

# Rewriting Broadband Regulation

David Bollier  
*Rapporteur*



THE ASPEN INSTITUTE

*Communications and Society Program*

Charles M. Firestone  
Executive Director  
Washington, D.C.

2011

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

The Aspen Institute  
Publications Office  
P.O. Box 222  
109 Houghton Lab Lane  
Queenstown, Maryland 21658  
Phone: (410) 820-5326  
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, NW  
Suite 700  
Washington, DC 20036  
Phone: (202) 736-5818  
Fax: (202) 467-0790

Charles M. Firestone  
*Executive Director*

Patricia K. Kelly  
*Assistant Director*

---

Copyright © 2011 by The Aspen Institute

This work is licensed under the Creative Commons Attribution-Noncommercial 3.0 United States License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc/3.0/us/> or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA.

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

Published in the United States of America in 2011  
by The Aspen Institute

All rights reserved

Printed in the United States of America

ISBN: 0-89843-548-X

11-009

1820CSP/11-BK

# Contents

**FOREWORD**, *Charles M. Firestone* .....v

**REWRITING BROADBAND REGULATION**, *David Bollier*

An Overview of the Challenges Facing the Internet and Broadband ..... 2

*How Shall We Conceptualize the Internet?*.....2

*The Topography of the Internet*.....4

*Four Significant Threats to the Internet as a Commons*.....6

*Varieties of Enclosure of the Internet Commons*..... 8

Digital Embassies for Data ..... 12

*National Sovereignty and the Internet* ..... 13

*Digital Embassies and the Free Flow of Commercial Data*.....14

*The Challenge of International Implementation*..... 18

The Future of Broadband ..... 21

*The International Broadband Experience*.....21

*Investment Trends in Broadband*.....26

*Jurisdiction, Universality and Competition*.....28

*Personal Data, Privacy and Other Social Goods* ..... 33

Conclusion..... 35

**APPENDIX**

Conference Participants ..... 39

About the Author..... 43

Previous Publications from the Aspen Institute

    Communications Policy Project ..... 45

About the Aspen Institute

    Communications and Society Program ..... 51

*This report is written from the perspective of an informed observer at the  
Twenty-Fifth Annual Aspen Institute Conference on Communications Policy.  
Unless attributed to a particular person, none of the comments or ideas contained  
in this report should be taken as embodying the views or carrying the endorsement  
of any specific participant at the Conference.*

# Foreword

It is perhaps appropriate that the 25th annual Aspen Institute Conference on Communications Policy comes as the world reaches a tipping point with respect to the broadband medium. If, as former FCC Chairman Reed Hundt has proposed, broadband is the new “common medium,” possibly subsuming broadcasting and telephony as we know them, then what are the implications for national and even international regulatory regimes and policies?

As debates of current regulatory jurisdictional issues arise, and on the heels of the release of America’s National Broadband Plan, the summer of 2010 was a critical time to reconsider broadband regulations. Reflecting on the National Broadband Plan and some international models, 38 leading experts in broadband technology, telecommunications policy and Internet commerce met August 11-14, 2010 in Aspen to consider how the United States should reform its broadband regulatory system. Participants looked at international models and examples, as well, and considered how data and communications should be protected in the international arena.

The resulting report, *Rewriting Broadband Regulation*, explores a range of policies for U.S. broadband regulation, many of them derivative of the National Broadband Plan adopted by the Federal Communications Commission only a few months before the conference. For the most part, conference participants refined policies and nuances of a rather familiar regulatory terrain.

But they ventured into new and interesting territory with the novel concept of “digital embassies.” They saw this as a way of dealing with jurisdictional issues associated with the treatment and protection of data in the cloud, i.e., data that is provided in one country but stored or manipulated in another. The concept is that the data would be treated throughout as if it were in a kind of virtual embassy, where the citizenship of the data (i.e., legal treatment) goes along with the data. This policy seed has since been cultivated in various other regulatory environments.

The conference itself included both plenary and working group sessions. At times the author refers to working group recommendations, which were refined proposals to the larger group. The conference did not vote or ask for consensus on any of the proposals. So the ensuing write-up is essentially what conference participants considered and generally agreed on, short of formally accepting. Accordingly, unless someone is actually quoted in the text, the reader should not assume that any particular participant or organization agrees with any specific statement in the text.

### **Acknowledgments**

I want to take this opportunity to thank our sponsors for making this conference possible: AT&T, Cablevision Systems, Cisco Systems, Comcast Corporation, Credit Suisse, Entertainment Software Association, Ford Foundation, Google, Intel Corporation, John S. and James L. Knight Foundation, Liberty Global Inc., Microsoft, National Association of Broadcasters, Qualcomm Inc., Regulatory Source Associates, Time Warner Cable, Verizon Communications, and The Walt Disney Company.

I also want to acknowledge and thank David Bollier for his intelligent account of the conference discussions; and our participants, listed in the Appendix, for their contributions to these complicated topics. Finally, I want to thank Sarah Eppehimer, Senior Project Manager, and Ian Smalley, Program Associate, for their help in producing the conference and this report, along with the Communications and Society Program's Assistant Director Patricia Kelly, who oversaw its editing and publication.

Charles M. Firestone  
Executive Director  
Communications and Society Program  
The Aspen Institute  
Washington, D.C.  
April 2011

**REWRITING BROADBAND REGULATION**

*David Bollier*





# Rewriting Broadband Regulation

*David Bollier*

By wide consensus, the evolution of broadband as the chief medium of access to the Internet has reached an inflection point. Many significant, interrelated developments are all unfolding at once, making it a timely moment to revisit the future of broadband regulation. Recent developments include court rulings and technological advancements; shifts in consumer demand and investment opportunities; an evolution in the component parts of the Internet, such as new applications and wireless services; a growing body of experience with international regulatory models; and new leadership at the Federal Communications Commission.

In an attempt to take stock of the many factors affecting broadband today and in the future, the Aspen Institute Communications and Society Program convened 38 leading experts in broadband technology, telecommunications policy and Internet commerce to identify and access the salient issues. Participants included representatives from cable system operators, telecommunications companies, software and computer companies, government agencies, policy think tanks, academia, consumer advocacy organizations and foundations.

The group met from August 11 to 14, 2010, in Aspen, Colorado, in a series of focused conversations moderated by Charles M. Firestone, Executive Director of the Aspen Institute Communications and Society Program. Rapporteur David Bollier prepared this interpretive synthesis of the far-ranging discussions in an effort to convey the key points of consensus, disagreement and recommended action for the future.

There was broad agreement that the future of broadband is critical to many aspects of American life—the economy, technological innovation, civic empowerment, social needs and convenience, and much else. However, because broadband is implicated in a much larger ecosystem of Internet technologies and policies, not to mention myriad national economic priorities and social concerns, any conversation about broadband quickly becomes embroiled in a complicated landscape of related, and arguably related, concerns.

The following pages provide an overview of the key themes of discussion, followed by a series of recommendations developed by conference participants via three working groups that reviewed different aspects of the broadband future. The working groups made recommendations about how to promote international trade in data services, which resulted in a “digital embassies” proposal; new ways to speed deployment and adoption of broadband; and new ways to protect personal data and promote trust in online contexts.

## **An Overview of the Challenges Facing the Internet and Broadband**

### *How Shall We Conceptualize the Internet?*

In talking about the future of broadband regulation, much depends upon what we mean when we talk about the Internet. Is it just the physical infrastructure that makes up wired, and now wireless, telecommunications? Or does it extend to what we use to connect to the Internet, the software applications that run on servers and devices, and the protocols used to transmit information?

“It’s not entirely clear to me what we’re talking about when we talk about the Internet,” said Robert Pepper, Vice President of Technology Policy at Cisco Systems. “Are we talking about the networks? The content? Mobile communications? Are we talking about the digital ecosystem?” Pepper noted that some Middle Eastern countries want to block RIM’s BlackBerry messaging service because they cannot control it. “Is *that* the Internet?” Pepper asked. “Is text messaging part of the Internet?”

Conference participants agreed that it is best to consider the entire ecosystem of digital technologies when talking about broadband. A broad array of technologies, regulatory policies and markets all play roles in the functioning of the Internet commons and directly or indirectly affect broadband. It is impossible to talk about digital devices, applications, mobile communications, content or broadband in isolation from the entire ecosystem. A “broader definition” is also appropriate because it takes account of the many different participants with a stake in the Internet, suggested Michael Gallagher, President and CEO

of the Entertainment Software Association, arguing that the providers of network infrastructure are not the only ones with a stake in broadband policies.

Indeed, we may be justified in treating the Internet as “essential infrastructure” similar to roads, bridges and ports. Eli Noam, Director of the Columbia Institute for Tele-Information at the Columbia Business School, pointed out, “The Internet has become so essential for everything—political life, culture, communications, etc.—that maybe we should think of it as a public service.” Other participants responded that treating broadband as a form of essential infrastructure is entirely appropriate.

Different societies have chosen different models for providing four essential infrastructures—water, energy, transportation and communications, noted Pepper. “Transportation tends to be a government-provided good,” he said. “Energy is a blend with private sector investment and public utilities, such as municipally owned electric systems. Water is ‘free,’ but in many places local governments charge for water, so it’s not free even if it’s provided by government. And in the U.S., the private sector has provided traditional telecommunications and people pay for it.”

Indeed, many Americans regard the Internet as a public good. “Benjamin Franklin and the Congress in the early days of our country saw a need to subsidize the free press through the postal system in order to help it proliferate,” said Safiya Noble, a doctoral student at the University of Illinois at Urbana-Champaign and an Aspen Institute Guest Scholar. “I see the Internet as a common good that we all should be protecting because it promotes values that are important to our citizenry, such as the ability to access information for free.”

