washington and Brussels; the same cannot be said about their abilities to decipher the political decisions invisibly embedded in products that emanate from Silicon Valley or Redmond.

Second, as Larry Lessig has demonstrated in his pathbreaking work, code is less amenable than law to resistance by individuals and to the oversight by democratic institutions that resistance facilitates. If you believe that a contract to which you’re a party interferes with your rights under the copyright law, you can breach it and thereby place the burden on the other party to sue you; what’s more, a court—a neutral and independent decision maker—will decide who’s right. But if you believe that the coded copyright protection scheme on your newly purchased software infringes your rights, resistance is far more difficult. If you can’t hack through the protection scheme (and most of us can’t), your options are to deal with the company (not exactly an unbiased adjudicator) or to sue in court yourself (an expensive and time-consuming burden that few people are likely to undertake).<sup>9</sup>

Third, the rise of code tends to privatize decision making because code-based solutions to governance problems originate disproportionately from private actors—and thus often reflect the preferred approach of those actors to the choices at hand. This last point is in a sense the “flip side” of the earlier point regarding transparency: It’s not just that the public can’t easily understand code, but also that it can’t easily write it, and isn’t abundantly represented by people who can. Laws enacted in legislatures typically reflect the input of numerous “public interest” groups that advocate on the public’s behalf; coded solutions to governance problems do so to a far lesser extent.

#### *From Where We Are to Where We Are Going*

The aim of the foregoing discussion has been to set the stage. We began by pausing to consider why it makes sense to think about Internet governance at all, then briefly canvassed some of the key trends that mark the present moment in the Net’s development. The survey of those trends has been necessarily selective: much more would need to be said to offer a complete picture of “where we are” (and providing such a complete picture was not one of the conference’s objectives). But the themes in the foregoing discussion frame the discussion to come. Amid the vanishing of the “borderless” Internet, the unfolding contest for control between states, private actors, and users, and the rise of “private governance” arrangements, can we arrive at guiding principles to help steer toward effective governance solutions for the Net? What are the proper roles for traditional and alternative governments—for states, private decision-making forums, corporations, NGOs, and users? And can the answers to these questions help address specific Internet governance challenges in areas such as extraterritoriality, user confidence, and namespace management?

### **Guiding Principles**

As conference participants emphasized time and again, reliable formulas for good governance do not exist in the Internet context any more than they do in the context of society writ large. Effective solutions to governance challenges on the Net are likely to emerge from the concrete particulars of problems, not from abstract prescriptions. Yet this reality does not mean that the search for



principles to guide decision making is wasted. On the contrary: Such principles—beacons in a sea of choices—can help decision makers chart a course away from known dangers and along routes more likely to lead to safe land. In their absence, navigation is more difficult and more perilous. The conference discussions pointed to several of these beacons.

### *Decision Making Based on Openly Debated and Clearly Articulated Values*

Participants generally agreed that regardless which institutions take the lead in any particular governance decision for the Internet, both the process of decision and the substantive outcome should be based on values that communities affected by the decision have openly debated and chosen. Ideally, everyone affected by a decision would reach consensus on these values, but in practice consensus may often be unachievable. In such cases, openly debating the values that will guide decision making and articulating the values chosen is a second-best objective.

Participants suggested numerous values that may merit consideration in any given governance decision. With respect to the process of decision making: Are the decision makers accountable? Is the process transparent? Does it provide adequate representation to those affected? Does it otherwise take account of their interests? Does it provide for a diversity of participants? Is it quick enough to respond to technological and market developments? Has it considered competing solutions and any empirical evidence as to their success or failure? With respect to the substantive result: Is it enforceable? Scaleable? Cost-effective? Has it factored in the existence of economic, technological, and regulatory uncertainty? What are its effects on innovation? On connectivity? On the public's access to information? On other values, such as the "end-to-end" principle? What, if any, are its distributive consequences? Its equity implications and impact on the "digital divide"? These questions are only a beginning, but they capture some of what should be included in public deliberation on appropriate values to guide governance decisions for the Net.

States and the communities that comprise them differ, of course, with regard to the values they hold dear. Participants suggested that

it will frequently be impossible for diverse communities linked together by the Net to harmonize their disparate values. No one should expect the emergence of a constitution for the Internet—at least not one that offers the far-reaching rights and privileges of many national constitutions. Still, a majority of states may be able to agree on a limited number of substantive norms—for instance, protecting the integrity of the Internet itself against terrorism, or prohibiting the distribution of child pornography in cyberspace. When agreements are unobtainable states may cooperate to make their rules for the Net “interoperable,” thereby minimizing outright conflicts.

The inevitability of normative disagreement between communities raises a difficult issue. Most political decision-making bodies in today’s world are local or national. Yet the Internet is a global medium, and some governance decisions regarding the Net (although it may be unclear which) are global in nature. How should the Net’s stakeholders deal with this asymmetry? Three relevant points emerged from the conference discussions. First, participants disagreed with one another about whether and to what extent Internet governance actors committed to “democratic” values have the prerogative, or the duty, to advance those values in jurisdictions that reject them. If an authoritarian state makes a practice of using the Internet to spy on the activities of political dissidents, for instance, how should a democratically oriented ISP that has entered the market in that state respond: by taking affirmative steps to foil the practice, by tolerating but refusing to abet it, or by complying with the state’s demands for cooperation? Participants offered widely divergent answers to this type of question.

They reached consensus, however, on a second point: illiberal regimes demanding that the rest of the world incorporate their values into the governance of the Net as the *sine qua non* of their connectivity should be flatly refused, even if this means sacrificing the Net’s global reach. One conference participant posed a prescient hypothetical scenario in teeing this point up for discussion: Suppose the Taliban suggested that they would permit widespread connections to the Internet within their jurisdiction as long as all photographs of women on the World Wide Web featured them clothed in *hijab*. The scenario is obviously an extreme one but all

participants agreed on how the Internet's existing stakeholders should respond to such an offer.

Participants also expressed agreement on a third point: that certain "democratic" values are embedded in the current architecture of the Net itself. The end-to-end principle provides perhaps the best (and most widely cited) example. Though originally adopted to promote the network's efficiency, not to protect the Internet's users from centralized control, the end-to-end principle has contributed in a profound way to the latter value. The "dumb" network we have today cannot filter the data packets it transports on the basis of their content; indeed, it does not "know" (and therefore cannot reveal) what those contents are. Of course, the end-to-end principle is not inherent to the Internet. On the contrary, an intense debate rages regarding whether and to what extent it should be retained as the Net's infrastructure evolves.<sup>10</sup> But as the various actors struggle to resolve normative differences between them in making global governance decisions for cyberspace, the values embedded in its existing infrastructure provide important "defaults." Participants generally agreed that the burden should lie with those who would modify these defaults and not with those who would retain them.

#### *Drawing on Relevant Historical and Legal Antecedents to Help Guide Decisions*

Just as values embedded in the infrastructure of the Internet are relevant to decisions regarding the Net's future, so too are values embedded in the historical and legal traditions of societies. Too often in conversations about cyberspace, several conference participants suggested, these values are forgotten or ignored. Thinking of governance decisions for the Internet as a *tabula rasa* is dangerous for at least two reasons. It cheats decision makers of accumulated wisdom that can help craft effective solutions, and it distances decision making from social values that often have already garnered legitimacy and public support, increasing the risk that governance choices will fail to reflect those values adequately.

Marc Rotenberg's recent scholarship powerfully demonstrates how a close analysis of historical and legal antecedents can cast light on societal values and norms that should bear on governance

decisions for the Internet.<sup>11</sup> Focusing on the area of privacy, Rotenberg mines the rich legal tradition of privacy protection in the United States: Justice Brandeis' classic dissent in *Olmstead v. United States*, the Supreme Court's adoption of Brandeis' view—and its recognition that the Fourth Amendment applies to telephone wiretaps—in the *Katz* case, Congress's adoption of the landmark Privacy Act of 1974, the evolution of Fair Information Practices, and the ensuing incorporation of these practices into a host of statutes, administrative rulings, and technical standards.<sup>12</sup> This tradition, Rotenberg posits, embodies a cohesive set of choices about how privacy should be protected in the United States, yet it has been almost entirely ignored by “cyber-pundits” in discussions regarding privacy protection in cyberspace. One need not agree with Rotenberg's position on the extent to which these historical choices merit assimilation into the Net to accept his contention that it is a mistake to omit them from conversation about Internet privacy. And the deeper point of his argument applies beyond the realm of privacy to the full array of governance decisions facing the Internet.

