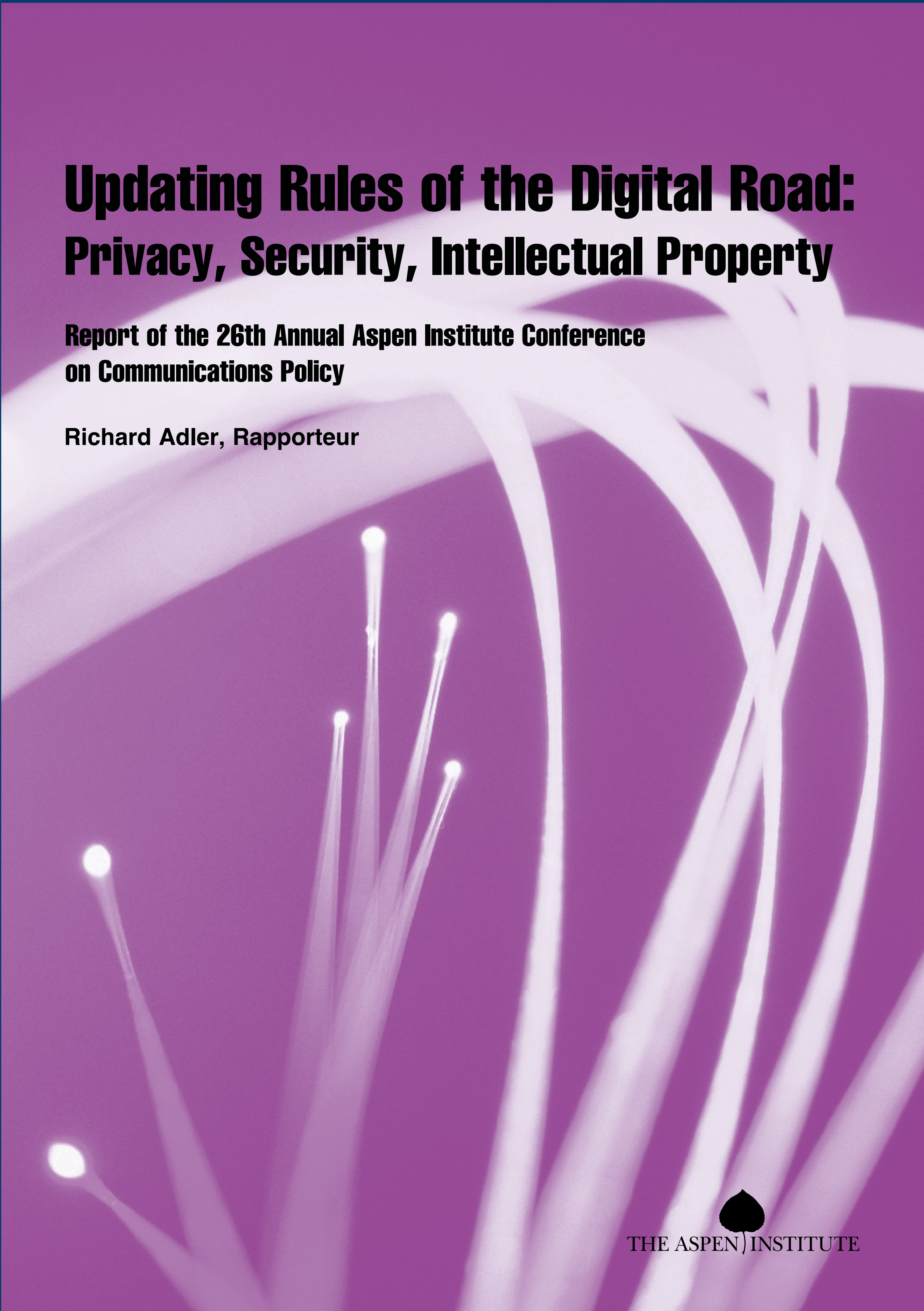
Communications and Society Program

Updating Rules of the Digital Road: Privacy, Security, Intellectual Property

Report of the 26th Annual Aspen Institute Conference on Communications Policy

Richard Adler, Rapporteur



THE ASPEN INSTITUTE

Updating Rules of the Digital Road: Privacy, Security, Intellectual Property

Richard Adler
Rapporteur

THE ASPEN INSTITUTE

Communications and Society Program
Charles M. Firestone
Executive Director
Washington, D.C.
2012

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

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	Patricia K. Kelly
Executive Director	*Assistant Director*

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

Published in the United States of America in 2012
by The Aspen Institute

Printed in the United States of America

ISBN: 0-89843-563-3

12-002

1859CSP/12-BK

Contents

This report is written from the perspective of an informed observer at the Twenty-Sixth 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

The Aspen Institute Conference on Communications Policy, now in its 26th year, is a critical forum for telecommunications, Internet and information industry executives, government leaders, consumer representatives and academic thought leaders to explore cutting-edge questions of broadband access, competition among firms and regulation. In recent years, the Conference has focused its attention on the first two issues—access and competition. But given the current growth and impact of the Internet, this year's Conference concentrated on the elements that will allow for greater use of broadband as the common medium: security, privacy and intellectual property regulation.