A key reason for keeping the design of the Internet open, flexible and transparent, said Aparna Sridhar, Policy Counsel for the citizens’ media organization Free Press, is to ensure that new sorts of not-yet-imagined technological, commercial and civic possibilities can emerge

**“The Internet has become so essential for everything—political life, culture, communications, etc.—that maybe we should think of it as a public service.”**

*Eli Noam*

in the future “because we can’t predict how things will move forward.” Sridhar believes that “we ought to design a system that maximizes public choice, innovation and profit while also encouraging civic engagement and other noneconomic benefits.”

The idea that the Internet infrastructure should be provided for “free,” in the manner of roads and bridges, struck some participants as wrong-headed. “Who’s going to pay for all the infrastructure costs?” asked Julia Johnson, President of Net Communications, a regulatory and public affairs firm. “Are we talking about taxpayers paying? If so, what kind of wealth redistribution will occur, and is it going to be a regressive structure?”

“Private capital is building the infrastructure,” said Catherine Bohigian, Vice President for Federal Affairs for Cablevision Systems Corporation. “It’s no different from private capital creating the content. If there is a consensus that Internet access needs to be free [no cost], then that has to be a completely separate conversation than the one we are having here, in terms of the values of the ecosystem.”

It is a business model question, said Dorothy Attwood, Senior Vice President for Public Policy and Chief Privacy Officer at AT&T Services. “In the business models [for network infrastructure], we want free and open. But of course, it’s not free [no cost]. The business model should promote greater development and innovation, but how do we get that innovation if the value created doesn’t follow the innovators?” Attwood believes that businesses must have the proper incentives to ensure that their business models align with “the values that we want to see grow on the Internet.”

### *The Topography of the Internet*

Thinking about the Internet’s institutional ecosystem as a series of “layers” is one way that policymakers have attempted to protect open, nondiscriminatory access to the network. There is the “physical layer” of hardware and transmission wires; the “logical layer” of software and transmission protocols; and the “content layer” of text, images and sounds. Each layer plays its own role in protecting or not protecting “openness,” and each layer is also connected to other layers.

“The layers model is both an abstract model and a way to protect the value of the Internet,” said Kevin Werbach, Associate Professor of Legal Studies and Business Ethics at the University of Pennsylvania Wharton School. “Part of the value is seeing the commonality—that similar things happen up and down the stacks. You can draw parallels between what’s going on in the content layer and all the way down to the physical layer.”

The value of talking about the different layers, said Werbach, is that it helps us “create the regulatory systems and meta-values so that the right values can emerge on the network. Our challenge is to try to come up with practical mechanisms that create a space so that the commons can emerge. That’s how commons happen. They don’t just happen because everyone forgets about their own selfish desires; they happen because there is an open space that everyone realizes, by accident, can work for them.” The layers model helps us look at “the enabling conditions at the different layers,” said Werbach.

Picking up on the “layers” analysis, Alan Davison, Google’s Director of Public Policy, Americas, warned, “We’ve conflated the issues surrounding access to the Internet with questions about *values* and the Internet.” There’s a difference between those two issues, he said. The ways in which the Internet itself operates are different from the ways that access to the Internet may be had.

Dorothy Attwood of AT&T proposed an alternative conceptualization of the Internet: “I prefer to think about the Internet as including roads, the community and stadiums,” she said. The road is not the infrastructure, but part of what we consider the community. And the community is a better framing than “the commons,” she said, “because it reflects the choices made by those who want to be part of the community; it isn’t an ‘everyone can come.’ The ‘stadiums’ are instances of commercial enterprises within the community, which might sell content, for example. The real question is, how much of the ‘stadium’ can you have without interfering with the notion that the community is available for all of us?”

**“... how much of the ‘stadium’ can you have without interfering with the notion that the community is available for all of us?”**

*Dorothy Attwood*

### *Four Significant Threats to the Internet as a Commons*

Managing the Internet to serve both public and cultural needs on the one hand and private, commercial interests on the other is one of the more significant challenges of our time. In approaching this task, Reed Hundt, former Chairman of the Federal Communications Commission and now a Principal with REH Advisors, believes that the Internet as a public medium is at an inflection point.

“If the god of technology is Shiva, then technology is both the creator and the destroyer. Technology has created a very large number of options—maybe even inevitabilities—that may pull apart the public nature of the public Internet,” warned Hundt. To explain, he recounted a brief history of the Internet:

From its inception, the Internet as a public medium consisted of borrowing the phone line and the personal computer, and connecting them to each other. That is to say, no firm created the technology of the Internet per se (excluding the backbone components). This cobbling together of pieces was done through the protocols released out of CERN<sup>1</sup> and utilized principally by the browser that Marc Andreessen and others helped us learn to use.

What was created was a park, or a commons. It was a free space, meaning that you could populate the space with things that you bought for some other purpose. For many years, it seemed that there wasn’t any way to do anything but create value and have it be shared. That is to say, there didn’t seem to be a way for anyone really to make money. This arrangement could not last, and it has not lasted.

Hundt identified the four significant threats to the Internet:

*First, the invention of new devices to access the Internet.* “It was inevitable that the personal computer would not always be the principal device for accessing the Internet, and that designers would design new devices

---

1 The European Organization for Nuclear Research, where Tim Berners-Lee was employed when he created the http protocol and the html language for the World Wide Web.

purposed for Internet communication,” said Hundt. Such devices have in fact proliferated, and none have become more captivating than those produced by Apple. “Apple has in fact created its own app world, which is a private world within the public Internet, or touching the public Internet. It is absolutely certain that many firms will imitate this particular approach to the public Internet, and that firms will create many, many private Internets in an attempt to serve customers better.”

*Second, Internet gatekeepers have new incentives to extract value from the Internet for themselves.* In the early days of the Internet, there were 5,000 Internet service providers and people used the telephone lines to connect to the Internet, at no additional cost. The consolidation of the Internet service providers (ISPs) over the past 15 years has changed the pricing structure for Internet access, however.

“In competition, firms tend to want to attract heavy users and charge them less per unit of consumption. But in consolidated markets, firms may want to charge heavy users as much as they will pay. And so, in consolidated markets, if a company has a heavy user, it wants to increase the price to him. That is what has happened in terms of the Internet’s gatekeepers: consolidation has produced the opportunity to charge different rates, and specifically, higher rates to heavy users. And yet heavy users, in some cases, appear to be the firms that are making the commons more valuable to everybody else. This paradox changes the evolutionary path of the Internet.”

The effect of this consolidation among business gatekeepers, said Hundt, is that the gatekeepers “now have the business incentive to *detract* from the value shared by everybody in the commons and take some of that value for themselves.”

“This is not an intrinsic evil,” Hundt noted. In fact, one of the key purposes of businesses is to create bottlenecks in the marketplace. “The purpose of competition is either to buy a bottleneck and hold it, or make one. Because a bottleneck is the same thing as a rent—an above-market return on profit. That’s what people do in competition. So it was inevitable that it would come to pass that we would have firms trying to create bottlenecks in the Internet.”

*Third, the aggregation of information in the cloud amounts to a private capture of the commons.* Hundt noted that digital technologies have responded to the complexity of the Internet by finding ways to make

information more centralized and efficient in operation. “This isn’t a bad thing, either,” said Hundt. “But if virtually all the data of the world becomes aggregated, not in the commons itself, but in specific geographical and physical locations owned by private parties—loosely called ‘the cloud,’ but in reality multiple data centers—you now have private parties exercising a form of control over information that didn’t exist in the early days of the Internet commons.”

*Fourth, governments are doing more to destroy the public Internet, not necessarily with bad motives.* In the beginning, the Internet did not pay attention to national boundaries, said Hundt. Unlike broadcasting and telephony, where governments could easily regulate access and use of the communications, the Internet was born wide open: “Internet standards were standard from the beginning, price was not a barrier to use, and governments for years did not seem to have any way to establish national boundaries or, in other words, to establish their own identity. Over the years, the Internet as a commons has gotten closer to fulfilling its fundamental disruptive tendencies to ‘dis-establishing’ establishments.”

But governments are now starting to fight back and attempt to assert control over the Internet as a commons, particularly in certain authoritarian countries, said Hundt. The good news for Americans, he said, is that our country was founded on an idea of “negative liberties”—that is, the idea that citizens are able to say what the government may not do. So the Internet is now posing a fundamental challenge to governments: “Is it a space where we want to establish ‘negative liberties,’ or is it a space where government should exercise some sort of control for the good of itself and/or the society that it governs?”

In identifying these threats to the Internet, Hundt conceded, “I want you to be alarmed. That has been my intent.” A critical element of the Internet’s success in its early days, he said, was “a common understanding about the values animating it. If we could just re-state that common understanding, and then define the obstacles to the reification of those values, then we would be able to do the right thing for the next generation.”

### *Varieties of Enclosure of the Internet Commons*

Picking up on Hundt’s description of the Internet as a commons, Michael Tyler, Founder and Managing Director of Tyler & Company



in London, pointed to a number of “enclosures happening on the Internet.” By “enclosure,” Tyler referred to the historical experience of shared, open fields—that is, “commons”—in Great Britain that were privatized and converted to market use in both medieval times and increasingly in the 18th and 19th centuries. “Enclosures were not without economic advantages,” Tyler conceded. “But they also caused enormous social distress and exclusion.”

As for Internet enclosures, Tyler pointed to the creation of “tiers of service” that may create economic value but also result in social exclusion. When national sporting events are “taken private” by premium TV networks that require premium payments, he said, “a critical, shared part of the national culture is enclosed.” Although rules against enclosure of the fixed-wire Internet may emerge, said Tyler, “the trend is for law and practice to treat enclosures of wireless access as permissible.” Tyler also pointed to the proprietary models of technology and service pioneered by Apple, which has often bypassed the open architecture of the Internet, as in the iPhone App Store, the iPod and iTunes.

There are also instances of *government* enclosure of the Internet, said Tyler, pointing to the ways in which the government of China has limited access to Google and thousands of websites.

David Bollier, the rapporteur for the conference and a long-time scholar of the commons, pointed out that “enclosure often has great productivity benefits for individual companies, but it also has certain consequences for social equity. It privileges the value proposition of the private capture of information rather than the value proposition of access and sharing among the people using the commons.”