*“Globality”: Truly Global Participation Where Decisions Are Truly Global in Impact*

Institutionally speaking, the Internet is an invention of the American government—a fact by now well known. Over time, the government has moved to privatize the Internet's administration. Yet several conference participants, particularly those based outside the United States, reported a widespread perception around the world that U.S. institutions and personnel still dominate key governance decisions for the Net. This perception, many participants agreed, is often accurate. A representative example: ICANN. Although ICANN has taken important steps to internationalize the composition of its executive board, numerous participants (based inside and outside the United States) noted that the organization retains an American “tilt.” Its headquarters are located in Los Angeles, for example, making the organization more naturally attuned to American input, and its staff consists disproportionately of U.S. nationals. Conference participants agreed that this situation needs to change: Where governance decisions for the Net are truly global in impact—for example, in decisions regarding the administration of the

domain name system or the transition to the next generation of the Internet Protocol (IPv6)—they should be made with truly global participation. Participants called this the “globality” principle. Respecting globality becomes increasingly important as we move toward a world in which China and India overtake the United States as states with the greatest number of Internet users.

Yet the globality principle has limits. As the Taliban example suggests, global participation does not trump all other values that impinge on Internet governance. Where such participation trades off against other values, participants agreed, it may need to give way. Furthermore, not all Internet governance decisions are global in nature. Commentators have often remarked that “cyberspace” consists of myriad “cyberspaces,” in which innumerable governance decisions are made through diverse forms of government (ranging from government by AOL to government by the agora). For most of the Net’s users, this federalism and the opportunities for local decision making it allows are an integral part of what makes the medium worthwhile. Accordingly, globality should not be mistaken as an endorsement of a “global government” for the Internet. The need for global participation in Internet governance decisions that have a global impact by no means suggests that all or even most governance decisions implicating the Net are global ones calling out for centralized authority.

#### *Turning Institutional and Procedural Heterogeneity into an Advantage*

The diversity of Internet governance actors alluded to above can be bewildering. The orderly structure of government that many of us were taught in civics class does not exist for the Internet (though whether its absence is cause for celebration or concern is debatable). Instead, Internet governance unfolds in a mosaic of interactions among multinational, national, and local entities operating in the public, private, and “third” sectors that wield influence through laws, norms, architectures, and markets (among other instruments). It is tempting to try to resolve which of these entities and instruments would be “best” suited to address governance challenges in specific areas—for instance, whether criminal law enforcement on the Net should be delegated principally to multinational, national, or local entities, how closely private actors (such as ISPs) should be involved,

and to what extent the problem should be addressed through modifications to the Internet's architecture, instead of (or in addition to) through law. Conference participants expressed widely divergent views on these types of questions. A few participants, for instance, sought to produce a matrix "matching" specific subject areas with certain actors. Others maintained that such a matrix could not do justice to the diversity of actors and modalities of influence that impinge on any given subject area in the Internet governance arena. Participants likewise disagreed on related questions: for instance, whether new governance institutions are needed for the Net to supplement those that already exist, which governance challenges are better addressed transnationally and which by individual nation-states, the proper balance of public and private action in particular governance areas, and how much faith to place in the "self-governance" arrangements of users. These disagreements made clear that the entities and instruments best suited to address the Net's governance challenges are likely to vary from case to case and to emerge only after competing solutions have been tried.

Yet it would be a mistake to regard the heterogeneity of Internet governance actors and instruments merely as a source of confusion and disagreement. It is also a source of opportunity. In the U.S. Constitution, the separation of powers among different branches of government (legislative, executive, and judicial) and the splitting of sovereignty among different levels of government (federal, state, and local) yield a system of checks and balances and democratic experimentation.<sup>13</sup> The checks and balances help prevent any individual governance actor from accreting an excess of power that would lend itself to abuse. Democratic experimentation, in turn, generates competing solutions to governance problems that enable decision makers to zero in on the most effective solution based on an empirical record of success and failure. The heterogeneity of entities and instruments interacting to make governance decisions for the Internet holds out the promise of similar advantages—if they can be orchestrated to complement (and check) one another to avoid Babelian cacophony.

To that end, conference participants observed that there is often room for multiple actors to participate helpfully even in a single area of governance, and that the intervention of a particular actor need

not occupy the field. Several distinctions illuminate the variegated nature of the space for intervention. One interrelated set of distinctions are those between coordination and control and between prevention and enforcement. These distinctions pertain principally to states and the agents to which they delegate or cede authority over Internet governance. At one extreme, states can intervene in an Internet governance decision solely in a coordinating capacity—for instance, to encourage industry standard-setting. Here states have no significant prevention or enforcement role, and space for other actors to participate in governance is wide. At another extreme—for example, in policing cyberterrorism—states can intervene to control conduct, and can deploy their full powers both to prevent certain conduct from happening and to punish it after the fact by enforcing the law. Here space for other actors to participate in governance is narrower, but it still exists. Indeed, states may seek to conscript private entities (such as ISPs) to assist them in monitoring and enforcement. Other private parties may participate voluntarily through alternative instruments of governance; users in chat rooms, for instance, might engage in a cyberspace version of “neighborhood policing” to report suspicious remarks or postings to authorities. Between the extremes of coordination and control lies a spectrum of varying degrees of sovereign intervention, corresponding to varying space for other actors to participate in governance.

Another distinction that highlights the opportunity (and need) for coordinated governance by multiple actors is that between “horizontal” and “vertical” decisions. “Horizontal” decisions produce rules that are specific to a discrete policy area (e.g., taxation). “Vertical” decisions, in contrast, seek to create cohesiveness between rules in different policy areas (e.g., taxation and criminal law enforcement). In practice, the distinction between horizontal and vertical decisions is less a dichotomy than a continuum: Rules that govern a particular area can have greater or lesser interconnectedness with rules in adjacent areas. Building an appropriate degree of interconnectedness between rules in different areas, participants suggested, should be an important part of the Internet governance agenda. Meeting this goal will necessarily involve multiple actors—not just the bodies responsible for rulemaking but also third parties (such as regulated entities and

watchdog organizations) with knowledge of how rules in different areas interact with one another at the implementation level.

To be sure, in rare cases space for multiple actors to participate robustly in Internet governance may not exist. In these cases—the “natural monopolies” of Internet governance—intervention by too many would-be decision makers would risk fragmentation of the Net or chaos. (Consider, for instance, the likely outcome if rivalrous actors undertook competing efforts to manage certain parts of the Internet’s core infrastructure.) Here, participants generally agreed, the task is to settle on a single, legitimate decision maker, entrusted with “final” authority, that can efficiently administer the resource at issue. Of course, this decision maker will succeed only with the cooperation of other actors—including, at minimum, their forbearance from intervention.

### **Roles of Different Actors (I): Traditional Governments**

The foregoing discussion suggests that the heterogeneity of entities and instruments for Internet governance may be a blessing—if these entities recognize the opportunities for, and imperative of, coordinated action. Spheres of Internet governance are rarely akin to natural monopolies; more often, these spheres resemble ecosystems in which diverse actors occupy discrete niches and thereby contribute to the well-being of the whole. The ecosystem analogy, however, raises an obvious yet difficult question: What are the appropriate niches of different actors? To expand the question: What are the distinctive strengths and weaknesses of potential participants in Internet governance arrangements? And in light of those strengths and weaknesses, as well as the trends that characterize today’s Internet policy agenda, what roles should those participants be expected to play? The discussion to come takes up these questions for an array of different actors, beginning with traditional governments.