Whether under the United States National Broadband Plan or other regimes throughout the world, broadband users want a trusted environment where their communications are secure, private and protected. As Cameron Kerry, General Counsel for the U.S. Department of Commerce, noted, *trust* is the "flagship issue" related to the future of the digital economy. With this in mind, 38 leading communications policy experts met August 16-19, 2011, in Aspen, Colorado, to discuss the regulatory and policy means of creating that trusted environment. They debated policies pertaining to the protection of data on the network and in the cloud, privacy regulations that will impact the development of broadband communications and principles that should apply to the protection of digital content.

The resulting report, *Updating Rules of the Digital Road: Privacy, Security, Intellectual Property*, provides a thorough discussion of the threats that plague the use of today's communications media as well as a series of policy recommendations to remedy those problems.

One of the interesting discussions that emerged in the area of privacy policy, for example, was the application of the Fair Information Practices (FIPs) to the current, rapidly changing information environment. Using the FIPs framework, participants offered recommendations for three critical emerging issues, including the evolving definition of personally identifiable information, mobile privacy and the misuse of data analytics.

The recommendations in this report are derived from both plenary and working group sessions. However, the Conference did not vote or ask for consensus on any of the proposals or recommendations. Thus 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

We would like to thank our attending sponsors of the 2011 Aspen Institute Communications and Society Program for making this and our other conferences possible: Microsoft and the Markle Foundation, *Senior Partners;* AT&T, Comcast Corporation, Google and The Walt Disney Company, *Corporate Sponsors;* Cablevision Systems Corporation, Cisco Systems, Credit Suisse, Ford Foundation, Liberty Global Inc., Qualcomm, Stifel Nicolaus, Time Warner Cable and Verizon Communications, *Corporate Associates.*

I also want to acknowledge and thank Richard Adler, our talented rapporteur, for his excellent synthesis of the discussions and debates that transpired during the Conference as well as our participants, listed in the Appendix, for their contributions to these important issues. 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.
February 2012

Updating Rules of the Digital Road: Privacy, Security, Intellectual Property

Richard Adler

Updating Rules of the Digital Road: Privacy, Security, Intellectual Property

Richard Adler

The Paradox of Openness

The Internet is rapidly becoming the main thoroughfare over which the vital functions of society—communications, commerce, news, finance, civic and government affairs—are carried. The Net has already had enormous impact on a range of industry sectors, ranging from retailing and financial services to publishing and entertainment, and it has begun to reshape critical institutions, ranging from education to health care. Virtually every enterprise, no matter what business it is in, has been touched in multiple ways by the digital revolution: functions such as advertising, business intelligence, research, sales, orders, payments, logistics and even the management of daily activities have moved online. Internet-driven connectivity has made the world increasingly "flat" by creating a global marketplace. Government agencies at all levels are in the midst of putting their functions online in order to increase efficiency of operations and enhance transparency. Social media have emerged as a new way for people—especially young people—to connect with one other and express their individuality. These online tools have also demonstrated the capacity to organize political action and to galvanize resistance to repressive regimes, even as they strive to exercise control over these grassroots networks. Wireless media have extended the reach of the Net to the entire world. A series of reports from the Aspen Institute Communications and Society Program have documented these tectonic shifts (see table) and explored some of the issues that they are raising.

Some Indicators of the Amazing Reach of the Net

- In May 2011, 78 percent of American adults used the Internet; among Americans ages 18 to 29, 95 percent were online; and 83 percent of adult Americans owned a cell phone.[1]
- The Indexed Web contained at least 11.6 billion pages as of September 2011.[2]
- Approximately two billion Google searches are conducted daily.[3]
- YouTube attracts 490 million unique users who spend 2.9 billion hours per month watching videos.[4]
- 107 trillion email messages were sent in 2010, of which 89 percent were estimated to be spam.[5]
- 133 million blogs have been indexed by Technorati since 2002.[6]
- There are more than 800 million active Facebook users, half of whom log onto Facebook on any given day.[7]
- U.S. retail e-commerce sales were $47.5 billion in the second quarter of 2011, or 4.6 percent of total retail sales, up from 2 percent of U.S. retail sales in 2005.[8]
- 29 percent of record companies' global revenues came from digital distribution of music in 2010.[9]
- iTunes has delivered more than 16 billion music downloads from 2003 to 2011.[10]
- In May 2011, Amazon announced that its sales of e-books exceeded sales of printed books (paperback and hardcover editions combined).[11]

[1] Demographics of Internet Users, Pew Internet and American Life Project. Available at: www.pewinternet.org/Static-Pages/Trend-Data/Whos-Online.aspx.