Bollier also noted that the purpose of enclosure is to displace certain “externalities”—or costs that lie beyond the strict market transaction—onto the ecosystem. And so if one is to sanction enclosures, he said, “let’s be frank about the value proposition of the commons that is being suppressed, repressed or diminished.” He added that there is a critical difference between monetizing value from the commons and enclosure. “Capturing value doesn’t necessarily undermine the integrity of the commons and its socially created value. But enclosure is something different because it intrudes upon the basic value proposition of the commons.”

Michael Gallagher, President and CEO of the Entertainment Software Association, took issue with the negative implications of enclosure:

“When we look at broadband connections, the capability of devices and their declining prices, the additional spectrum that’s been made available, the lower barriers to entry, the anytime/anywhere ability to communicate, the applications—these are the fruits of enclosure, to use the nomenclature that we’ve adopted here. They have happened because of companies like Microsoft, Cisco, Intel, Google and Apple. There are new companies that are formed, such as Facebook and Zynga today. The ecosystem is indeed strong. So I would posit this as a much more optimistic assessment, and say, ‘How do we continue this?’”

**... the Internet is  
both a public good  
and a private good....**

*Blair Levin*

Blair Levin, the former Executive Director of the Omnibus Broadband Initiative at the FCC and now a Fellow with the Aspen Institute Communications and Society Program, offered that the real challenge is “to figure out what it is that government should make sure everyone

can have access to. That is probably the single most important thing to decide in terms of universal service because the Internet does present a new opportunity.”

It is difficult to answer this question, Levin pointed out, because the Internet is both a public good and a private good, and it is not self-evident “what framework should guide us in saying that government has a right to do *x* or *y*.” If every citizen does not have a right to access high-value content on the Internet, what bundle of rights *should* belong to every citizen or Internet user?

The traditional answer to this question is “universal service,” said Levin, agreeing that that is very important. But he argued that the current policy framework is premised on the belief that the single most important metric for evaluating a national broadband policy is “the wireline speeds to the last 10 percent of the population served.” Levin argued we should look at other metrics such as “the line speed to research institutions because that will drive a lot of economic activity.”

Ben Scott, Policy Advisor for Innovation in the Office of the Secretary of State, worries about the ways in which governments may exploit commercial enclosures of open networks. “Enclosure creates control points on the Internet that can be exploited by either companies or governments,” he said. “And the problem is that the economic

benefits to companies to exploit these enclosures don't come without providing the same tools to governments."

Scott pointed to the four threats to the Internet identified by Reed Hundt, noting that the enclosures of Internet-access devices, Internet service providers and personal data in the cloud, each give governments new opportunities to gain access to personal information about citizens. Scott described a scenario in which a government might want to intercept information from a citizen's BlackBerry. It could go first to the network operator to try to obtain the data, and then to the device maker, and then to the company running the enterprise server hosting the data.

The threat of government interception of data at any one point may induce citizens and investors to shift their use of technologies, or move them to a different country or a different context, in order to evade government snooping, Scott warned. "My point is to note the interdependence and interconnectivity of the network," said Scott. "The threats that Reed [Hundt] has identified are very, very real, and they are very, very difficult to unravel because enclosure in one area has ripple effects. There is no law and no enforcement power that can draw a line between one technology and another. And so as a country, I think we have to identify what our general policy is going to be about this kind of activity."

"I fail to understand why you're putting together economic enclosure and government enclosure," said Anna-Marie Kovacs of Regulatory Source Associates, who believes that both businesses and government can interfere with the openness of the Internet, but that "they're not necessarily connected." Kovacs added that technological trends cannot simply be reversed: "We are not going to be able to go back to an Internet that is purely 'free flow.'"

Scott replied: "The point I'm trying to make is that economic enclosures create the control points that governments exploit. The creation of these control points validates the threat that Reed [Hundt] is identifying—that we have a real problem that we need to deal with in some way."

Hundt agreed: "If there are choke points that marketplace competition and innovation are producing, then it is a reality that people will try to put their hands around them and use them. What Ben [Scott] and Jackie [Ruff, Vice President International Public Policy and Regulatory Affairs at Verizon Communications] are saying is that government—certainly in some countries that we can name, and potentially any-

where—will want to put its hands around those chokepoints. That means that government action may, in fact, challenge the concept of negative liberties in the commons. I don't have any doubt about this."

Chokepoints will actually become stronger and stronger, not weaker and weaker, Hundt said. And the reason is that the scale of investment required to maintain them—given the scale of information on the Internet—is always growing greater and greater. "It's possible to imagine markets in which there can be disruptive outsiders and entrepreneurs that can create bypasses around chokepoints. As a country, our economic policies usually try to do exactly that. But that's not the way of the world. And it's not clear that we are fully committed as a country to that particular approach—although we are in a hot debate about it."

Hundt conceded that competition, innovation and profit motive do indeed cause a "continual upgrading" of the features of the Internet, as suggested by Dorothy Attwood's account of the Internet as "roads, communities and stadiums." But for Hundt, "the question is whether there is encroachment on the Internet commons. If we tolerate that encroachment, we are privileging certain values over others. We're privileging making money over sharing information—which is why this group ought to try to be precise about the values that we think the commons ought to reify."

The Conference then proceeded to devise an answer to some of these vexing problems.

### **Digital Embassies for Data**

For years, the nation-state has been troubled by the ascendant Internet and its disregard of national borders. The free flow of data has encroached upon one of the traditional rights of national governments, the control of electronic communications within their borders. To the nation-state, unconstrained information flows and storage can prove disruptive. To individuals and corporations, uncertainties about the legal status of data and communications can be an impediment to commerce and a threat to personal privacy and sensitive commercial information. Laws governing information vary from one nation to another, and it is not necessarily clear which nation's laws apply to a given body of information or data transmissions.

A spirited discussion at the conference focused on this issue—and in particular, on a proposal to establish a new regime of “digital embassies” for data through an international treaty. The idea is to establish predictable, enforceable rules for establishing national jurisdiction over digital information. The innovative scheme proposed by the working group headed by Robert Atkinson of the Information Technology and Innovation Foundation, could help reconcile the workings of the global Internet with the prerogatives of national sovereignty.

### *National Sovereignty and the Internet*

“We used to have this notion of the global Internet,” said Robert Pepper, Vice President for Global Technology Policy at Cisco Systems. “We would talk about how the Internet violates sovereignty, and isn’t that a good thing?—and that countries would not be able to control it. Well, guess what? Wrong! Countries *are* controlling it for a variety of good and bad reasons. Sovereignty still exists. It hasn’t disappeared.”

In regulating Internet content, national governments are sometimes acting upon a widely shared or politically powerful sentiment within their countries. For example, Italy has banned the websites of foreign gambling entities and the United States prohibits online gambling with the effect of protecting gambling enterprises such as those in Las Vegas and Atlantic City.

For Pepper, the more serious concern is the fragmentation of the global Internet into “subnets.” In many instances, governments have been trying to leverage their influence with international organizations, such as the International Telecommunication Union and the Internet Governance Forum, and at meetings, such as the World Summit on the Information Society, to try to “break the global Internet,” said Pepper. Their intent is to domesticate and neuter the Internet as an open platform through international regulation, he suggested.

Robert Atkinson, Founder and President of the Information Technology and Innovation Foundation, a technology policy think tank based in Washington, D.C., is not distressed by the principle that governments can censor or limit what might appear on the Internet within their borders. He cited, for example, the case of the King Bhumibhol Adulyadej of Thailand, who censored a Wikipedia article on him in October 2008, and Germany, which bans displays of Nazi paraphernalia.

“We have to accept, at some level, the notion that countries are sovereign,” said Atkinson. “They do what they do. Within some bounds, countries have a right to control what goes on within their borders. That doesn’t mean that we just have to sit back and accept it,” he added. “We should press countries to be more open and incentivize them to be more open. But I really think it’s both naïve and wrong to say that our values are superior and every country should have our values.”

**“Free expression isn’t an American value... it’s an international value, guaranteed in the international human rights system.”**

*Andrew Puddephatt*

Andrew Puddephatt, Director of Global Partners and Associates, an organization that promotes good governance, democracy and human rights, took issue with Atkinson’s remarks: “Free expression isn’t an American value,” he said. “It’s an international value, guaranteed in the international human rights system. Most countries don’t have a First Amendment; that’s very American and exceptional. But

most countries and many citizens within those countries do want the international standards created in 1948 by an international committee of experts from across different cultures, religions and backgrounds, to be upheld in their own country.”<sup>2</sup>

“As governments begin to challenge the way that the Internet is governed, it’s very, very important that governments have a more explicit pro-democracy, pro-transparency, pro-free expression stance in those debates,” Puddephatt said. “U.S. silence is often interpreted as a defense of U.S. commercial interests. I think it’s very important to challenge that conception, and to say something more positive about free expression.”

### *Digital Embassies and the Free Flow of Commercial Data*

The clash between Internet communications and national sovereignty takes many forms; one that received considerable attention in the conference was the ways in which national sovereignty is introducing obstructions and inefficiencies in the free flow of commercial data

---

2 The Universal Declaration of Human Rights.

stored on remote data sites—“the cloud.” Some conference participants sought to address this issue through an imaginative proposal to establish an international regime of “digital embassies.”

“An embassy is basically American soil in another country,” said Atkinson. “Foreign governments don’t have access to what goes on there. We’re proposing something similar for data, so that when you store data on the Microsoft server, and it ends up storing the data in another country, it would be subject only to U.S. law and not to anybody else’s law. Data tagged by a seal of its ‘nationality’ and stored in ‘virtual embassies’ would essentially solve the conflict of jurisdiction problem,” he said.

A conference working group compared the problems affecting data flows to the distortions that international tax regimes impose on the free flow of investments and profits. For example, a company may build a factory in Germany, financed by a subsidiary in Luxembourg, and then shuffle its profits and interest payments using various accounting maneuvers in order to avoid high taxes and maximize profits. Now, as data flows become more international and significant in size, the inefficiencies and restrictions in national laws for privacy, data security and general business operations are distorting the markets for data services and storage.