#### *A Brief History: Traditional Governments and the Internet from Then to Now*

During the early years of the Internet’s explosive growth phase, conventional wisdom held that traditional governments should “stay out” of regulating cyberspace. Policymakers, cyberpundits, and



academics alike recited this conventional wisdom as gospel. Thus, the Clinton administration's influential white paper, *A Framework for Global Electronic Commerce*, argued that government should regulate the Internet only when "necessary" and should generally avoid intervening in its development.<sup>14</sup> Activist John Perry Barlow's much-cited *Declaration of the Independence of Cyberspace* told governments they had "no sovereignty where we gather" and asked them to "leave us alone."<sup>15</sup> And in the *Stanford Law Review*, attorneys David Johnson and David Post published a seminal article contending that cyberspace should be governed not by the laws of any traditional sovereign but by the rulemaking efforts of its constituent communities.<sup>16</sup>

As the Internet has matured and its integration with economic, political, and social life in the "physical" world has increased, governments have abandoned the old conventional wisdom and started to assert some of their traditional regulatory authority in cyberspace. Their efforts have been motivated at least in part by a "Red Queen effect"—a recognition that they must expand the reach of their laws into the Internet if they hope to preserve the force of those laws within their physical territories. As governments are discovering, however, enforcing traditional laws is far less straightforward in cyberspace than in the physical world. Private governance arrangements increasingly compete with and displace those laws altogether. P2P and anonymizing applications enable individuals to transact on the Internet largely free from centralized control. And the fact that the Internet allows individuals to be in two places at once—at their desks as well as online—presents states with an extraterritoriality conundrum. To enforce domestic laws against citizens surfing the Web at their desks, states must seek to apply those laws to websites based entirely abroad, creating conflict with foreign sovereigns. We revisit this problem in greater detail below.

### *Why States Aren't Going Away*

Notwithstanding these difficulties, states are unlikely to take leave from Internet governance matters. On the contrary: Conference participants agreed that states are likely to remain dominant actors on the scene, for several reasons. First, as one participant—a leading policy advisor—pointed out, traditional governments tend to

believe they have the power, legitimacy, tools, and obligation to address Internet governance. The difficulties they have met in applying their customary regulatory authority in cyberspace has not dissuaded them from this conviction. Second (and relatedly), states are unlikely to allow their sovereignty in the “physical” world to be lost to actors in the virtual world without their consent. So long as cyberspace appeared to be a “separate” realm where “Netizens” gathered to experiment in self-governance, states could afford to stand back and permit the grand experiment to unfold. But as the interpenetration of cyberspace and physical space has increased, and states have come to realize that this interpenetration puts their sovereignty over the physical world at risk, they have lost their inclination to forbear from intervening. Third, even where states forbear from *direct* intervention, they are likely to remain a looming presence; their powers may be invoked to help prevent the breakdown of private mechanisms and to referee disputes that arise when such breakdowns occur. Conference participants agreed that state powers will predictably be called upon, for instance, to monitor self-governance schemes, prevent fraud, police the exercise of market power, enforce private agreements, and remedy the perceived failure of alternate decision makers—among other purposes.

### *States’ Handicaps and the Need for Self-Restraint*

The fact that states are likely to play leading roles in Internet governance does not mean that they are ideally suited to do so. Indeed, conference participants cited several factors that handicap traditional governments in this sphere. Internet governance decisions are typically technical in nature, but states often lack technical expertise. The pace of change in technology and global electronic marketplaces is highly rapid, but government decision making is notoriously slow. And the most powerful instrument through which to mediate governance solutions in cyberspace frequently is code, but states traditionally express their governance decisions through law.<sup>17</sup>

These mismatches (among other reasons) motivated many conference participants to posit that states should be encouraged to exercise self-restraint in Internet governance arrangements. Participants cited numerous factors that might influence states to

forbear from intervening. These factors include conclusions by states that their vital interests, and those of their constituents, are not at stake, that other organizations occupy the field and have gained a measure of legitimacy, that nonstate solutions (e.g., self-governance by users) offer the most cost-effective and legitimate means of promoting the public interest, and that the nature or scale of the activity does not yet justify deploying the state's powers. Obviously, each of these "forbearance factors" raises questions of its own. Gauging the legitimacy of nonstate actors and solutions, for example, is far from straightforward. Yet the difficulty of describing precisely where forbearance by states is appropriate should not obscure the general point that states should regard self-restraint in matters of Internet governance as a virtue.

#### *States' Strengths and the Need for Their Continued Involvement*

Not, however, the only virtue. For conference participants also suggested that states have a responsibility to help promote the emergence of positive civic orders on the Internet, and that the emergence of such orders hinges on states' assuming active roles in several areas. Many participants, for instance, agreed that states are well-suited to capture and consolidate the collectively shared values that should guide Internet governance decisions. AOL, W3C, and nonprofit organizations such as TRUSTe do not afford individuals the rights of democratic participation and representation through which collectively shared values are often expressed and crystalized. Many traditional governments do. Recognizing that traditional governments constitute repositories for these values does not commit one to any particular position on how they should intervene to advance them in Internet governance decisions, or even whether they should intervene at all. But, at minimum, such a recognition suggests that traditional governments are well-suited to serve the referee and safety-net functions earlier mentioned when private governance mechanisms in cyberspace break down.

Several conference participants—though far from all—also maintained that states have a broader duty in Internet governance: to mediate relationships between individuals and private actors in cyberspace in a way that protects individuals' rights and the values that society deems inalienable. As Larry Lessig and others have

compellingly argued, one way that traditional governments can fulfill this duty is to deploy public policy in support of Internet architectures that comport with collectively shared values. What those architectures might be is hotly contested; frequently mentioned examples include an “end-to-end” network, open-source software for Internet applications, and “open access” to broadband conduits.<sup>18</sup> One may question the desirability of each of these architectures and still support the active involvement of traditional government in architectural design decisions for the Net.

Another, related role that traditional governments can play in fulfilling the more expansive duty that several participants posited is to vet “self-governance” arrangements in cyberspace for their accord with collectively shared values. Although such arrangements come in different shapes and sizes, some emerge not from grassroots organizations but from industry consortia. These consortia, in turn, often design self-governance arrangements with industry’s interests, not the public’s, in mind. Because relationships between corporations and individuals on the Internet are characterized by asymmetric power, users are frequently unable to bargain fairly regarding the “terms” of these arrangements, nor to reject them in favor of others once they are in place. Here is where traditional governments can usefully intercede: By vetting these arrangements before they take effect, governments can seek to incorporate protections for social values and utilize their weight to block arrangements that fail to protect those values adequately.

The European Union’s (EU) scrutiny of the Platform for Privacy Preferences (P3P) offers a recent example of traditional government playing this type of role. P3P, sponsored by W3C, is a privacy management architecture that would take input from users regarding their privacy preferences and then determine if any given website met those preferences. Seeking to assess the impact of P3P on legal rights in force under its privacy directive, the EU assigned a working group to examine the proposed scheme. This working group, in turn, concluded that P3P would “not in itself be sufficient to protect privacy on the Web” and would succeed in doing so only if “applied within the context of a framework of enforceable data protection rules, which provide a minimum and non-negotiable level of privacy protection for all individuals.”<sup>19</sup> The working group

report prompted the EU to withhold its support from P3P—despite the fact that it had been endorsed in the United States by leading government officials and by privacy NGOs. This is not to say that the EU's decision is correct, but that governments may help to ensure that private arrangements reflect societal values.

### *A Sense of Balance*

Not surprisingly, in light of their diversity, conference participants expressed broadly divergent views on the proper role of traditional governments in governing the Net. Some argued that governments should err on the side of self-restraint, others that they should err on the side of active involvement. What emerges, perhaps, is that governments should strive for a sense of balance. As permanent participants in this ecosystem, governments should take care neither to dominate it themselves nor to permit it to be dominated by other actors.

## **Roles of Different Actors (II): Alternative Governance Organizations**

As traditional governments strive for balanced engagement with Internet governance matters, they will need to pay special attention to a cluster of alternative governance organizations (AGOs) that play an important role in the Net's ongoing evolution. These alternative decision makers—such as ICANN, IETF, and W3C—are diverse in their own right but share several common characteristics. Although their authority is typically limited to advice-giving, standard-setting, and (occasionally) private-sector rulemaking, in practice their decisions are often incorporated into the Net's architecture with little input from traditional governments. This influence over the Net's architecture stems in part from the “technical” matters on which these organizations focus: for instance, administering the Net's domain name system (ICANN), shaping the next-generation Internet Protocol (IETF), or designing a system for filtering content on the World Wide Web (W3C). Yet while the decisions made by AGOs are typically “technical” (i.e., readily understood only by those with specialized knowledge), they are also political—directly affecting the distribution of resources and creating “winners” and “losers.” Unlike many traditional entities that make political

decisions, however, AGOs are often neither representative of, nor accountable to, the public. Though ostensibly “open” to participation by all comers, they are characteristically populated and run by private-sector representatives with relevant expertise. Similarly, though ostensibly “global” in membership, they typically include few or no representatives from the developing world in their leadership ranks, despite making decisions that are often genuinely global in impact. And though ostensibly “transparent” in their decision processes, AGOs remain virtually invisible to the public because their work receives so little attention from the popular media.