[2] The size of the World Wide Web, September 26, 2011. Available at: www.worldwidewebsize.com/.

[3] "How many searches has Google done?" Mathew Ingram, September 5, 2008. Available at: http://www.mathewingram.com/work/2008/09/05/how-many-searches-has-google-done/.

[4] Ten Fascinating YouTube Facts that May Surprise You, Mashable, February 19, 2011. Available at: http://mashable.com/2011/02/19/youtube-facts.

[5] Internet 2010 in numbers, Pingdom, January 12, 2011. Available at: http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/.

6. Social Media, Web 2.0 And Internet Stats, Future Buzz, January 12, 2009. Available at: http://thefuturebuzz.com/2009/01/12/social-media-web-20-internet-numbers-stats/.
7. Statistics, Facebook, September 26, 2011. Available at: www.facebook.com/press/info.php?statistics.
8. Quarterly Retail E-Commerce Sales, 2nd Quarter 2011, U.S. Census Bureau, August 16, 2011. Available at: www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf.
9. IFPI Digital Music Report 2011, International Federation of the Phonographic Industry. Available at: www.ifpi.org/content/library/DMR2011.pdf.
10. "Apple: 16 billion iTunes songs downloaded, 300 million iPods sold," Engadget, October 4, 2011. Available at: www.engadget.com/2011/10/04/apple-16-billion-itunes-songs-downloaded-300-million-ipods-sol.
11. "That Was Fast: Amazon's Kindle Ebook Sales Surpass Print (It Only Took Four Years)," Tech Crunch, May 19, 2011. Available at: http://techcrunch.com/2011/05/19/that-was-fast-amazons-kindle-ebook-sales-surpass-print-it-only-took-four-years/.

Accompanying the growth of the Internet and its benefits has been a darker side: the emergence of threats that have the potential to undermine the integrity of the Net and diminish the willingness of users to conduct activities online. Part of this threat comes from the technological nature of the Net that leads, almost inevitably, to concerns about the availability and reliability of online communications. Few if any users of modern technology have escaped the frustration of dropped cell phone calls, crashed servers, network slowdowns or periodic outages of Internet services. But of more concern is the threat from illegitimate and/or illegal actions that have the potential to erode users' confidence in the safety of their online activities, inhibiting individual use as well as compromising the overall value of the Net.

An ironic paradox about the contemporary Internet is that the same fundamental design philosophy that has played a key role in its success is also responsible for some of its most serious vulnerabilities. This philosophy stems directly from the way the Net began and how it grew in its early days. When the Arpanet—the first embodiment of the technology that evolved into today's Internet—was developed in the mid-1960s, it was a network intended to connect a limited number of government and academic computer research centers. This development took place in an era when computers were still relatively esoteric devices, the use of which was restricted to a community of highly trained professionals. When the Arpanet was launched in 1969, it linked just four locations,[1] all federally funded computer research sites, in order to expand access to these complex and expensive resources. Moreover, the design of the network was highly decentralized with no single point of control.

Over the next several decades, the Arpanet continued to grow in the academic world, initially with federal support, then with broader funding. Because there was never a central authority operating the Arpanet, no one who had access to it had to ask permission to develop and offer new services for it. A community of users (most of whom were computer professionals or students with computer skills) took responsibility for managing the network and developing new capabilities. The Internet community deliberately cultivated an open, non-hierarchical culture that imposed few restrictions on how the network could be used. They saw little reason to build in elaborate safeguards against potential misuse—based on the assumption that everyone who had access to the network could be trusted to act responsibly and appropriately. As a result, the network included no provisions that would provide authentication that users were in fact who they said they were.

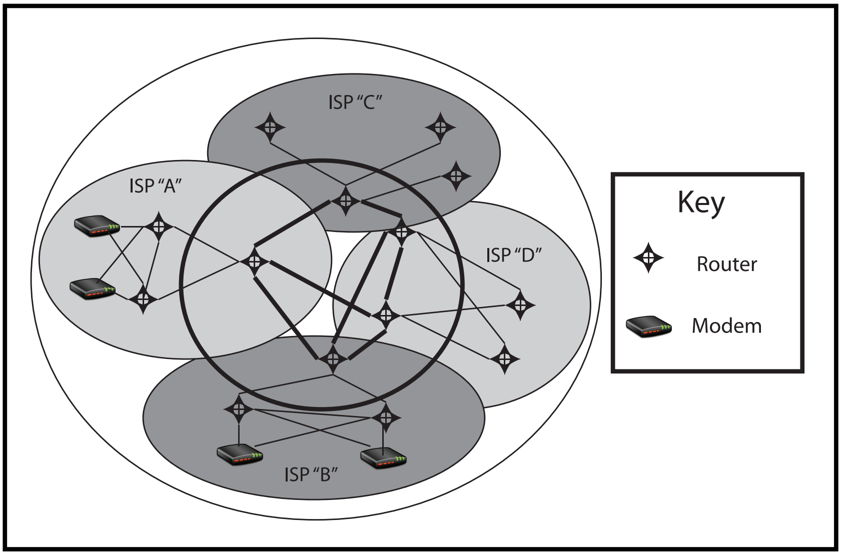
By contrast, the early commercial "online" computer services were closed systems that linked users over proprietary networks to remote computer resources that were completely controlled by the service provider. Because users (initially businesses and later individuals equipped with inexpensive PCs) were typically billed for their usage, mechanisms were built in to establish and verify their identities.