It is important to “see data as manufacturing,” said Hundt. “That is to say, data services are a kind of value-added commerce. Companies apply algorithms on data to increase its value, for example, or they build platforms that enable data to proliferate (e.g., Facebook) and thus increase in value.” The point, Hundt said, is that this sort of value-added commerce should be encouraged through free trade, and that the Western rule of law gives Western companies a fundamental advantage in this commerce.

Too often, however, Western companies encounter countries such as China that stipulate strict terms for gaining access to their markets. Hundt sees the digital embassy regime as a way for multinational companies to push back: “It allows an American company to say, ‘Well, you know, our country is following the digital embassy regime, and so when we send data to China, we need to house it in the virtual equivalent of U.S. property.’”

Instead of trying to establish a privacy and security regime for the cloud—which would then have to be harmonized through international law (an impossible task)—Working Group III proposed a new type of governance system for data that would honor individual ownership of data no matter where in the world it is stored. “It should not make any difference conceptually or legally whether my data is on my server in my basement or in a server that I’m renting anywhere in the world,” said Robert Atkinson, Founder and President of the Information Technology and Innovation Foundation.

Atkinson explained the policy choices: “We can just say that no data-sharing is possible whatsoever because there is just too much international conflict over the issue, and the odds of us getting to a global regime of total harmonization is zero. Or two, we could say that we are going to allow data-sharing but that individual companies will always be in conflict over how it should be legally managed. Or three, we could accept our proposal of ‘digital embassies’ as a way to solve the problem of conflict of jurisdiction.”

Hundt noted that the digital embassy regime would be a boon to companies that are vulnerable to commercial theft. “No American software company can be comfortable putting their data, their algorithms, anywhere in the world and feel confident that American rule of law protects them,” said Hundt. “What we’re trying to create is the ability of an American firm to take data and put it in Country X with the assurance that American rule of law would apply. If a bad actor in the commercial sector goes on that property, that bad actor would be subject to American jurisdiction and could be sued civilly or criminally prosecuted—because that’s the effect of going on American property.” This would apply, as well, for other countries.

Atkinson offered an illustrative scenario: “I have this data and need to store it somewhere. I decide to store it on a site that has a U.S. flag attached to it. That will assure me that no matter where I store the data around the world, only the U.S. will have access to the data if it has the U.S. digital embassy seal on it, and it is stored in countries that respect that legal regime.”

“The basic principle,” said Atkinson, “is that your data is yours, regardless of where it is physically stored.” The proposal also aspires to affirm the principle that a user would not have less legal protection when data is stored in the cloud than when it is stored on a hard drive.



That said, legal rules for intercepting data would apply when there is a criminal investigation.

Just because there is a digital embassy system would not mean that an American citizen's data would automatically be covered by American law. An American might voluntarily and knowingly store his data on a French server and elect to be covered by French laws for data access and protection rather than American laws. This option would of course require that there be sufficient disclosure about what national body of law would govern a given set of data.

Atkinson also pointed out, "We don't want to set up a regime in which you could store your documents on the servers of some Caribbean nation that decides they will get into the business of totally secure cloud hosting that will be inaccessible to any government. We should not have 'digital Swiss banks.'" A Mafioso might be able to "export" data to an offshore server under the new rules—and thereby be less accessible to U.S. law enforcement—but that does not change anything from the current situation.

Atkinson offered a scenario of a U.S. citizen using T-Mobile, a German company with an American subsidiary that sends its data to Germany: "So who has access? What law is applied? We assume that Germany is a signatory to the digital embassy agreement, as the U.S. would be. That means the German government would not have access to any of the data from the American subsidiary, even though the data is managed by a German company and stored in Germany. However, the U.S. government would have access to it—and if they wanted access to the data through normal legal channels, they would go directly to T-Mobile."

Another scenario: an American individual user buys a book from Amazon Germany. In this case, if intelligence agencies wanted to know what book was bought on the site, the digital embassy regime would *not* apply. But through a reciprocal Mutual Legal Assistance Treaty-type agreement, the U.S. government could go to the German government and say, "You tell Amazon Germany to give us this data."

But when some participants proposed complicated scenarios in which users might store their data on servers in Zimbabwe that were owned by an American company, it was not immediately clear if the user's citizenship or the corporate domicile would dictate the legal

jurisdiction for the data. “We need to think more deeply about these issues,” conceded Kevin Werbach of the Wharton School.

Other uncertainties were raised: would software applications be considered “data” subject to digital embassy rules? Would derivative types of data be classified according to the users’ nationality and thus be governed by that legal jurisdiction?

### *The Challenge of International Implementation*

How could the “digital embassy” scheme be enacted?

Kevin Werbach reported a summary from the third working group which suggested a number of possibilities. First, the Organization for Economic Cooperation and Development (OECD) could find a nucleus of nations that could multilaterally agree to a compact; this beginning could then attract more signatories. OECD could also help develop some technical mechanisms and requirements for the system to work, something that may become easier as individual use of digital signatures and tagging mechanisms for data become more routine.

Another idea is to develop a basic treaty framework that would allow for a multiplicity of implementations because countries have many different views about how to protect privacy and security. Rather than seek an elaborate and rigid set of rules, the treaty could set forth “a core compact about principles” that could be applied in a variety of different ways.

If countries decline to sign the treaty or if they do not comply with its terms, the U.S. State Department could set up a blacklist similar to terrorism watch-lists. The purpose would be to prevent U.S. data from going abroad to countries that are not trustworthy—or at least notify users of the ramifications. Provisions would also have to be made for the Mutual Legal Assistance Treaty, or MLAT, under which countries cooperate to enforce criminal and civil laws. “When foreign law enforcement wants to obtain data from a U.S. service provider, there would be a process for doing so. It’s cumbersome and messy, and it needs to be cleaned up, but it would apply here,” said Werbach.

Another way of moving forward would be to develop a model law or set of rules that would specify how the system would work in different areas such as data security, privacy and transparency. “We figured that

smaller nations might simply sign up for this mechanism, as opposed to figuring out all the specifics themselves, and gradually legal regimes would converge,” said Werbach.

In addition to a treaty, OECD initiative or model law, the digital embassy regime might be pursued by trying to promote international norms. International bodies that might help do this include Asian-Pacific Economic Cooperation (APEC), the International Telecommunication Union (ITU) and the Free Trade Agreements (FTAs).

However the idea is advanced, the digital embassies regime would require a number of new legal and technical systems. Law enforcement agencies would need specific guidance and rules for how to go to court to secure lawful access to data. Similarly, rules governing the privacy of data—and mandatory disclosures of any breaches or losses of data—would need to be established and harmonized. A primary goal would be to foster user trust in the system. Transparency is important to the functioning of the system for the same reason. It would enhance consumer trust and give cloud providers the incentive to assure rigorous data protection.

Companies that meet four basic criteria would be eligible for a “digital embassy seal” certifying their compliance with minimally acceptable principles of data protection. A company could obtain a seal only if (1) it agreed not to store data in countries that had not ratified the digital embassy regime; (2) it establishes adequate security measures, as defined by the seal program; (3) it encrypts the data it holds; and (4) it reports all violations to the digital seal program, which would make the reports publicly available.

The disclosure of violations would resemble the current system in which Google reports instances in which countries force them to violate the rules. “If there is a rule and mandatory disclosure,” explained Atkinson, “then countries cannot play individual companies off against one another. Everyone can say, truthfully, ‘We had no excuse [but to disclose a violation]. We have to do this, so you [a national government] have to live with it.’”

“The digital embassies proposal is not a utopian scheme where backdoor access to data would never be allowed,” Atkinson cautioned. The “front door” is when national governments or law enforcement agencies provide a legal piece of paper to obtain access to data; the “back

door” is when a national government or a rogue actor obtains illicit, secret access to the data without disclosing it to anyone. “The ‘front door’ is what the U.S. Department of Justice generally uses, while the C.I.A. is more likely to use the ‘back door,’” said Atkinson. It bears noting that backdoor access could occur on an American server on U.S. soil by a foreign government, e.g., if China hired a rogue hacker to get access to an Amazon server.

Michael Tyler of Tyler & Company predicted great political resistance to a treaty of this sort. “The term ‘digital embassy’ would immediately trigger a set of—shall we say—‘allergic reactions’ among nations who would object to a further erosion of their own jurisdiction in their own territory, by the exercise of new privileges and immunities by foreign entities,” Tyler said.

“If the proposal were cast as an American-led initiative to extend the existing regime of privileges and immunities to corporate interests, particularly American ones, it would be dead in the water from Day One,” he said. Foreign resistance to the idea could be especially acute, agreed Andrew Puddephatt of Global Partners and Associates, “given the violations of national sovereignty that the U.S. government has committed over the past period of time.”

The digital embassies idea would garner support only if it could be seen as “legitimate, genuinely reciprocal and serving the public interest,” said Tyler. One way to do this would be to attempt to secure an initially bilateral arrangement between EU countries and the U.S. that would be seen as highly reciprocal. Robert Atkinson considers this quite realistic because “any rational European would see this as a real benefit to Europe because it protects European data from the prying eyes of the U.S. government.”

Curiously, said Richard Green, Board Member of Liberty Global, “The most difficult country to sell this idea to is the United States because we have some very strong data-intercept issues.” Having said that, Green added, “This is a very powerful concept because it really enables cloud computing. If you don’t do something like this, we’ll be caught in a hodgepodge of rules and regulations and impossible barriers. This is at least one way of addressing it.”

## The Future of Broadband

The future evolution of the Internet—and the benefits that may or may not result will depend a great deal on future investment in and regulation of broadband. Accordingly, the rest of the conference looked at these issues as well as future competition policies, universal access programs and protections for privacy and personal data. To try to set the stage for these discussions, the conference focused on the lessons that might be learned from international broadband regulation and from current investment trends in broadband.