The emergence of this new class of governance organizations is not unique to the Internet. As journalist Richard Longworth noted in *The American Prospect*, their growth is part of the globalization phenomenon, in which “the global economy has escaped national boundaries, but democracy and its practitioners have not.”<sup>20</sup> Thus, ICANN, IETF, and W3C have much in common with entities that traffic in very different subject matters, such as the International Accounting Standards Board, the International Organization for Standardization, and (to a lesser extent) the Bank for International Settlements. Yet if the rise of AGOs is not unique to the Internet, certain of the Net’s characteristics—the technical nature of decisions about its future course, its transnational reach, and the fact that traditional governments long encouraged other actors to lead its development—have given AGOs particularly powerful roles in Internet governance.

### *The Legitimacy Gap*

Power, but not legitimacy. Many conference participants observed that while alternative governance organizations have contributed much to the Internet’s development, their lack of accountability to the public has rendered their decisions less than fully legitimate.<sup>21</sup> Participants focused on ICANN as a representative case study.

ICANN was formed to internationalize and privatize the administration of the Internet’s domain name system (DNS) and other related tasks.<sup>22</sup> Before ICANN existed, administration of the DNS resided with the U.S. government—which, in practice, delegated it to a small group of expert technologists and private

firms. ICANN, then, was conceived as a “good governance” measure: Administering the DNS through a single private body with international composition would (the theory held) improve the results *and* make them more legitimate. But ironically, as several conference participants pointed out, ICANN faced a legitimacy gap from its inception: The selection of its initial board members was shrouded in secrecy and yielded a board composed predominantly of U.S. nationals.

ICANN has since taken steps to meliorate these problems. Five of its 19 board members are now elected by a vote of Internet users worldwide, and a majority hail from outside the United States. Yet many conference participants agreed that such measures, though doubtless improvements, have failed to address deeper issues that continue to undermine the legitimacy of ICANN’s decision making. Those issues—which, several participants noted, are just as relevant to IETF and W3C as to ICANN—concern a host of ambiguities surrounding the organization’s role and responsibilities. What are ICANN’s goals? Are they purely substantive—for instance, to administer the DNS in a manner that preserves a “single root” for Internet addressing? Or are they also procedural—for instance, to represent the interests of all communities affected by the organization’s decisions? Assuming that ICANN does have some procedural duty to the public, is this duty to represent the public’s *interest*, to be representative *of* the public, or to allow the public to *participate* in ICANN’s deliberations? If to represent the public’s interest, how should one define that interest—by resort to traditional legal definitions or to others? And what kinds of constituencies (geographic, demographic, psychographic) should be the focus as ICANN directors assess which interests make up the “public interest?” Different answers to these questions point to very different choices for institutional design, but conference participants agreed that these questions have not yet been adequately answered. Until they are, ICANN (and similar entities) will continue to suffer from a “legitimacy gap.”

That legitimacy gap, in turn, may undermine the standing of alternative governance organizations in the eyes of traditional governments and ultimately threaten their ability to contribute the valuable expertise that even critics concede they possess.

### *Addressing the Legitimacy Gap*

Participants voiced diverse views on ICANN's mission and goals. Some suggested that the organization should seek to serve the public interest but not necessarily to represent the public. Others posited that ICANN's deliberations should allow for public participation, absent which the organization's decisions would fall short of robust legitimacy. Still others advanced arguments that neither the "public interest" nor "public participation" are proper touchstones for ICANN and that the organization should instead focus on narrow substantive goals such as ensuring the continued existence of a single, unified DNS. By focusing on narrow substantive goals instead of broad procedural ones, these participants maintained, ICANN would minimize the risk of a continual expansion in its mission that could lead (as some critics have already charged) to a "United Nations for the Internet."

Although conference participants did not resolve these disagreements, they did arrive at a rough consensus on several strategies to address the legitimacy gap facing ICANN and other AGOs in the Internet sphere. First, whatever their procedural goals, alternative governance organizations should be bound by well-defined substantive agendas centered on finding solutions to a discrete set of problems. As a corollary, they should be reluctant to assume new responsibilities once their initial mandates have been articulated. Adhering to these principles should largely prevent "mission creep"—which, most participants agreed, does pose a danger of stretching an institution such as ICANN beyond its own capabilities and competence. (As one participant who has had a longstanding involvement with ICANN put it, "ICANN" should not become a synecdoche for "Internet governance.")

Second, alternative governance organizations should diversify their leadership circles and their implementation staffs. In part, this diversification needs to be geographical: AGOs should include representatives from all corners of the globe (and the developing world in particular) if they seek to respect the globality principle. But geographical diversity alone is not enough; AGOs should also work to diversify the perspectives of their membership so that their decision making reflects the input not only of private industry but also of consumer advocates, local user communities, and other



stakeholders in Internet governance arrangements. To paraphrase one conference participant, taking globality seriously means thinking about the implications of governance decisions for humanity writ large, not just including token representatives from states around the globe. Ensuring that an AGO's deliberations are based on diverse perspectives is a precondition of such an enterprise.

Third and last, alternative governance organizations themselves—or, if need be, the traditional governments that retain power to displace them—should devise and implement checks that render AGOs more accountable to the public. In the United States (as in other countries), administrative agencies that concentrate technical expertise within the government are empowered to make decisions with considerable independence from the more “political” branches. Yet these agencies are also constrained in ways that make them publicly accountable. For starters, their mandates are textually defined in law. Stakeholders who believe that an agency has abused its mandate can seek redress from Congress, which conducts regular oversight hearings. Or they can complain to the executive branch, whose head (the president) typically nominates the agency's leadership. Or they can challenge the agency's decision in the federal courts, which retain power to reverse a decision if it exceeds the agency's delegated authority. Similar mechanisms do not exist to check the decisions of ICANN, IETF, and W3C.<sup>23</sup> (Traditional governments can of course attempt to “undo” the decisions of these AGOs by enacting laws, but that check is more drastic—and far more difficult for complaining stakeholders to effect.) All of this is not to suggest that the checks on agency decision making in the United States should (or could) be imposed on ICANN and its ilk, which after all are private entities. Such checks may serve as points of departure, however, as public policymakers think about how to attenuate the insulation of these AGOs from public accountability.

### **Roles of Different Actors (III): Corporations, Traditional NGOs, and Users**

Conference discussions on the roles of different actors in Internet governance focused predominantly on nation-states and on AGOs such as ICANN. Yet participants uniformly agreed that other actors—corporations, traditional non-governmental organizations,

and users—are often just as integral in formulating effective governance solutions for the Net. Although participants did not address the challenges and opportunities confronting these other actors in detail, they did broach questions and insights that illuminate the relations of these actors to one another, to traditional governments and AGOs, and to the Net’s overall governance ecosystem.

### *Corporations*

With dominion over websites visited by more people per day than inhabit most cities, significant influence in shaping the Internet’s architecture, and greater proximity to the Net’s users and infrastructure than either nation-states or AGOs, corporations could well be described as the 800-pound gorillas of Internet governance. As nation-states increasingly seek to enlist their cooperation in policing the Net, and the Net itself spreads to non-Western states (such as China) with different expectations regarding the responsibilities of corporate actors, the importance of corporations in Internet governance is likely to grow larger still. This likelihood raises a host of difficult questions for both corporations and the traditional governments that regulate them. Broadly speaking, corporations need to ask themselves what their obligations are to the public beyond their shareholders when they act as *de facto* private governments whose decisions affect the lives of millions and implicate core societal values (such as free speech and privacy). Traditional governments, in turn, need to ask themselves whether it makes sense to continue to regulate firms in the same way where they exercise quasi-governmental authority over a sphere as important to society as the Internet.

The latter question addresses itself in different ways to different branches of traditional governments. For legislatures and executives, the key question may be whether and how to devise incentives that align corporate interests with a more expansive public interest—for instance, by encouraging corporations to adopt open-source code, meaningful privacy protections, and intellectual property regimes that safeguard the traditional fair-use rights of users on the Net. For courts, the question may be whether and how to redraw the doctrinal line separating “public” from “private” action—or to put it

another way, whether to broaden what lawyers call “state action” to include certain corporate conduct now considered private.<sup>24</sup> Broadening the state action rubric would bring more conduct within the ambit of many statutory and constitutional constraints and thereby provide users greater protections from abuse. It might also, however, discourage innovation and dampen private investment.