These "walled gardens" were relatively safe, but they were inherently limited. The services offered on any given network system were restricted to those developed by or permitted by the system operator. In addition, users of one online network could only communicate with other users of the same system (much as was the case in the early days of telephony, when each phone network was a separate entity and users had to have multiple phones to use multiple networks).

The closed, commercial services enjoyed an early period of success (think of AOL), but many eventually lost out to the vastly larger, more dynamic and more open world of the Internet. Initially, the Internet seemed to be an unlikely competitor, with no centralized planning or control, but it provided an open environment that proved to be ideal for the experimentation that led to such innovations as the World Wide Web, blogs, eBay, Google, Wikipedia, craigslist, Facebook, Skype and YouTube, which collectively generated more value than walled-garden services could match. And because the Internet was open to all, the value of being on the Internet increased exponentially as the user base grew and it became possible to send messages to anyone with an Internet email address—which rapidly became almost everyone.

A hallmark of the Internet today is its diversity: it is, in fact, not a single network but a heterogeneous, global network of networks held together only by a series of voluntary agreements about standards and protocols among a host of participants (see figure below). Among the key players are the Internet Service Providers (ISPs), who offer access to the Internet and deliver users' messages to the appropriate destinations. ISPs include large national and multinational operators as well as a myriad of small, local service providers, public and private.

Internet Infrastructure: A Network of Networks



Source: Jamie Barnett, presented to the Aspen Institute Conference on Communications Policy on August 17, 2011.

As Jamie Barnett, Chief of the Federal Communications Commission's (FCC) Public Safety and Homeland Security Bureau, notes, the Internet was designed from the beginning to grow organically, with new networks able to join the family of networks with relatively few restrictions. Remarkably, this decentralized network model has scaled successfully and has accommodated phenomenal growth.[2]

The Internet is not only diverse in a technical sense, but it is also highly diverse in terms of its users: the universe of some two billion users globally includes individuals, ranging from educated elites to poor peasants, in every country on the planet; businesses both large and small; government agencies; and, perhaps of greatest concern, critical infrastructure providers that rely on the Internet to manage the operations of such vital components of society as health care systems, the electrical power grid, gas and oil pipelines, emergency services, banking and financial services as well as key military and intelligence assets. And, of course, the Internet is also home to hackers, criminals, terrorists and even hostile nations that consider other Internet users as targets to attack.

In assessing threats and devising solutions, it is necessary to recognize that different types of users will require different types of protection. On one hand, particular attention needs to be given to the needs of the most vulnerable populations, including unsophisticated groups such as children—who have been described by the Chairman of the Federal Trade Commission (FTC) as "tech-savvy but judgment-poor"[3] —the elderly and the poor. On the other hand, critical network users may be more sophisticated but their social and economic importance demand especially high levels of protection. And, while the primary focus of concern here is on domestic issues, it is important to keep in mind that the Internet is now truly global, and solutions that work only within the borders of this country may not be sufficient.

It is useful to keep these fundamental characteristics of openness, decentralization and heterogeneity in mind as we consider three key issues that need to be addressed if the Internet is to reach its full potential. These issues are related to threats to security, to privacy and to intellectual property.

Security Threats

Internet users do vary tremendously in their levels of sophistication and the resources they have available to protect themselves. But despite their differences, they are all potentially confronted with security threats that arise from misuse of the open architecture and interconnected nature of the Internet.

According to a recent review of emerging security threats from the Georgia Tech Cyber Security Summit 2011, "In the past year, we have witnessed cyber attacks of unprecedented sophistication and reach."[4] Among the most prominent security threats are botnets, spam and malware infections.

Botnets are networks of captive computers under the control of a malicious, often criminal, server complex. At the command of their masters, botnets are able to direct large streams of traffic across the network, resulting in floods of spam email or denial-of-service attacks intended to disrupt the operation of legitimate service providers. Botnets can spread virally through covert software delivered over the Internet to unsuspecting victims and can be quite large: the so-called "Bredolab botnet," which emerged in 2009 and was taken down by Dutch law enforcement authorities in October 2010, at one point controlled as many as 30 million "zombie" computers that were capable of sending out more than three billion spam messages a day.[5] Users who have become members of a botnet army may be unaware of their captivity, at least until they notice a degradation of their computer's performance or suffer personal loss due to malicious actions by the bot software. According to the Georgia Tech review of emerging cyber threats, "While botnets have plagued the Internet for some time, their usage in advanced persistent threats is evolving, as are the tactics, techniques and procedures for command and control."[6] In other words, attacks are becoming more sophisticated.