### *The International Broadband Experience*

Michael Tyler, telecom consultant, offered some perspective on how American broadband policy might evolve by reviewing the state of broadband deployment and broadband policies in various countries around the world. He identified “four pillars” that he believes should be present in fair, effective broadband policies:

1. Universal access to broadband, particularly by households, schools, libraries and businesses
2. Robust competition in the marketplace
3. “Equitable use”—a term that Tyler used because it is a broader, more comprehensive category than “net neutrality”
4. “Good order”—a term that includes basic policies against consumer fraud, child pornography, identity theft and other basic protections.

For Tyler, a key metric in assessing broadband policies is the percentage of households that actually have access—or “take-up.” Tyler said this number is much more meaningful than the commonly quoted but poorly conceived measure called broadband “penetration,” which simply takes the population of a country and divides it by the number of broadband connections.

According to statistics compiled by Strategy Analytics of Boston and cited by Tyler, the most important finding “is that the time when the Internet was really all about the United States, and other countries were

trying to catch up, is over in much of the world.” Apart from a few very high take-up countries like Korea (95 percent) and Norway (83 percent), “many countries are increasingly in roughly the same bracket as the U.S. (66 percent according to a recent Pew Foundation study), others are not quite in that bracket yet but have nevertheless caught up spectacularly in the last few years.” France and Germany had 68 percent and 58 percent take-up, respectively, in 2008, and the United Kingdom had 63 percent in 2009.

Two key messages that emerge from the data, said Tyler, is that “broadband is a worldwide phenomenon, and reaching the last, hard-to-reach segments of the population is a serious challenge, even in relatively compact countries like the United Kingdom.” There is also consensus that access to broadband is not wide enough and that speeds need to increase. Some countries, such as Finland and Germany, have defied the advice of economists and set specific dates for ambitious increases in the speed and take-up of broadband.

How should government policymakers respond to these issues? The traditional view is that the market should be left to sort things out over time. But a number of countries, impatient at the slow pace of broadband take-up, have initiated public/private partnerships to construct broadband or make it more affordable. Singapore and South Korea have had such programs all along, but Australia and New Zealand have recently moved toward similar models. The U.K., which once considered a surcharge on telephone bills to pay for a universal service fund to expand broadband access, is the main exception: it has actually retreated from such plans and now (at least for the present) looks to a market solution with little or no government intervention.

Competition policy is also seen as a way to spur greater broadband deployment and access. Here, the question is whether government needs to intervene to make the market more competitive or not. This issue is debated, of course, but there is a general concession that even where there is competition, it will be an oligopolistic situation, with two or perhaps three competitors such as cable broadband, telephone-wire DSL and wireless.

Many observers argue that a “tri-opoly,” where it exists, is good enough, Tyler reported. But for those jurisdictions that want more, one option is mandatory, regulated resale forcing the incumbent operators

to resell unbundled, wholesale, local-access broadband capacity to rival service providers, including entrepreneurs.

As for achieving “equitable use” as a policy, Tyler said that the key issue is the market power of broadband operators, who sit in-between Internet users on the one side and application and content providers on the other. A key question for Tyler is whether broadband operators are able to assert market power to the detriment of consumers or application and content providers.

“The prevailing view,” said Tyler, is that we should at least be worried about this issue, which is why many people are worried about net neutrality. “Is there illegitimate discrimination and legitimate discrimination in data transmission?” asked Tyler. “Is all discrimination among packets illegitimate; or only some particular kinds of discrimination?”

Tyler noted that in most markets, market segmentation by price is a normal phenomenon: “Nobody particularly objects to business-class seats on airplanes. Why shouldn’t that exist on the Internet?”

Others countered that if some forms of discrimination among data and differential pricing are allowed on a system that is a limited local resource, there is a corresponding need for minimal requirements for quality of service to those unable or unwilling to purchase the premium service.

Yet market power is not without its virtues, noted Eli Noam, Director of the Columbia Institute for Tele-Information: “In some ways, the oligopoly model has actually worked reasonably well. The problem is the monopoly model, which tends to be slower and anti-competitive. On the other hand, a truly competitive environment, which is the most desirable one, of course, leads to all sorts of instabilities, ups-and-downs and collapses, as happened in the late 1990s. The oligopoly model, while second best, gives companies some space for profitability that makes investment possible ahead of demand. It’s all a tradeoff.”

Noam’s comments were echoed by Robert Atkinson of the Information Technology and Innovation Foundation. “The ‘fourth

**“Nobody particularly objects to business-class seats on airplanes. Why shouldn’t that exist on the Internet?”**

*Michael Tyler*

pillar’ [of broadband regulation] should be network innovation on the Internet,” he said. “And then the question is, how do we get there? The problem with competition is that it implies that two is good, three

**“If you have too little competition in markets, you don’t get enough innovation; if you have too much competition, you don’t get innovation.”**

*Robert Atkinson*

is better and four is better than that. I don’t think that’s the case. If you have too little competition in markets, you don’t get enough innovation; if you have too much competition, you don’t get innovation. The whole Schumpeterian model of innovation is that innovation produces profits that then support further innovation. If you have no profits, you can’t innovate.”

It is true that certain geographic regions and sectors of the economy tend to be subject to natural monopolies, said Reed Hundt, former FCC Chairman and Principal of REH Advisors. Citing his consulting work for the Australian broadband plan, he said that remote rural areas are generally subject to natural monopolies for fiber, while more concentrated urban areas can support vigorous competition.

That said, Hundt pointed out that government often plays a critical role in prodding investment and innovation—and indeed, in deciding what is a natural monopoly and what investments need to be subsidized. He noted that when Telstra in Australia resisted investment in fiber lines, the government threatened to nationalize it, which in turn “brought Telstra to the bargaining table” because “it might be better to have a commercial deal than to be expropriated.” Similarly, the Korean government prodded (and subsidized) SK Telecom to build out fiber lines.

Robert Pepper of Cisco Systems believes that there is a “continuum of public/private partnerships” that are possible in building out broadband service. He advised, “The first line of policy should be to leave it to the market and see how well that works. Then do a ‘gap analysis’ [assessing the extent of broadband availability and take-up], and then determine whether or not broadband investment is on track and how fast it is moving.”



Pepper noted that “government has a lot of levers and dials” that can be used to promote broadband build-out and adoption. There are government subsidies, tax credits, the Universal Service Fund, support from municipal, provincial and regional governments, and spectrum policy. In Mexico, the government auctioned off use of national electric utility fiber in order to promote competitive broadband service in rural, unserved parts of the country—an exemplary and creative public/private partnership, Pepper said.

Building out a broadband system is one thing; expanding consumer adoption of it is often another. Conference participants cited a variety of factors that may impede the take-up of broadband: behavioral obstacles, such as unfamiliarity with computers and the Internet, and cultural factors. In the U.S., Hispanics as a group are under-adopters of wired broadband service, noted Blair Levin. In Korea, the government has aggressively pushed digital literacy and training and facilitated school children’s access to computers and “very high-speed Internet” service.

One lesson that can be drawn from diverse national experiences with broadband is that each country has its own specific technological, political and cultural history. Certain policies that work in one country may or may not be transferable to other countries.

Market structure can be a pivotal factor, however, said Kevin Werbach of the Wharton School. In that regard, he believes that the United States could follow two different paths: (1) the “messy oligopoly model,” in which there is some “inter-modal but limited competition;” and (2) a “shared-access model,” in which broadband providers are required to offer nondiscriminatory access to its lines to competitors. The interesting question is not whether we should switch from one model to another, said Werbach, but “what’s the difference in performance between the two models?” We do not really know the answer.

A duopoly broadband model seems likely for wireline, said Reed Hundt: “From the early 1990s until a few years ago, we all indulged the belief that we would have a cable and telco alternative, house-by-house. There was the sense that it wasn’t quite there, but it would happen. Now I don’t see that trend happening over the next 10 years. If people want a high-speed fixed line at a really good price, most houses are going to get that offer from cable or telco.”

Blair Levin, former Executive Director of the Omnibus Broadband Initiative at the FCC and now Fellow at the Aspen Institute Communications and Society Program, pointed out a change in the current market structure: “For the first time since the Internet became a mass medium, there will be a huge asymmetry between one broadband provider and another in approximately 70 percent of our homes by the year 2015. What we don’t know is whether that will matter.”

Levin added that we also do not know what competitive impact 4G wireless transmission will have. Will wireless computing compete with fixed-line broadband, and how rapidly might that proceed? Will ISPs compete on the basis of broadband speed? Levin noted, “It’s perilous to lock-in a broadband policy framework in those parts of the broadband ecosystem where you really don’t know what is going to happen.”

### *Investment Trends in Broadband*

Even in the absence of a clear broadband policy framework, investors are making choices. What do those trends suggest?

Reed Hundt finds it doubtful that alternative fiber paths to the home will materialize: “It looks like we are getting to a point of having dominant fixed-line providers,” he said. “However, my sense is that great companies like AT&T and Verizon are putting their investment money primarily into wireless, and so we’ll actually get a slow separation [in the market]. And so the ‘convenient duopoly’ of cable and telephone companies—convenient because it spared us dealing with certain regulatory issues—is not necessarily static,” said Hundt. “And why would it be? There are many reasons why these two huge companies [AT&T and Verizon] would go towards wireless when their cable rivals don’t have a wireless business.”

Hundt sees little interest, at least before the stimulus program, in long-term investments in broadband, and blames public policy for this outcome: “We have not seen much business enthusiasm for investment. That’s not because they’re bad; it’s because they don’t know what to do. But it is a bad thing for our country that our communications companies haven’t been able to decide that there’s something really important to invest in. They are sitting on cash; their price/earnings ratios are preternaturally low. To some degree, the world of policy is the culprit”—by which Hundt means that policy decisions need to appear to “have

enough future to them that they would empower companies to make big bets. Say what you will about the 1990s—people made big bets.”