Legislatures, executives, courts, and corporations are each likely to wrestle with the implications of new kinds of governance partnerships between nation-states and firms. Arrangements in which states enlist (and sometimes conscript) the powers of private actors to serve traditional governmental functions such as law enforcement are particularly laden with challenges and tradeoffs. In certain cases—for example, in combating cyberterrorism—efforts by states to seek the assistance of corporations in policing illicit conduct that confounds traditional law enforcement techniques may yield substantial public benefit. But such efforts are not without costs, however: They risk reducing the transparency of regulation if, for instance, governments use corporate intermediaries to engage in widespread surveillance of the population without resort to the political process that ordinarily casts light on this kind of activity. And in other cases, government attempts to deputize private actors may have no positive public benefit at all to counterbalance the costs—for instance, where authoritarian regimes demand that firms assist them in rooting out political dissidents or “undesirables.” Conference participants did not delve deeply into the difficulties raised by the emerging class of public-private partnerships in Internet governance. It seems safe to say, however, that corporations will need to commit themselves to uphold certain public values on a “nonnegotiable” basis if they are to resist coercion by governments to engage in improper activities. Delivering on such a commitment is unlikely to come naturally to institutions whose primary mission is enhancing shareholder value and who rely on tolerance from their governmental hosts. But because many corporations operate multinationally, they may face pressure from customers in democratic societies (e.g., boycotts and protests) if they fail to do so. And corporations themselves may be more willing to take stands of principle if they are convinced that the growth of the Internet depends, in the long run, on the maintenance of key values that made the medium so attractive to begin with.<sup>25</sup>

### *Traditional NGOs*

Fortunately, corporations are not the only parties that can serve as a check on government actors. Long before the advent of the Internet, traditional non-governmental organizations contributed to society by performing a related cluster of oversight activities—reporting to the media and the public on corporate and governmental decisions, “translating” the implications of these decisions into terms that the public could more easily understand, and challenging them through relevant channels when they deviated from legal obligations, accepted norms, or the public’s interest. Several conference participants observed that in the Internet age—in which far-reaching political choices often are made outside the political arena and cast as “mere” technical decisions—these activities have become even more important. By serving as “transparency enforcers,” watchdogs, and whistleblowers, entities such as the Center for Democracy and Technology (CDT), the Electronic Privacy Information Center (EPIC), the Electronic Frontier Foundation (EFF), and other Net-focused NGOs occupy a critical niche in the Internet governance ecosystem.

Nor are Internet-focused NGO’s limited to these oversight roles. In some instances, they can also act as intermediaries in governance arrangements, facilitating interactions between states, corporations, and users by assuming coordination, enforcement, and other functions. A case in point: TRUSTe, a nonprofit organization whose stated mission is to build users’ confidence on the Net and, in so doing, to accelerate growth in e-commerce. The keystone of TRUSTe’s approach is a branded online seal that the organization awards to websites if they adhere to certain minimum privacy principles and agree to comply with TRUSTe’s oversight and complaint resolution process. Visitors to participating websites may feel more confident transacting there once they see TRUSTe’s imprimatur. The organization promotes compliance with its policies by demanding that participating sites sign a contract with TRUSTe; participants also have an incentive to comply because of the reputational harms they would likely incur if they were to embroil themselves in a controversy with the organization. The privacy principles to which TRUSTe requires adherence evolve periodically and reflect some input from the U.S. and other governments. The

current version of TRUSTe's participant contract, for instance, ostensibly incorporates the principles set forth in the Children's Online Privacy Protection Act.<sup>26</sup>

The TRUSTe model is not immune from criticism. Some may question whether it is realistic to assume, as TRUSTe does, that the interests of corporations and users in safeguarding individuals' privacy in cyberspace are naturally aligned because both benefit from promoting greater "trust" on the Net. Others may argue that TRUSTe actually undermines the public good by giving users the false impression that participating websites have agreed to respect their privacy. (In fact, the current TRUSTe contract requires only that participants disclose to users what personal information they are gathering, how they will employ it, with whom they will share it, and whether users have an option to control its dissemination—protections that are procedural and do not actually forbid participating sites from collecting or sharing certain types of information.) Regardless whether such criticisms have merit, however, TRUSTe provides an important demonstration of how NGOs can serve as alternatives to the state in facilitating Internet governance arrangements. At a minimum, this model points to the possibility of fruitful competition between state-mandated and NGO-enabled solutions to certain Net governance challenges.<sup>27</sup>

### *Users*

Ideally, governance solutions for the Internet would reflect not only the complex interactions of states, AGOs, corporations, and NGOs but also the consent of the governed—that is, the Internet users whose lives are affected. But in practice, the growing significance of the Internet to everyday life and the accompanying intercession of public and private actors in Net governance have made it increasingly difficult for users to create meaningful spheres of self-governance or even to influence governance decisions that affect them. Early adopters of new Net-related applications and technologies, participants agreed, can still exercise real influence over governance decisions pertaining to an innovation because they collectively wield the threat of deserting before the innovation "takes off." Paradoxically, once mass adoption has occurred, it may be harder for users to shape how an application or technology is

regulated. This effect—an inverse relationship between the total number of users and their democratic power—gives early adopters the onus (or opportunity) of being the public’s representatives at decision-making tables.<sup>28</sup> Early adopters, however, sometimes do not have the same concerns and values regarding technologies as later-stage adopters, and may not favor the same types of solutions to public policy challenges. Conference participants did not arrive at any conclusions on how to address these challenges, if at all. But in light of their consensus that users generally deserve a larger role in Internet governance arrangements, one upshot may be that building public accountability is an important goal at several stages of decision making regarding Net-related technologies—both in early stages, when critical architectural decisions are being made, and at later stages, when a greater number of “everyday” individuals have become stakeholders.

### **Coming Full Circle: Three Specific Governance Challenges**

While many of the conference’s discussions focused on mapping the interactions between different actors in the Internet governance ecosystem, participants also discussed three specific governance challenges facing the Internet: extraterritoriality, user confidence issues, and, more briefly, namespace management. Participants chose to focus on these three areas based in part on their sense that each is important to the future of the Net. They also agreed, however, that other issues are of equal (and perhaps greater) importance. And they were acutely aware that each of the three areas has attracted a wealth of prior discussion and scholarship, including symposia, articles, and books. Accordingly, participants did not seek to arrive at even provisional “solutions” to these challenges. Instead they sought to air their thoughts, in a deliberative forum, on what the right questions are and on what dangers public policymakers need to avoid.

#### *Extraterritoriality*

Attempts by states to enforce their laws beyond their territorial borders are nothing new. Many governments, for instance, have long maintained a right to prosecute terrorists under domestic laws for crimes committed against their citizens abroad. Prior to the

popularization of the Internet, states had developed an array of legal devices to resolve such extraterritorial assertions of power. Reciprocal extradition treaties bound states to deliver fugitives to one another under defined circumstances, for instance, and the doctrine of comity called on courts in competing jurisdictions to defer to one another's authority to handle a case after weighing various factors.

The explosive growth of the Internet, however, threatens to compromise the effectiveness of these old legal devices and to make extraterritoriality a major conundrum. The reasons are familiar. The Net has made it vastly easier for content and conduct to traverse national borders and has exponentially increased the volume of cross-border transactions. A mouse click in the United States can generate a storm in China—and the number of clicks per day that transmit data across national borders numbers, conservatively, in the billions. What's more, states can't easily police these transactions: There are no customs inspection points for data on the information superhighway. Reacting to the new porousness of their borders, states increasingly seek to impose what were formerly local requirements on distant actors. This trend potentially subjects Internet users and service providers to the laws of hundreds of different jurisdictions whose rules may be in conflict. The conceptual difficulty of tracing a particular Internet transaction to a single "place" in the physical world renders extraterritorial assertions of authority more complicated still.