Spam has been around for as long as email, but it started to show a darker side when email messages began to appear purporting to represent foreign dignitaries seeking assistance in moving large sums of money abroad in order to entrap Internet users in fraudulent financial schemes.[7] This type of scam has morphed into other, even more deceptive types of cyber threats that include "phishing" messages that seem to come from a legitimate institution asking users to divulge information on their bank accounts or emails that appear to have come from a family member with an attached photograph that is actually cleverly disguised malware. More recently, users have received innocent-looking emails inviting them to visit websites that can infect their computers with malware in much the same way that spam can.

Many of these threats take advantage of the foundation of trust and the consequent lack of authentication procedures that have always existed on the Internet. In the earliest years of the Internet, when users were known to each other and had no reason to doubt, this trust could be justified. But the Internet has evolved into a global mass communications medium open to everyone and offers no simple method of verifying that a communication that looks like it is from your daughter really *is* from your daughter.

According to the FCC's Barnett, botnets, spam and website infections are not the only cybersecurity problems of concern. While these threats are focused on the endpoints of the Internet (i.e., network users' systems), the basic infrastructure of the Internet contains vulnerabilities that also have their roots in the legacy of trust that existed among the Internet's pioneers. This trust, along with a desire to make the network as user-friendly and simple as possible, allocating higher-level functionality to the network edge, drove the Internet's designers to strip virtually all security functionality out of the network protocols. Perhaps most critical among these missing functionalities is the absence of effective authentication mechanisms, which shows up in two critical areas—the Internet's internal routing methods and its domain name system.

Internet routing—the procedures that govern how a given message makes its way from its origin to its intended destination—often involves moving content through multiple separate but interconnected networks. A specific set of rules known as the border gateway protocol (BGP) is used to manage connections between routers that link different networks. When a new network joins the Internet, it announces itself and all the other networks to which it can connect. Most of the time, this information is accurate. However, a network operations center (NOC) operator may sometimes make a mistake and send out the wrong route information. Unfortunately, since there is no way to check the accuracy or authenticity of the information, the rest of the Internet takes the NOC operator's instructions at face value. This has led to some dangerous but accidental misroutes on the Internet, which have generally been noticed and corrected relatively quickly. But some misroutes, called “route hijacks,” are suspected of being malicious in nature. In April 2010, for example, as much as 15 percent of all domestic U.S. Internet traffic was misrouted offshore to China.[8] Users would not have noticed the misrouting (since messages ultimately reached their intended destinations) except that an eavesdropper in China happened to be in a good position to monitor U.S. Internet traffic at the time of the event and saw what was happening.

The domain name system (DNS) is the equivalent of directory service for the Internet, converting English language website addresses (e.g., amazon.com or stanford.edu) to machine-readable addresses for destination servers. Given its historical context and its singular purpose, the DNS implicitly relies on user trust, which has provided ill-intentioned hackers with an opportunity to manipulate the DNS infrastructure. For example, hackers have deliberately tampered with the DNS system in order to redirect users to malicious websites designed to harvest personally identifiable information or to plant malware on user machines.

In these cases, the prevailing rules that govern operation of the Internet are based on the assumption that users are who they say they are and that the information they provide is accurate and trustworthy. Because this assumption is so deeply embedded in the design of the Internet’s architecture, it has been challenging to develop solutions that provide robust protection against these kinds of threats while preserving the efficiency and openness that have helped make the Internet so successful.

Privacy Threats

A second type of threat to the integrity of the Internet involves the unauthorized disclosure of individuals’ personal information that has been entrusted to third parties. As more and more activities move online, the amount of data generated by people in their daily lives has grown enormously. And as personal data online proliferates, it becomes increasingly easy for users to lose track of who has access to what information about them—and what happens to that information.

Some of this data is created by users directly, through activities such as online shopping or online banking. With the rise of social media, users are voluntarily sharing more and more personal information about their lives. Other types of information are gathered from consumers in the course of their daily lives and are stored in online databases.

The vast reach of the Net opens new possibilities for privacy breaches by parties whose identities may be difficult to determine and who may be located anywhere in the world. In addition, "data-mining" techniques make it possible to assemble and analyze hitherto unconnected information about an individual's life to create a remarkably detailed portrait of that person's activities, preferences, assets, relationships, etc., without, at least in some cases, an individual's knowledge or permission.