Then as now, policy will have a critical influence on future investment in broadband. As Catherine Bohigian, Vice President, Federal Affairs, for Cablevision Systems Corporation, noted, “If cable is going to have a monopoly, and government’s answer is regulation, then why would cable put more money into its infrastructure?” Bohigian also pointed out that it is not yet clear if consumers truly want faster broadband speeds, and so cable operators have not rapidly adopted DOCSIS 3.0, a technical standard that enables high-speed Internet access via an existing cable system.

There are other knotty, unresolved policy issues that make it less attractive to invest in broadband, said Michael Gallagher of the Entertainment Software Association. These issues include cyber-security, intellectual property protection, privacy, national security powers, law enforcement and child pornography. “Investment will come when you uncork these things,” he said.

But it is also possible that investment in network infrastructure is lagging because the more significant returns will come from applications and middleware, not broadband. A number of conference participants concurred that new investment will hinge more upon new applications and uses of the network than on the appeal of DOCSIS 3.0 or other network infrastructure issues.

Dorothy Attwood, Senior Vice President, Public Policy and Chief Privacy Officer at AT&T Services, took issue with Hundt’s analysis, however: “There is a huge amount of interest in creating the capabilities that integrate wired and wireless. AT&T is still heavily investing in wired plans. Everybody has different models, however, and the nut that’s never been cracked is the hard-to-reach distance/density issues in certain areas. But if you’re talking about markets where cable is, it’s dead-on heavy investment and it remains that way.... The future, and certainly the growth potential, are in an integrated product. You don’t invest in one or the other; you invest in a platform.”

Hundt replied that “AT&T is spending proportionately much more in wireless” and Blair Levin added: “The level of depreciation in AT&T’s fixed-wire plan is greater than the level of investment. In plain English, that means that AT&T is disinvesting in its fixed plan. Now,

I'm not really criticizing it; I'm just saying that it's very different than what is happening on the wireless side."

The issue for some people is whether wireless and fixed-wire broadband are separate platforms or a new, integrated platform. Hundt said that it is unclear whether wireless will provide a competitive alternative to wire-based broadband. Purely from a technical standpoint, Professor Dale Hatfield is doubtful: "Using back-of-the-envelope analyses, the additional 500 megahertz of spectrum [from wireless] is not going to cut it. If we're really going to have a vibrant wireless network, we have to have a really fiber-rich network. The fiber has to be deep enough to provide a reasonable amount of frequency and speeds."

"The end game," said Kevin Kahn, Senior Fellow and Director, Communications Architecture for Intel Labs, "is cells of extremely small size that start to look an awful lot like fiber-to-curb, where there's a cell at every curb. It sort of begins to look a lot like Wi-Fi. It's not Wi-Fi, I understand, but it's as if there were a Wi-Fi transmitter at your mailbox as the source of everything that you get in your house."

Robert Pepper agreed with these assessments: "There is no such thing as a wireless network. It's wireless access to a fiber network." Pepper said that the "architectural importance of fiber" will grow as wireless grows, driven in part by the desire to move data from the radio waves into the network as quickly as possible so that the network can more easily scale.

The ultimate challenge, said David Don, Senior Director, Public Policy for Comcast Corporation, is "how to incentivize the next-generation build-out of broadband?" In Europe, this question is being addressed right now where many of the regulatory requirements are not being extended to next generation networks. In the United States, he noted, it is unlikely that government subsidies will be sufficient.

### *Jurisdiction, Universality and Competition*

How should broadband regulation be structured in the future? A conference working group headed by Blair Levin wrestled with this question. It tackled three key issues: what is the appropriate scope of the FCC's regulatory jurisdiction over broadband? How should the government spur competition and innovation? And how should the FCC help provide near-universal access to broadband? (An important

disclaimer: Although FCC Commissioner Mignon L. Clyburn attended this working group, nothing in the group's report should be construed as representing her point of view.)

***Jurisdiction.*** A case can be made that broadband technology is so different from existing telecommunications systems that a new statutory title for regulating broadband should be added to the Communications Act, which in turn would grant the FCC new types of authority in guiding the evolution of broadband. However, the conference demurred. "Our position was that we are not there yet," said Blair Levin, moderator of the working group that looked closely at the issue. "The market is still developing and a new statutory title would probably be too comprehensive an approach." He added, "We also couldn't figure out a way to do it."

So rather than establish a new Title 7 to the Communications Act, participants recommended that existing titles be amended as necessary and that concurrent jurisdiction with other federal agencies continue. In considering actions to increase regulatory jurisdiction or authority, the group urged that the international implications of broadband policies be considered. The point is to avoid the adoption of frameworks or rules that would encourage countries to impose harmful constraints on Internet-based services and applications.

The working group offered another jurisdiction-related proposal: to expand the role of the Broadband Internet Tech Advisory Group, or BITAG, led by Dale Hatfield, Executive Director of the Silicon Flatirons Center at the University of Colorado at Boulder. Conference participants supported BITAG as a way to "consider all technical issues related to the health of the broadband ecosystem." This would include annual reports to the FCC on potential threats, a complaint process with appeals to the FCC, and a BITAG-appointed—and funded—ombudsman to assist with private complaints.

Hatfield warned, however, that BITAG "is not dispute resolution in a traditional sense" because it consists of "engineers coming together for a common purpose and wanting to do the right thing. We're not the normative group to decide whether an unintended consequence ought to result in some sort of regulatory action."

Edward Lazarus, the FCC Chief of Staff, agreed: "There is some line between engineering questions and policy questions. The beauty of a group like BITAG is that it is an attempt to isolate the engineering ques-

tions from the policy questions. I don't think that the commission can or should delegate to that group the ultimate policy determinations. It's absolutely essential that the ultimate decision process occur at the commission."

**Universality.** In promoting greater deployment and adoption of broadband, a conference group recommended that any government program should "limit support for universal access to a percentage of the telecom industry's revenue base." This would essentially replace the current system, which includes an interstate access charge among other things, said Levin. The working group suggested that a new funding mechanism should not begin until the money is distributed only to new broadband projects (and not voice networks, for example) to ensure that it is funding networks that will offer the services of the future.

The new funding mechanism should establish new targets and make a transition from the voice-based funding model. Over the short term, there should be an increase in the percentage of money spent on adoption programs because broadband requires addressing issues of device literacy and Internet literacy. The working group urged that the government use a variety of community-based approaches and leverage existing government mechanisms.

As far as deployment, there was a consensus that a fund should be established for the currently under-served, with a broadband speed requirement of four megabits per second (Mbps) downstream and one Mbps upstream, a standard that would be reconsidered every five years. (It was noted that no rural phone companies were part of the working group proposing this standard, which parallels that of the FCC's Broadband Plan.) The fund could draw upon existing funds that are not effectively serving public purposes which Levin identified as Sprint and Verizon ETC [eligible telecommunications carriers] funds and interstate access support. He also advocated freezing interstate common-line support and phasing out remaining ETC funds.

The group recommended creating a 10-year transition plan from the current system, eventually merging the high-cost fund into a broadband fund. The inter-carrier compensation regime would also need to be reformed.

The fund should establish distribution criteria so that it would provide support only where there is no funding or business case for

broadband. One big issue, said Levin, is how to define the geographic territory served by broadband providers. Historically, this has been defined by the fixed-wire network architecture for telephony, a concept that makes less sense in today's environment. The working group thought that letting the parties define the territories they would like to serve is workable, if tricky.

Two months after the Aspen broadband conference, Blair Levin, writing as a Communications and Society Fellow at the Aspen Institute, published a white paper, "Universal Broadband: Targeting Investments to Deliver Broadband Services to All Americans."<sup>3</sup> The paper, prepared as a follow-up to the report of the Knight Commission on the Information Needs of Communities in a Democracy, proposes a universal service fund of \$10 billion over 10 years drawn from existing, no-longer-efficient programs that are part of the Universal Service Fund. The paper proposes the following:

[T]hat the funds be distributed through a transparent, market-based approach; that funds be provided only to areas where, without such funding, there is no private sector case to provide broadband; and that funds are provided to one provider per area. The criteria should be company- and technology-agnostic, and the recipients should be accountable for achieving universal broadband access in the relevant geographic areas.

Levin's report also proposes that government should expand, and eventually transform, the current Lifeline and LinkUp programs from subsidizing voice services to making broadband affordable to low-income individuals. Government agencies and nonprofits should form partnerships to address relevance barriers with targeted programs.

His report also urges the creation of a Digital Literacy Corps and an Online Digital Literacy Portal. Broadband adoption could also be spurred by an Executive Branch Disability Working Group, new efforts to monitor affordability and an "Apps for Inclusion" competition that would reward innovators who develop mobile, desktop or web programs that help citizens take advantage of community, state or federal services online.

---

3 [http://www.knightcomm.org/wp-content/uploads/2010/09/Universal\\_Broadband\\_Blair\\_Levin.pdf](http://www.knightcomm.org/wp-content/uploads/2010/09/Universal_Broadband_Blair_Levin.pdf).

**Competition.** There are several key questions that must be addressed in setting competition policy: how to set the right balance for competition? How to let the rules evolve to changing circumstances? How to prevent companies from leveraging their “bottlenecks” to capture adjacent markets? And how to incentivize constant upgrading of broadband quality?

A first step in addressing these questions, said Levin, should be the collection of data that reveals how markets change in light of the rollout of 4G wireless systems and DOCSIS 3.0 broadband provided via cable systems.

As far as “equitable use” policies for broadband, the general principle has been “no blocking or degrading of any legal content or devices” or “unreasonable discrimination,” subject to “reasonable network management” by broadband providers. A decisive issue, of course, is how to define what is “reasonable” and what is “unreasonable.” Generally, the standard has been whether an action is anti-competitive or anti-consumer in its effect or “not narrowly tailored to achieve a legitimate management purpose.” Wireless would have much greater flexibility in meeting this standard because of the more acute technological constraints.