The challenges posed by the rise of extraterritoriality in the Internet age are exemplified by the well-known *Yahoo!* case. The case began when a group of French plaintiffs led by a French civil rights organization sued Yahoo! in French court for violating a domestic statute that forbids the public display in France of Nazi-related symbols. The groups sought to prevent Yahoo! from hosting auctions for Nazi memorabilia. A French court, applying the French statute, ordered Yahoo! to block access to the disputed auctions by Internet users in France even though the auctions were hosted on a U.S. server and accessed at the URL "http://www.yahoo.com." (Notably, Yahoo! did not host the auctions on the servers of its French subsidiary, accessible at "http://fr.yahoo.com.") After collecting expert testimony, the French court later clarified that it

expected Yahoo! to reengineer its content servers in the United States and elsewhere to come into compliance with the order. Yahoo! then initiated its own lawsuit in U.S. federal district court seeking a declaratory judgment that the French court's order violated the First Amendment to the U.S. Constitution and was therefore unenforceable in the United States. In November 2001, the U.S. district court sided with Yahoo!, ruling that the company could not be compelled to comply with the French order in the United States.<sup>29</sup>

While the *Yahoo!* case centers on freedom of expression, Internet traffic is raising similar jurisdictional conflicts in the areas of taxation, intellectual property rights, consumer protection, privacy, and criminal action (among others). Discussing the *Yahoo!* case as well as the jurisdictional conflicts arising in these other areas, conference participants expressed diverse views on the problem of extraterritoriality. On three points, however, a rough consensus emerged.

First, as touched on earlier, participants agreed that states are unlikely to resolve the normative and policy differences that underlie their jurisdictional conflicts. France and the United States, for instance, are unlikely to harmonize their differences on the appropriate boundaries of freedom of expression. Thus, it is probably unrealistic to expect the problem of extraterritoriality to be solved by a grand treaty that spells out permitted and forbidden conduct throughout cyberspace.

Second, most participants also agreed that states have strong claims to regulate conduct within their own territory. Thus, France's claim to prohibit the display of Nazi memorabilia in France is strong; but by the very same principle, so is the United States' claim to permit the display of such memorabilia in the U.S. In practice this "pluralism principle" suggests that the French court's order is defensible insofar as it seeks to regulate behavior in France but that the American judicial decision declining to enforce the French order as it applies to Yahoo!'s U.S.-based servers is similarly defensible. Of course, if Yahoo! has assets in France, it may be vulnerable to edicts of the French judiciary despite the American court's refusal to enforce the French order.

Finally, most participants agreed that states' claims to regulate conduct outside their territory—even conduct that affects their



interests—is weaker. Participants voiced divergent views on whether extraterritorial assertions of power aimed at foreign-based Internet users and service providers are justifiable under *any* circumstances. Some answered “yes,” particularly where a state’s “vital interests” are implicated—for instance, in protecting its citizens from physical harm, ensuring the integrity of its electoral processes, or perhaps even safeguarding the functionality of the Internet itself. Other participants answered with a categorical “no.” These differences of opinion, however, highlighted a general consensus that states are on far weaker footing when they seek to impose their normative and policy choices beyond their borders.

### *Confidence Issues*

Extraterritoriality represents an age-old problem that the Internet has made more complicated. In contrast, confidence issues—the cluster of issues centering on how to promote privacy, security, and trust on the Net—present problems as novel as cyberspace itself. Two brief comparisons illustrate the gap between our confidence in the “physical” world as opposed to the “virtual.” First, compare letters and e-mail. When one sends a postal letter, one can be reasonably certain that no one will open and read the contents while it is in transit. Similarly, one can safely assume that the letter is unlikely to be disseminated further once it has reached its intended destination. Neither assumption is valid with respect to e-mail. Second, compare information distributed through traditional media (such as television) with information available on the Net. Polls suggest that approximately 70 percent of Americans consider the former to be trustworthy, whereas a similar proportion of the population deems the latter to be untrustworthy.<sup>30</sup>

These comparisons suggest that we have a ways to go before individuals conduct their business in cyberspace with the same degree of confidence that they do in the physical world. Time will surely help narrow the gap; after all, the Internet is still relatively young as a mass medium for commerce and information. Yet closing the gap entirely, many participants agreed, will not be easy—in part because of the tradeoff on the Net between privacy and what might be called “transactionability.” Privacy is available to users on the Net in a continuum, ranging from pure anonymity (no one knows any

facts about you at all) to pseudonymity (others know selected facts about you but not your identity) to full identity (others know all the relevant facts about you that are true). Often, Net users prefer more privacy to less, and in many contexts they would just as soon remain anonymous to others in cyberspace if that option were available. The problem is that anonymity prevents the development of reputation—an essential component in a significant number of transactions. Consider, for instance, a deal for the purchase of valuable assets over the Internet between parties who had not previously transacted with one another. Unless an intermediary were available to supply the missing trust (e.g., by vouching for the reputation of the parties or insuring the deal), the anonymity of either buyer or seller would likely preclude the transaction. As P2P applications proliferate and the number of direct, unmediated transactions between individuals increases, reputation is likely to become even more important. The foregoing discussion, then, suggests that privacy and reputation systems in cyberspace must develop hand-in-hand if users are to enjoy greater confidence transacting on the Net. Striking the proper balance between the two will be difficult, but a balance must be struck lest users limit their interactions on the Net for want of either.

While conference participants agreed on the need to balance privacy and reputation, they diverged on the proper role of traditional governments in promoting privacy in cyberspace and on “how much” privacy is enough. In one camp were participants who advocated a market approach to privacy. This approach would involve minimal government regulation; instead, it would rely on “self-governance” measures designed to facilitate user choices on privacy matters. Adherents of the market approach maintained that “privacy” is a murky concept on which there is little agreement among individuals, that significant government regulation in this sphere would create a regulatory morass without yielding satisfactory privacy protection, and that self-governance solutions (such as TRUSTe or P3P) are superior because they allow users to decide for themselves whether a given website’s policies accord with their privacy preferences. In another camp were participants who advocated government intervention to safeguard individuals’ privacy on the Internet. These participants argued that most people

desire a substantial basic level of privacy protection that a market-based approach would not afford—in particular, a requirement that a website notify them of its privacy practices and obtain their informed consent before collecting and sharing information about them. A basic level of privacy protection would also, these participants maintained, have broader benefits for society irrespective of its popular support; for example, it would likely make Internet users more comfortable experimenting with new forms of interaction on the Net.

The divergent views that emerged in the conference discussions are representative of a debate over Internet privacy that has been unfolding in legal, political, and technological circles in the United States for some time. While some disagreements between the two camps in this debate may be irreconcilable, those camps have not yet confronted the challenge of working out a mutually agreeable solution through the crucible of the federal legislative process. Both camps may need to reassess their long-held views given the events of September 11, 2001, and the greater emphasis on security issues that has ensued. This debate, it appears, is far from over.

### *Namespace Management*

The past five years have witnessed dramatic changes in Internet namespaces. Previously, the single namespace that facilitated interaction on the Net (the domain name system) was a commons “owned” by no one. Today, privately owned namespaces—such as ICQ, AIM, and Napster—collectively include far more addresses than does the DNS. These new namespaces differ not just in ownership but also in architecture. Increasingly, the addresses they contain refer to people, not to machines, making them “portable” in a way that IP addresses are not. Such address portability frees users to make connections with one another directly, through P2P applications, and to abandon their reliance on centralized servers—servers which are much more amenable to control by governments or private actors.

These changes, participants agreed, introduce a host of governance challenges with which society is only beginning to wrestle. Should the public feel comfortable with corporate ownership of giant namespaces composed principally of the names

of millions of users and information about when those users go online? Should these private namespaces be regulated to prevent conduct by owners that arguably harms consumer welfare—such as refusal to interconnect with similar namespaces or detailed monitoring of users’ behavior on the Net? Or is the ability of Internet users to “vote with their mice” a sufficient check on these harms? To frame the problem slightly differently, what are the responsibilities of namespace owners to users and other service providers? To governments that seek their cooperation in regulating the “wild frontier” of P2P connectivity? To the future growth and success of the Internet? Although participants did not hazard answers, they agreed that these questions will grow in importance and merit a prominent place on the Internet governance agenda.

## **Conclusion**

This report began with the uncontroversial observation that the days of the borderless Internet are gone. What will take its place? The future is already rapidly emerging through the choices of the Net’s stakeholders. It would be hubris to hope that a conference could map out that future. Our conference had a different aim: to contribute an imperfect map of dangers and opportunities. The Net’s stakeholders—users, firms, states, AGOs, NGOs—each have their own destinations in mind. Many are deeply engaged in efforts to steer the Net toward their preferred future. Working together with a shared map of the pitfalls and promises along the journey, they may be able to chart a path that is safer and more rewarding for all. Hopefully, and at the very least, a shared map will encourage broader dialogue among these diverse stakeholders, and between them and the public that will inhabit the Internet to come.