To inform consumers about what happens to the information they provide to third parties, companies that collect data are legally required to provide customers with a written privacy policy statement annually, and websites must make their privacy policies available to their users. In theory, these statements provide a helpful degree of transparency, but in practice, lengthy privacy documents, typically written in dense legalese, are less than effective. As Thomas Power, former Chief of Staff of the National Telecommunications and Information Administration, pointed out during his tenure, privacy statements are generally not very informative for non-lawyers. A 2008 study from researchers at Carnegie Mellon concluded that these statements are generally "hard to read, [are] read infrequently, and do not support rational decision making." The study's authors estimated that approximately 200 hours—the equivalent of five full work weeks—would be required to read through all of the privacy statements encountered by an average person each year, and they calculated that the annual "national opportunity cost to read all of these policies" was approximately $781 billion—considerably more than the value of all online advertising.[9] While some progress has been made in simplifying these disclosers, more work needs to be done.

The practical effectiveness of privacy schemes developed in other areas has also been called into question. For example, a 2008 report from the Association of Academic Health Centers called attention to some of the problems created by the privacy rule contained in the Health Insurance Portability and Accountability Act (HIPAA), which was designed to protect patients' confidential medical records. According to the report, unintended consequences of HIPAA include "confusion for patients, misinterpretation by research participants, barriers to patient recruitment [into clinical trials], and burdensome administrative procedures that increase research costs." The report also found that the "goal of [patient] protection through informed consent is undermined by the complexity of consent forms that are required of patients and participants, which approach a level of incomprehensibility to average individuals."[10] Another problem arises from the fact that HIPAA rules were developed well before the emergence of contemporary social media. Many of the practices of open sharing that are well-accepted in the world of social media and that are proving to be useful in supporting greater communication among doctors and between doctors and their patients may run afoul of HIPAA regulations.[11]

The growing ubiquity of mobile devices is raising additional privacy concerns. Cell phones equipped with GPS have the ability to track the location of users who typically carry their phones with them at all times and keep them on constantly. As the number of "apps" on smart phones and other mobile devices has proliferated, so has the quantity of information that these apps collect, often without the knowledge of their users. Just who has access to this information is unclear. In 2010, *The Wall Street Journal* reported on an investigation of 101 smart phone apps that included games and other types of software for Apple iPhones and Android devices. The investigators found that "56 [of these apps] transmitted the phone's unique device ID to other companies without users' awareness or consent; 47 transmitted the phone's location in some way; [and] five sent age, gender and other personal details to outsiders."[12] The *Journal*'s reporters also found that many of these apps did not disclose the types of information that they were collecting or the identities of the third parties with whom this information was being shared.

In other cases, sensitive information collected offline—such as medical or credit records—is stored electronically and is made accessible online, presumably restricted to authorized parties. In fact, once any information can be accessed on the Internet, it is potentially available to unauthorized users. Data breaches can also occur when computers, hard drives or DVDs containing records with personal information are broken into, lost, stolen or when an individual who has legitimate access to confidential information chooses accidentally or deliberately to release it publicly.

Is Privacy Overrated?

Some years ago, Scott McNealy, then-CEO of Sun Microsystems, famously commented: "Privacy is dead. Get used to it."

In *Public Parts*, published in 2011, blogger Jeff Jarvis comes not to bury privacy but to praise the value of what he calls "publicness." Jarvis believes that one of the most distinctive contributions of the Internet is to vastly expand access to the public space, making it easier for people to find, communicate and collaborate with others with common interests. But in order to do this, people have to be willing to disclose who they are. According to Jarvis, the kids who are comfortable sharing online with others what adults might consider intimate details of their daily lives have it right.

This does not mean that privacy is obsolete, however. Jarvis sees privacy and publicness as two sides of the same coin; each is necessary to define the other. But Jarvis believes that traditional privacy advocates who consider privacy to be an absolute value requiring elaborate protections are missing the valuable opportunities available to those who are willing to redefine what they want to keep private and what they are comfortable sharing with others.

Jarvis does not look at privacy so much from a legal perspective as from a cultural and pragmatic perspective. He notes, for example, that the same Germans who were extremely upset at having the fronts of their homes appear on Google's Street View (going so far as to require Google to pixilate the images of homes of people who protested) are comfortable being nude in public co-ed saunas, which would be strange to many Americans.

Jarvis' goal is to persuade his readers that, as the subtitle of the book indicates, "sharing in the digital age improves the way we work and live." If this involves giving up some privacy, he believes the trade-off is worth it.

Unfortunately, sharing of user data without the user's knowledge or permission happens every day, and breaches of supposedly secure data occur with alarming frequency. Some incidents have been fairly spectacular. In April 2011, in what may have been the largest privacy breach to date, Sony reported that a break-in to its PlayStation Network resulted in the possible theft of names, addresses, birthdates, passwords and credit card numbers of 77 million users of its online game network.[13] A desktop computer stolen in October 2011 from an office in

Sacramento, California contained unencrypted records of more than 3.3 million patients of the Sutter Health Network.[14] It was recently discovered that information on some 20,000 patients treated at the Stanford Hospital emergency room had been openly available online for nearly a year, not as a result of a malicious hacker but rather of a series of inadvertent errors in how the data was handled by employees and contractors.[15] The release of thousands of State Department diplomatic cables in November 2010 by WikiLeaks is yet another example of the vulnerability of supposedly confidential and/or secret files to unauthorized disclosure. There is little doubt that these kinds of privacy breaches will continue to happen.