There was some discussion among conference participants about the adequacy of BITAG in making these determinations, and whether such determinations are a nondelegable responsibility of the FCC. But in either case, the underlying question is how to allow Internet service providers to offer new sorts of “specialized services” or “managed services” without eclipsing their obligations to provide “best efforts” in providing nondiscriminatory data transmission. In other words, any premium, specialized service “could not interfere with or swallow up regular service, however that was defined,” said Levin.

Information about the services must be provided to the FCC, conference participants suggested, and the FCC must re-evaluate its rules in light of material shifts in competitive market structures over time. So, for example, if it turns out that wireless does compete with broadband, or if there is greater consolidation of the industry for whatever reason, the commission could take appropriate steps.

Should wireless be included in the framework outlined above? There was no consensus. Some people believe that the current market for wire-



less services does not warrant this sort of oversight and that wireless has different network management needs in any case. As Kevin Kahn put it, “The principles of access are the same, but the details of what is reasonable in the context of applying those principles, are different.”

Or as Dorothy Attwood of AT&T argued, “The issue is do you need to have an extension of those [nondiscrimination] rules to ensure that the Internet ecosystem is free and open, or to ensure that wireless services are, in fact, developing that way? That’s where the disagreement is. Wireless is different.”

### *Personal Data, Privacy and Other Social Goods*

A third working group focused on how to promote a “trust environment for personal data, privacy and other social goods on the Internet.” There was a strong consensus that trust matters a great deal in fostering growth and innovation on the Internet, and in facilitating adoption.

Jane Mago, Executive Vice President and General Counsel for Legal and Regulatory Affairs at the National Association of Broadcasters, reported that her working group decided to focus on “a user-control model” as the best way to encourage trust. This model requires several key elements, she said: education, transparency, compliance and enforcement mechanisms, and an awareness of international regimes for protecting privacy.

In building out a framework for building online trust, the government, private sector and users all play important roles. Government must act “as a regulator and facilitator,” said Mago, “in establishing the baseline rules that should prevail in the United States. Government can play a role in convening the key stakeholders to identify the issues that need resolution and in promoting digital literacy and exercising some meaningful enforcement authority.”

The private sector, for its part, “should try to come up with self-regulatory approaches,” said Mago, and help with the governance process. Individual users have the right to some digital literacy training, she said, adding, “They have to believe that their rights are genuinely protected.” At the same time, users also have some responsibilities. The group’s recommendations were of a general nature:

1. The executive branch should convene a representative set of stakeholders to establish baseline principles for privacy protection, both on the domestic and international fronts. The long-term goal should be to harmonize the two sets of principles and try to affirm user choice, transparency, meaningful disclosure and effective enforcement.
2. The executive branch should make some of its information from the Broadband Technology Opportunities Program (BTOP) more widely available. This could help promote digital literacy.
3. A “user-identity browser” could help people create online identities with personalized parameters for privacy protection. Government might help convene this process and promote development of an interactive interface.
4. Self-regulation should be emphasized as the best way to tackle privacy protection.
5. A process should be established to help reap societal benefits from general sharing of certain types of information, especially personal health data. Mago explained, “If I could, as a consumer, create some expectation that my information would be able to be used—that, for example, I might be able to sell it or trade it off in different environments—that could lead to a social good.”

It was pointed out that personal health information could yield enormous social benefits if aggregated—but that would require anonymity protections and a reliable approval process. However, Andrew Puddephatt, Director of Global Partners and Associates, pointed out, “We need more research into identifying specific, clear benefits to society from data-sharing” as well as new mechanisms “to assure that checks and balances are built into the system” to protect privacy.

6. Programs should be created to promote digital literacy about privacy and security in the use of both computers and digital devices. Working Group II proposed that educating users could be included in elementary school curricula and in public service announcements, for example. Currently, nine states have laws that put digital literacy in middle-school curricula, and the industry has developed a program called WebWiseKids. Another idea was to condition eligibility for e-rate grants on the availability of digital literacy tools.

## Conclusion

The Internet as a hosting infrastructure for diverse technologies and vast activity in commerce, culture and democratic life has come a long way from its early days. This maturing of the system, its technologies, the economic models and the cultural expectations, make it all the more complicated to develop appropriate policies to support the broadband infrastructure.

Conference discussions pointed to the dangers of “market enclosure of the Internet commons” as well as the manifold benefits that commercial activity on the Internet has generated. In many respects, the challenge facing public policy is how to reconcile these values and develop a coherent, stable synthesis for our time.

One key lesson from the conference was that broadband does not exist in isolation from other aspects of commerce and culture, but rather it is implicated in a dense ecosystem of technology, markets and social life. As such, any new policies for broadband must take account of this rich environment and the repercussions that will invariably follow.

Although the conference did not yield a clear consensus on many issues, it clarified many of the core questions that must be addressed. It also advanced some specific proposals for further consideration. It offered some new ideas for improving broadband deployment and adoption, and for improving privacy and security in computing and

**...broadband does not exist in isolation from other aspects of commerce and culture....**

on the Internet. The “digital embassies” proposal was widely seen as a breakthrough concept that may help resolve many of the knotty issues surrounding the use of data in cloud computing. Since the fate of the U.S. broadband infrastructure requires our immediate attention, these ideas may have some timely application in the near future.

# APPENDIX

---



## *Rewriting Broadband Regulation*

Aspen, Colorado  
August 11–14, 2010

### Conference Participants

**Robert Atkinson**

Founder and President  
The Information Technology and  
Innovation Foundation

**Dorothy Attwood**

Senior Vice President,  
Public Policy and  
Chief Privacy Officer  
AT&T Services, Inc.

**Catherine Bohigian**

Vice President, Federal Affairs  
Cablevision Systems Corporation

**David Bollier**

Independent Journalist and  
Consultant  
Onthecommons.org

**Laura Carter**

Senior Attorney-Regulatory  
Affairs  
Legal and Corporate Affairs  
Microsoft Corporation

**Jonathan Chaplin**

Director  
Credit Suisse

**Mignon Clyburn**

Commissioner  
Federal Communications  
Commission

**Alan Davidson**

Director of Public Policy,  
Americas  
Google

**David Don**

Senior Director, Public Policy  
Comcast Corporation

**Charles M. Firestone**

Executive Director  
Communications and Society  
Program  
The Aspen Institute

**Susan Fox**

Vice President, Government  
Relations  
The Walt Disney Company

**Michael Gallagher**

President and Chief Executive  
Officer  
Entertainment Software  
Association

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

**Richard Green**

Board Member  
Liberty Global Inc.

**Dale Hatfield**

Executive Director,  
Silicon Flatirons Center  
and  
Adjunct Professor  
University of Colorado at  
Boulder

**Reed Hundt**

Principal  
REH Advisors

**Julia Johnson**

President  
Net Communications

**Kevin Kahn**

Senior Fellow, and  
Director, Communications  
Architecture  
Intel Labs  
Intel Corp

**Anna-Maria Kovacs**

Founder and President  
Regulatory Source  
Associates, LLC

**John Kuzin**

Senior Director, Regulatory  
Qualcomm, Inc.

**Edward Lazarus**

Chief of Staff  
Federal Communications  
Commission

**Blair Levin**

Senior Fellow  
Communications and Society  
Program  
The Aspen Institute

**Jane Mago**

Executive Vice President and  
General Counsel  
Legal and Regulatory Affairs  
National Association of  
Broadcasters

**Pamela Miller**

Director General  
Telecommunications  
Policy Branch  
Strategic Policy Sector  
Industry Canada

**Eli Noam**

Director, Columbia Institute for  
Tele-Information, and  
Professor of Economics and  
Finance  
Columbia Business School  
Columbia University

**Safiya Noble**

Program Associate  
University of Illinois at  
Urbana-Champaign  
and  
Aspen Institute Guest Scholar

**Robert Pepper**

Vice President Global  
Technology Policy  
Cisco Systems



**Andrew Puddephatt**

Director  
Global Partners and Associates

**Jacquelynn Ruff**

Vice President  
International Public Policy and  
Regulatory Affairs  
Verizon Communications

**Andrew Schwartzman**

Senior Vice President and Policy  
Director  
Media Access Project

**Ben Scott**

Policy Advisor for Innovation  
Office of the Secretary of State

**Aparna Sridhar**

Policy Counsel  
Free Press

**Lawrence Strickling**

Assistant Secretary for  
Communications and  
Information  
National Telecommunications  
and Information Administration  
U.S. Department of Commerce

**Steven Teplitz**

Senior Vice President  
Government Relations  
Time Warner Cable

**Damian Thorman**

National Program Director  
John S. and James L. Knight  
Foundation

**Jenny Toomey**

Program Officer  
Media Rights & Access  
Ford Foundation

**Nicol Turner-Lee**

Vice President and Director  
Media and Technology Institute  
Joint Center for Political and  
Economic Studies

**Michael Tyler**

Founder and Managing Director  
Tyler & Company

**Kevin Werbach**

Associate Professor of Legal  
Studies and Business Ethics  
Wharton School  
University of Pennsylvania

*Staff:*

**Sarah Eppheimer (Snodgrass)**

Senior Project Manager  
Communications and Society  
Program  
The Aspen Institute



## About the Author

**David Bollier** is an author, activist, blogger and consultant who studies the commons as a new paradigm of economics and culture. He has pursued this work over the past 10 years with a variety of international and domestic partners, including the Commons Strategy Group, an international consulting project that he recently co-founded, and a new blog, Bollier.org.

Bollier has worked with American television writer/producer Norman Lear since 1984 on a variety of nontelevision, public affairs projects. He is also Senior Fellow at the Norman Lear Center at the USC Annenberg School for Communication and co-founder and board member of Public Knowledge, a Washington policy advocacy organization dedicated to protecting the information commons.

Bollier's commons scholarship and advocacy has taken many forms: as an author, conference organizer and frequent international speaker; as the host of an educational film, *This Land Is Our Land: The Fight to Reclaim the Commons* (2010); as the Croxton Lecturer at Amherst College where he taught "The Rise of the Commons;" and as an expert witness for the "design commons" in a trademark lawsuit; among other initiatives. From 2004 to 2010, Bollier was Founding Editor of Onthecommons.org and a Fellow of On the Commons.