## Notes

1. A “namespace” is an online database whose records contain addresses of some kind. Namespaces have different characteristics: The addresses they contain, for instance, can point to open-ended resources (as in a “keyword” system that allows users to search for whatever they wish) or to particular types of resources (as in a namespace of book or music titles). Examples of namespaces include the domain name system, keyword systems (such as those of AOL or RealNames), and instant messaging systems (such as AIM or ICQ). Thanks to Keith Teare of RealNames for providing a basic explanation of the concept.
2. See, e.g., Patrick Butler et al., “A Revolution in Interaction,” *McKinsey Quarterly*, no. 1 (1997), 9–14.
3. See William J. Mitchell, *City of Bits: Place, Space, and the Infobahn* (1995); Mitch Kapor, quoted at <http://cyber.law.harvard.edu/people/reagle/inet-quotations-19990709.html> (last accessed January 31, 2002); Larry Lessig, *Code: and Other Laws of Cyberspace* (1999).
4. U.S. Constitution, art. vi, §2: “This Constitution, and the Laws of the United States which shall be made in Pursuance thereof; and all Treaties made, or which shall be made, under the Authority of the United States, shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any State to the Contrary notwithstanding.”
5. Colloquially speaking, the end-to-end principle posits that networks should be designed to place control over key features in applications residing at the “edges” (or “ends”) of the network rather than in the network itself. This principle empowers users at the expense of those who would make choices on users’ behalf and build these choices into the network. For more detailed expositions of the end-to-end principle, see David P. Reed, *The End of the End-to-End Argument* (2000), available at <http://www.reed.com/dprframeweb/dprframe.asp?section=paper&fn=endofendoend.html> (last accessed January 2, 2002), and Jerome H. Saltzer, David P. Reed, and David Clark, *End-to-End Arguments in System Design* (1984), available at <http://www.reed.com/Papers/EndtoEnd.html> (last accessed January 31, 2002).
6. See Jeff Quan, “Case Study: Regulating Online Gambling,” Cnet News, July 11, 1997, available at <http://news.cnet.com/news/0,10000,0-1005-201-320416-0,00.html> (last accessed Dec. 23, 2001).
7. See Wendy M. Grossman, “Surveillance by Design,” *Scientific American*, September 2001, available at <http://www.siam.com/2001/0901issue/0901scicit5.html> (last accessed January 31, 2002).
8. One risk of regulation through private terms-of-service agreements is that such regulation would likely offer little protection against arbitrary or discriminatory conduct by the firm. If subject to the judicial scrutiny applied to state action, this type of regulation might well be struck down. That standard of scrutiny is probably not appropriate under the current scope of the state action doctrine, but it does suggest some of the problems of devolving regulation ordinarily entrusted to the state into private hands.
9. The example discussed in this paragraph is Lessig’s. See Lessig, *Code*, 136.
10. The papers presented at the Stanford Program in Law, Science, and Technology’s December 2000 conference on “The Policy Implications of End-to-End” provide a good introduction to

this debate. These papers are available at <http://lawschool.stanford.edu/e2e/papers.html> (last accessed January 2, 2002).

11. The citations to Rotenberg's work in this paragraph refer to Marc Rotenberg, "Fair Information Practices and the Architecture of Privacy," *2001 Stanford Technology Law Review* (2001), 1.
12. In *Olmstead v. United States*, 277 U.S. 438 (1928), the Supreme Court upheld the constitutionality of a telephone wiretap installed without a warrant, reasoning that the Fourth Amendment's protection against unreasonable searches and seizures does not extend to telephone conversations. In dissent, Justice Brandeis maintained that the amendment should be interpreted to protect people against all unjustifiable government intrusions on their privacy, including intrusions on their uses of new technologies—such as the telephone—that did not exist when the amendment was adopted. In *Katz v. United States*, 389 U.S. 347 (1967), the Court embraced the core of Brandeis' view, ruling that the Fourth Amendment protects persons against all unreasonable searches and seizures, including those of a phone conversation. The Privacy Act of 1974 (as amended), codified at 5 U.S.C. 552A, created broad limitations on the collection, use, and dissemination of personal information held by government agencies. The key principles underlying the Act were first articulated in a 1973 report of the Department of Health, Education and Welfare's Advisory Committee on Automated Personal Data Systems. The Advisory Committee's proposed "Code of Fair Information Practices" formed the basis for the Privacy Act and much subsequent privacy legislation. This original Code is excerpted at [http://www.epic.org/privacy/consumer/code\\_fair\\_info.html](http://www.epic.org/privacy/consumer/code_fair_info.html) (last accessed January 31, 2002).
13. For a detailed elaboration of these features of the American Constitution, see Akhil Reed Amar, "Of Sovereignty and Federalism," 96 *Yale Law Journal* (1987), 1425. Of course, separation of powers and co-existent sovereigns—though arguably American inventions—are no longer exclusive characteristics of the American system of government. In many other settings, such as the European Union, decisions are made at supra-national, national, and local levels, imparting similar benefits.
14. William J. Clinton and Albert Gore, *A Framework for Global Electronic Commerce* (1997), available at <http://www.iitf.nist.gov/elecomm/ecom.htm> (last accessed January 31, 2002).
15. John Perry Barlow, *A Declaration of the Independence of Cyberspace* (1996), available at <http://www.eff.org/~barlow/Declaration-Final.html> (last accessed December 20, 2001).
16. David R. Johnson and David G. Post, "Law and Border: The Rise of Law in Cyberspace," *Stanford Law Review* 48 (1996): 1367, available at <http://www.temple.edu/lawschool/dpost/Borders.html> (last accessed January 31, 2002).
17. Because it is unlikely that states can overcome these handicaps, one response may be to heighten the awareness of codewriters and hardware engineers regarding the policy implications of their work. This goal might be accomplished through a "reverse Office of Technology Assessment"—an organization that would identify the policy choices that are available to be implemented in software and hardware.
18. See, e.g., Larry Lessig, "Innovation, Regulation, and the Internet," *American Prospect* 11, no. 10 (March 27–April 20, 2000), available at <http://www.prospect.org/print/V11/10/lessig-1.html> (last accessed January 31, 2002).
19. The working group's assessment is quoted in Rotenberg, "Fair Information Practices," paragraph 78.

20. Richard C. Longworth, "Government Without Democracy," *American Prospect* 12, no. 12 (July 2–16, 2001), available at <http://www.prospect.org/print/V12/12/longworth-r.html> (last accessed January 31, 2002).
21. Lack of accountability to the public is not the sole reason that many AGOs face a legitimacy gap. As several conference participants pointed out, longevity (i.e., the amount of time an institution has existed) is another important driver of legitimacy, and AGOs participating in Internet governance obviously have not accrued the longevity of traditional governments and even some corporations and NGOs. But this facet of their legitimacy gap will narrow with time, if they can overcome other problems (e.g., their lack of public accountability) and survive in the Internet governance ecosystem.
22. The DNS is the method by which Internet addresses in mnemonic form such as "www.yahoo.com" are converted into numeric IP addresses on which the Net's routing architecture relies.
23. A recent decision of the U.S. Court of Appeals for the First Circuit held that under the U.S. Anticybersquatting Consumer Protection Act, persons ordered to give up their domain names in rulings arising from ICANN's Uniform Domain-Name Dispute Resolution Policy can challenge those rulings and seek to retain title to their domain names by suing in U.S. courts. See *Sallen v. Corinthians Licenciamientos LDTA*, Case. No. 01-1197 (1st Cir. 2001), available at <http://www.ca1.uscourts.gov/cgi-bin/getopn.pl? OPINION=01-1197.01A> (last accessed January 3, 2002); Gwendolyn Mariano, "Court: U.S. Law Trumps Domain Decisions," *CNet News*, Dec. 7, 2001, available at <http://news.cnet.com/news/0-1005-200-8105325.html? tag=lh> (last accessed January 31, 2002). It is too early to tell whether this decision presages a trend, but at present American law does not provide a generally applicable mechanism for judicial review of rulings by AGOs.
24. Here—as in many other parts of the Internet governance puzzle—the pathbreaking scholarship is Larry Lessig's. See Lessig, *Code*, 217–18 (suggesting that the proper scope of the "state action" doctrine in the Internet context is ambiguous and that one could mount a plausible argument that the Constitution's strictures should apply to Internet design decisions).
25. What those key values are, of course, is open to debate. At minimum, they would seem to encompass the values essential to the preservation of the central characteristics of the Internet. These characteristics include the ability to communicate with any other willing user online; to access any content made available to the public; and to choose content, services, and features on the Net free from intrusive constraints built into the network itself.
26. See *The TRUSTe Story: Building Trust Online—TRUSTe, Privacy, and Self-Governance* (2000), note 8; available at <http://www.truste.org/about/oprah.doc> (last accessed January 31, 2002).
27. The TRUSTe model also illustrates the tacit yet important relationship between NGO-enabled solutions and private governance arrangements. Private governance arrangements for the Net are on the rise at least in part because firms, working with and through organizations such as TRUSTe (as well as through associations such as the Global Business Dialogue for Electronic Commerce), have found receptive ears for their arguments in favor of self-regulation.
28. The inverse relationship also suggests a difficulty that corporations face in assessing the policy implications of the "code" they write: The feedback they receive typically reflects the perspective of technologically sophisticated users, not the broader public.