The Importance of Trust

U.S. Commerce Department General Counsel Cameron Kerry calls trust the "flagship issue" related to the future of the digital economy in the United States. Any threat to the privacy of users' information is likely to undermine their trust in the integrity and safety of their online activities. Kerry noted that in an exercise to generate both positive and negative scenarios for the future of broadband, the issue of trust was the one common element in all of the scenarios.

The Department of Commerce has been working actively on this issue. In December 2010, the Department's Internet Policy Task Force issued a "Green Paper" that attempts to make the connection between protecting privacy and the ability of the Internet to continue to act as an engine for economic growth.[16] The document argues that "strong commercial data privacy protections are critical to ensuring that the Internet fulfills its social and economic potential." The report attempts to reframe traditional privacy principles to make them more dynamic in keeping with the rapidly changing digital environment that continually generates new uses that raise novel issues. While calling on consumers to take more responsibility for protecting their own information, the report proposes that the Department of Commerce convene a broad-based "multi-stakeholder process" to seek consensus on a consumer-data-privacy bill of rights that will help make users more aware of what is potentially at stake and inform them of how their privacy is being protected.

One area where there has been a fair amount of action is in setting requirements for companies to notify customers when privacy breaches occur. According to the National Conference of State Legislatures, "forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information."[17] Not surprisingly, these laws are not uniform and can create uncertainty about which state's laws pertain to breaches that involve individuals in multiple states.

A key challenge to getting legislators and regulators to act more forcefully on these issues is uncertainty about the actual harm that comes from breaches of privacy, as well as the potential benefits from providing more robust privacy protection.

Threats to Intellectual Property

A third category of issues that arise from the shift to digital media and the growth of online networks has to do with the fate of intellectual property. The "digitization of everything" in a hyper-connected world has disrupted one content industry after another—music, print publishing, movies and television—and challenged their fundamental business models. Particularly difficult problems have been posed by the ease of making an infinite number of perfect copies of original materials as long as they are in digital form. The emergence of peer-to-peer technologies (such as BitTorrent) makes it possible for users to share large quantities of digital content without the need for any gatekeepers.[18] What some users may perceive as innocent "sharing" of content is viewed by publishers and copyright holders as illegal piracy that robs them of legitimate revenues.

The scale of illicit digital copying is hard to pin down precisely, but it is indisputably large. A 2007 study by the Institute for Policy Innovation concluded that "the unauthorized copying and distribution of motion pictures, sound recordings, business and entertainment software and video games cost the U.S. economy $58 billion in total output, cost American workers 373,375 jobs and $16.3 billion in earnings, and cost federal, state and local governments $2.6 billion in tax revenue."[19] In terms of music, the study found that piracy was responsible for $12.5 billion in losses annually.[20] A more recent study by the European-based

International Federation of the Phonographic Industry (IFPI) concluded that digital piracy is largely responsible for a 30 percent decline in global music sales from 2004 to 2009.[21] A 2005 report prepared by L.E.K. Consulting for the Motion Picture Association asserted that "piracy is the biggest threat to the U.S. motion picture industry" and was responsible for worldwide losses of $6.1 billion to the U.S. movie industry, 80 percent of which resulted from overseas piracy and 20 percent from domestic piracy. The report estimated that 62 percent of losses came from pirated DVDs, while 38 percent came from illicit downloading of movies over the Internet.[22]

Digital activists and free speech advocates argue that estimates like these are generally not based on rigorous analysis and may be exaggerated in order to justify more aggressive enforcement of copyright protection. In fact, the actual economic impact of piracy is difficult to measure, and it is unclear the extent to which unauthorized copying undercuts legitimate sales. But there is little doubt that illicit copying of digital content is widespread and poses a major challenge to traditional copyright protections.

Finding Remedies

We are all living in a connected world: there are already some two billion people—nearly 30 percent of the global population—who are connected to the Internet worldwide, and billions more are coming online rapidly. New technologies and new applications that increase the utility of the Net are certain to be developed.

As Charles M. Firestone, Executive Director of the Aspen Institute Communications and Society Program, noted, the Internet has become our global commons, with enormous potential for bettering the lives of the world's population. But if this is to happen, we need to address the multiple challenges posed by threats to security, privacy and intellectual property. Many of these challenges are global, but the United States—the place where the Internet began and where much of the key innovation is still taking place—is a critical venue for dealing with these issues.