Bollier has written 10 books. The most recent include *Viral Spiral: How the Commoners Built a Digital Republic of Their Own* (2009); *Brand Name Bullies: The Quest to Own and Control Culture* (2005); and *Silent Theft: The Private Plunder of Our Commons Wealth* (2002). He lives in Amherst, Massachusetts.



# Previous Publications from the Aspen Institute Communications Policy Project

*Scenarios for a National Broadband Policy*, by David Bollier

The report of the 24th Annual Aspen Institute Conference on Communications Policy in Aspen, Colorado, captures the scenario building process that participants used to map four imaginary scenarios of how the economy and society might evolve in the future, and the implications for broadband policy. It identifies how certain trends—economic, political, cultural, and technological—might require specific types of government policy intervention or action. 2010, 52 pages, ISBN Paper: 0-89843-517-X, \$12.00

*Rethinking Spectrum Policy: A Fiber Intensive Wireless Architecture*, by Mark MacCarthy

The report resulting from the 2009 Aspen Institute Roundtable on Spectrum Policy explores innovative ways to respond to the projections of exponential growth in the demand for wireless services and additional spectrum. In addition to discussing spectrum reallocations, improved receivers, shared use and secondary markets as important components for meeting demand, the report also examines opportunities for changes in network architecture, such as shifting the mix between fiber and wireless. 2010, 58 pages, ISBN Paper: 0-89843-520-X, \$12.00

*ICT: The 21st Century Transitional Initiative*, by Simon Wilkie

The report of the 23rd Annual Aspen Institute Conference on Communications Policy in Aspen, Colorado addresses how the United States can leverage information and communications technologies (ICT) to help stimulate the economy and establish long-term economic growth. The report, written by Roundtable rapporteur Simon Wilkie, details the Aspen Plan, as developed in the summer of 2008, prior to the economic meltdown beginning in September 2008 and prior to the election of Barack Obama as President. The Plan recommends how

the Federal Government—through executive leadership, government services and investment—can leverage ICTs to serve the double bottom line of stimulating the economy and serving crucial social needs such as energy efficiency and environmental stewardship. 2009, 80 pages, ISBN Paper: 0-89843-500-5, \$12.00

*A Framework for a National Broadband Policy*, by Philip J. Weiser

While the importance of broadband access to functioning modern society is now clear, millions of Americans remain unconnected, and Washington has not yet presented any clear plan for fixing the problem.

Condensing discussions from the 2008 Conference on Communications Policy and Aspen Institute Roundtable on Spectrum Policy (AIRS) into a single report, Professor Philip Weiser of the University of Colorado at Boulder offers a series of specific and concrete policy recommendations for expanding access, affordability, and adoption of broadband in the United States. 2008, 94 pages, ISBN Paper: 0-89843-484-X, \$12.00

*The Future of Video: New Approaches to Communications Regulation*, by Philip J. Weiser

As the converged worlds of telecommunications and information are changing the way most Americans receive and relate to video entertainment and information, the regulatory regimes governing their delivery have not changed in tune with the times. These changes raise several crucial questions: Is there a comprehensive way to consider the next generation of video delivery? What needs to change to bring about a regulatory regime appropriate to the new world of video? The report of the 21st Annual Conference on Communications Policy in Aspen, Colorado, outlines a series of important issues related to the emergence of a new video marketplace based on the promise of Internet technology and offers recommendations for guiding it into the years ahead. 2006, 70 pages, ISBN Paper: 0-89843-458-0, \$12.00

*Clearing the Air: Convergence and the Safety Enterprise*, by Philip J. Weiser

The report describes the communications problems facing the safety enterprise community and their potential solutions. The report offers several steps toward a solution, focusing on integrating communications across the safety sector on an Internet-Protocol-based backbone network, which could include existing radio systems and thus make systems more dependable during emergencies and reduce costs by taking advantage of economies of scale. The conference participants stressed that the greatest barriers to these advances were not due to lagging technology but to cultural reluctance in adopting recent advances. Writes Weiser, “The public safety community should migrate away from its traditional reliance on specialized equipment and embrace an integrated broadband infrastructure that will leverage technological innovations routinely being used in commercial sectors and the military.” 2006, 55 pages, ISBN Paper: 0-89843-4, \$12.00

*Reforming Telecommunications Regulation*,

by Robert M. Entman

The report of the 19th Annual Aspen Institute Conference on Telecommunications Policy describes how the telecommunications regulatory regime in the United States will need to change as a result of technological advances and competition among broadband digital subscriber line (DSL), cable modems, and other players such as wireless broadband providers. The report proposes major revisions of the Communications Act and FCC regulations and suggests an interim transitional scheme toward ultimate deregulation of basic telecommunications, revising the current method for universal service subsidies, and changing the way regulators look at rural communications. 2005, 47 pages, ISBN Paper: 0-89843-428-9, \$12.00

*Challenging the Theology of Spectrum: Policy Reformation Ahead*,

by Robert M. Entman

This report examines the theology of spectrum—that is, the assumptions and mythology surrounding its management and use. The report looks at how new technologies affecting spectrum, such as software-defined radio, can challenge the conventional wisdom about how spec-

trum should be managed. Such innovations allow for access to unused frequency space or time on frequencies that are otherwise licensed to an exclusive user. 2004, 43 pages, ISBN Paper: 0-89843-420-3, \$12.00

*Spectrum and Network Policy for Next Generation Telecommunications*,  
by Robert M. Entman

The report of the 18th Annual Aspen Institute Conference on Telecommunications Policy offers policy alternatives in both spectrum and network policy to achieve new gains for the telecommunications field. The first essay suggests new management approaches to encourage more efficient uses of spectrum while preserving the commitment to reliability of service and public safety values. The second essay debates the competitive structure of the telecommunications industry and its implications for building next-generation networks (NGN) and identifies three areas to encourage optimal development of the NGN: operate the NGN on a price-deregulated basis and begin to address access regulation issues, secure the intellectual property rights of content suppliers, and adjust the system of subsidized pricing to bring about competitively neutral pricing. 2004, 92 pages, ISBN Paper: 0-89843-394-0, \$12.00

*Balancing Policy Options in a Turbulent Telecommunications Market*,  
by Robert M. Entman

This report assesses the future of communications regulatory paradigms in light of desirable changes in spectrum policy, telecommunications market environments, and regulatory goals. It suggests four models of regulation, including government allocation, private spectrum rights, unlicensed commons, and a hybrid system of dynamic spectrum access. It also addresses how changes in spectrum and other telecommunications policies, as well as new business realities, might affect current regulatory regimes for the telecommunications industries. The report includes an essay on spectrum management, "The Current Status of Spectrum Management," by Dale Hatfield. 2003, 79 pages, ISBN Paper: 0-89843-370-3, \$12.00



*Telecommunications Competition in a Consolidating Marketplace,*

by Robert M. Entman

In the telecommunications world, what would a fully competitive environment look like? What communications initiatives should policy-makers develop—considering the ultimate welfare of the consumer—to implement change in the regulatory climate? This report explores ways to reshape the current regulatory environment into a new competitive space. It addresses competition not only within but across separate platforms of communications such as cable, wireline telephony, wireless, satellite, and broadcast. The report also includes an essay on an innovative approach to wireless regulation, “Opening the Walled Airwave,” by Eli Noam. 2002, 64 pages, ISBN Paper: 0-89843-330-4, \$12.00

*Transition to an IP Environment,* by Robert M. Entman

This report examines a “layered approach” to regulation. By viewing telecommunications in four separate layers—content, application, network, and data link—policy discussions can address concerns in one layer without negatively affecting useful existing policy in other layers. Also presented are beliefs that the growth of broadband should prompt a new discussion about universal service reform. The report also includes “Thoughts on the Implications of Technological Change for Telecommunications Policy,” by Michael L. Katz. 2001, 78 pages, ISBN Paper: 0-89843-309-6, \$12.00

---

Reports can be ordered online at [www.aspeninstitute.org/publications](http://www.aspeninstitute.org/publications) or by sending an email request to [publications@aspeninstitute.org](mailto:publications@aspeninstitute.org).



# About the Aspen Institute Communications and Society Program

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

The Communications and Society Program is an active venue for global leaders and experts to exchange new insights on the societal impact of digital technology and network communications. The Program also creates a multi-disciplinary space in the communications policy-making world where veteran and emerging decision-makers can explore new concepts, find personal growth, and develop new networks for the betterment of society.

The Program's projects fall into one or more of three categories: communications and media policy, digital technologies and democratic values, and network technology and social change. Ongoing activities of the Communications and Society Program include annual roundtables on journalism and society (e.g., journalism and national security), communications policy in a converged world (e.g., the future of international digital economy), the impact of advances in information technology (e.g., "when push comes to pull"), and serving the information needs of communities. For the past three years, the Program has taken a deeper look at community information needs through the work of the Knight Commission on the Information Needs of Communities in a Democracy, a project of the Aspen Institute and the John S. and James L. Knight Foundation. The Program also convenes the Aspen Institute Forum on Communications and Society, in which chief executive-level leaders of business, government and the non-profit sector examine issues relating to the changing media and technology environment.

Most conferences utilize the signature Aspen Institute seminar format: approximately 25 leaders from a variety of disciplines and perspectives engaged in roundtable dialogue, moderated with the objective of driving the agenda to specific conclusions and recommendations.

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, [www.aspeninstitute.org/cc&s](http://www.aspeninstitute.org/cc&s).

The Program's Executive Director is Charles M. Firestone, who has served in that capacity since 1989, and has also served as Executive Vice President of the Aspen Institute. He is a communications attorney and law professor, formerly director of the UCLA Communications Law Program, first president of the Los Angeles Board of Telecommunications Commissioners, and an appellate attorney for the U.S. Federal Communications Commission.