29. See *Yahoo!, Inc. v. La Ligue Contre Le Racisme Et Le Antisemitisme*, Order Granting Motion for Summary Judgment, Case No. C-00-21275 JF (N.D. Cal. 2001), available at [http://www.cand.uscourts.gov/cand/tentrule.nsf/4f9d4c4a03b0cf70882567980073b2e4/daaf80f58b9fb3e188256b060081288f/\\$FILE/yahoo%20sj%20%5Bconst%5D.PDF](http://www.cand.uscourts.gov/cand/tentrule.nsf/4f9d4c4a03b0cf70882567980073b2e4/daaf80f58b9fb3e188256b060081288f/$FILE/yahoo%20sj%20%5Bconst%5D.PDF) (last accessed January 3, 2002).
30. On the public's trust of information disseminated through traditional news media such as television, see, for example, Gallup Poll, July 13–14, 1998 (finding that 73 percent of Americans believe they “can trust” information provided on their local television news), available at [http://www.pollingreport.com/media.htm# Accuracy of News Reports](http://www.pollingreport.com/media.htm#Accuracy%20of%20News%20Reports) (last accessed January 31, 2002). On the public's distrust of information available on the Internet, see, for example, Markle Foundation, *Toward a Framework for Internet Accountability* ii (2001) (finding that 70 percent of respondents agree with the proposition that “you have to question the truthfulness of most things you read on the Internet,” as opposed to the proposition that “you can trust most things you read on the Internet”).





# APPENDIX





The Aspen Institute Internet Policy Project

*Rethinking Boundaries in Cyberspace*

**List of Conference Participants**

Aspen, Colorado  
July 22-25, 2001

**Izumi Aizu**

Principal  
Asia Network Research, Inc.  
JAPAN

**Zoë Baird**

President  
The Markle Foundation

**Yochai Benkler**

Professor of Law  
School of Law  
New York University

**Ramsen V. Betfarhad**

Counsel  
House Energy and Commerce  
Committee  
United States House of  
Representatives

**Vint Cerf**

Senior Vice President  
Internet Architecture and  
Technology  
WorldCom

**Kilnam Chon**

Professor  
Computer Science Department  
Korea Advanced Institute of  
Science  
Technology  
REPUBLIC OF KOREA

**Adam Ciongoli**

Counselor to the Attorney  
General  
United States Department of  
Justice

**Roger Cochetti**

Senior Vice President for Policy  
VeriSign

**Esther Dyson**

Chief Executive Officer  
EDventure Holdings, Inc.

**Charles M. Firestone**

Executive Director  
Communications and Society  
Program  
The Aspen Institute

**Link Hoewing**

Assistant Vice President  
Internet and Technology Issues  
Verizon

**David R. Johnson**

Partner  
Wilmer, Cutler, & Pickering

**Erez Kalir**

Rapporteur

Note: Titles and affiliations are as of the date of the conference.

**Stephanie Keller-Bottom**

Director  
Innovent  
Nokia

**Tara Lemmey**

Founder and Chief Executive  
Officer  
LENS Ventures  
and  
Founder and Chairman  
Psoom, Inc.

**Mark MacCarthy**

Senior Vice President  
Public Policy  
VISA U.S.A., Inc.

**Ira Magaziner**

President  
SJS, Incorporated

**Elliot Maxwell**

Senior Fellow  
Communications and Society  
Program  
and  
Director  
Internet Policy Project  
The Aspen Institute

**Lori McLean**

Vice President  
Events and EBC Centers  
Nortel Networks

**David Nassef**

Vice President  
Federal Relations  
Pitney Bowes, Inc.

**T. Michael Nevens**

Managing Director  
High Tech Practice  
McKinsey & Company, Inc.

**Niels Christian Nielsen**

President and CEO  
Catenas, Ltd.  
UNITED KINGDOM

**Clay Shirky**

Writer and Consultant

**James B. Steinberg**

Vice President  
and  
Director  
Foreign Policy Studies  
The Brookings Institution

**Keith Teare**

CEO and Founder  
RealNames Corporation

**Paul Verhoef**

Acting Head of Unit  
International Aspects  
DG Information Society  
European Commission

**William Whyman**

President  
The Precursor Group

*Staff:***Lisa Dauernheim**

Program Coordinator  
Communications and Society  
Program  
The Aspen Institute

**Amanda Mills**

Research Assistant  
Communications and Society  
Program  
The Aspen Institute

## About the Authors

**Erez Kalir** is a management consultant, and was special assistant to the General Counsel at the Federal Communications Commission in 2001. He helped advise the FCC's General Counsel and commissioners on the law and policy of open access, spectrum management, merger reviews, and implementation of the 1996 Telecommunications Act (among other matters). Kalir is a graduate of Stanford University, Oxford University where he studied as a Rhodes Scholar, and Yale Law School where he served as a senior member of the Law Journal.

**Elliot E. Maxwell** is an information and communications technology consultant focusing on the Internet and electronic commerce. He was senior fellow for the digital economy and director of the Internet Policy Project for the Aspen Institute's Communications and Society Program in 2001. Prior to joining the Institute, Maxwell was special advisor to the Secretary of Commerce for the digital economy. In that position he served as principal advisor to the Secretary on the Internet and electronic commerce. He coordinated the Commerce Department's efforts to establish a legal framework for electronic commerce, ensure privacy, protect intellectual property, increase Internet security, encourage broadband deployment, expand Internet participation, and analyze the impact of electronic commerce on all aspects of business and the economy. He was a member of the U.S. Government Interagency Working Group on Electronic Commerce from its creation until January, 2001.

Previously, Maxwell worked for almost ten years as assistant vice president for corporate strategy of Pacific Telesis Group, where he combined business, technology, and public policy planning. He served at the Federal Communications Commission as special assistant to the chairman, deputy chief of the Office of Plans and Policy, and deputy chief of the Office of Science and Technology, and he was director of international technology policy at the Department of Commerce. Maxwell also worked as senior counsel to the U.S. Senate Select Committee on Intelligence Activities.

Maxwell graduated from Brown University and Yale University Law School. He has written and spoken widely on issues involving electronic commerce, telecommunications, and technology policy.



# **The Aspen Institute Communications and Society Program**

**[www.aspeninstitute.org/c&s](http://www.aspeninstitute.org/c&s)**

The Communications and Society Program is a global forum for leveraging the power of leaders and experts from business, government and the nonprofit sector in the communications and information fields for the benefit of society. Its roundtable forums and other projects aim to improve democratic societies and diverse organizations through innovative, multidisciplinary, values-based policymaking. They promote constructive inquiry and dialogue and the development and dissemination of new models and options for informed and wise policy decisions.

In particular, the Program provides an active venue for global leaders and experts from a variety of disciplines and backgrounds to exchange and gain new knowledge and insights on the societal impact of advances in digital technology and network communications. The Program also creates a multidisciplinary space in the communications policymaking world where veteran and emerging decision makers can explore new concepts, find personal growth and insight, and develop new networks for the betterment of the policymaking process and society.

The Program's projects fall into one or more of three categories: communications and media policy, communications technology and the democratic process, and information technology and social change. Ongoing activities of the Communications and Society Program include annual roundtables on journalism and society, international journalism, telecommunications policy, Internet policy, information technology, and diversity and the media. The Program also convenes the Aspen Institute Forum on Communications and Society, in which CEOs of business, government, and the nonprofit sector examine issues relating to the new technologies and lifelong learning.

Conference reports and other materials are distributed to key policymakers and opinion leaders within the United States and around the world. They are also available to the public at large through the World Wide Web.







THE ASPEN INSTITUTE

Fulfillment Office

P.O. Box 222

109 Houghton Lab Lane

Queenstown, MD 21658

02-007