To be sure, there is already an array of laws and regulations that attempt to address challenges such as these. But as new technologies spawn new uses and generate new threats, there is a continuing need for rules that keep pace with the changing environment. Just as the

Internet has disrupted the business models of many industries, so it has disrupted regulatory schemes designed to protect security, privacy and intellectual property.

As the 2011 Communications Policy Conference participants attempted to identify the areas of most urgent need for action within these three domains and considered possible solutions, they were reminded by FCC Public Safety and Homeland Security Chief Barnett that there are a number of environmental factors that condition and constrain the kinds of policy responses that are feasible.

First, the United States is an open society that places high value on liberty and privacy. This value can cut two ways: on one hand, it can supply a strong impetus for policies that provide stronger protections of privacy. On the other hand, the desire to protect individual privacy can conflict with efforts to reduce security risks that entail restricting the right to anonymity online or imposing more stringent requirements for individual authentication. A continuing source of controversy and debate will be the extent to which behavior norms in the online world should conform to those in the real world or whether much of the value of being online comes from the ability to act anonymously in ways that are not possible in the real world.

A second factor that will inevitably shape the development of new policies is the economic environment. The United States, along with most of the world, is gradually emerging (one hopes) from a catastrophic financial crisis of historic proportions. With millions out of work, with the economy growing slowly if at all and with businesses continuing to be reluctant to expand, we need to consider the extent to which businesses can be expected to make the financial commitments that may be needed to reduce security risks, strengthen privacy protections and safeguard intellectual property. Given the difficult economic environment, it may be more realistic to seek incremental solutions that move in the right direction but that do not require large-scale capital investments.

On the political level, it is clear that the United States has entered into a period of extreme partisanship on almost all issues, making it more difficult to reach compromises. In recent years, for example, instead of collaborating on the development of policies to govern new telecommunications technologies, a debate has emerged in Washington about whether any regulation of telecommunications is justified.[23] This kind of paralysis makes it harder for the government to act forcefully to reduce threats to security, privacy and intellectual property. At the same time, there is a legitimate argument to be made about the proper role of government in protecting individuals online. As Barnett asked: if people leave their pocketbooks open and get their money stolen, do we therefore need government standards for zippers?

Voluntary, marketplace-based solutions are generally preferable—at least as a first resort—to government action. According to Dorothy Attwood, Senior Vice President for Global Public Policy for The Walt Disney Company, because companies are protective of the value of their brands, they do have an incentive to "make at least some nod" to acknowledging security concerns.

However, the extent to which the marketplace, on its own, is capable of developing and enforcing effective policies to protect users remains an open question. As Attwood notes, the most glaring market failures in protecting security and privacy are in areas that are not easily addressed by individual companies but require broader collaboration. For example, there is currently no incentive for firms to develop a single, interoperable "trusted online environment" for consumers, even if such an environment would be of substantial benefit both to consumers and the firms that serve them. One useful role that the government can play, short of imposing new rules, is to act as a catalyst or convener of industry players to encourage them to act jointly.

Finally, in terms of the realities of the consumer environment, many of today's users are largely unaware of the risks that they face online and therefore lack the motivation to change their behavior to make themselves less vulnerable. For example, numerous studies have shown that users (even users who might be considered relatively sophisticated) tend to choose passwords that are easy to remember but are also easily guessed by hackers.[24] The potential damage from the unauthorized disclosure of password information is magnified by another common practice—the use of the same password for multiple services.

Users often fail to adopt readily available practices that would make them more secure. According to Alan Davidson, Director of Public Policy for the Americas for Google, when his company developed a relatively simple two-step authentication process for access to Google accounts that significantly increased user security, almost no one bothered to make use of it.

All of the blame for security breaches cannot be placed on users, however. Companies that hold user information contribute to the likelihood of problems arising when they fail to employ best security practices. Marc Rotenberg, Executive Director of the Electronic Privacy Information Center (EPIC), suggested that Sony bears responsibility for the PlayStation data breach because it kept outdated information available online and failed to keep the information in encrypted form. The criticism that Sony received for its failure to protect the personal information of PlayStation users demonstrates the cost to companies of failing to establish meaningful privacy safeguards.

Reducing the threats to online activities in order to create a trusted, safe environment is an ongoing effort that will almost certainly involve making all parties—users as well as providers—part of the solution rather than indifferent, but not necessarily innocent, bystanders.

Policy levers. A variety of policy levers are available for updating and strengthening the rules of the digital road (see table below). They range from voluntary individual or collective actions by industry participants (or users themselves) to the development of new legal sanctions targeted against bad behavior. These six types of levers are not independent or mutually exclusive; they can be used in various combinations as responses to specific policy issues. Some of these levers (such as tax policy) are unique to government; others can be used by a variety of public and private sector participants.

First, in terms of ***institutions***, options include either reforming an existing institution to respond to a changed environment or, when necessary, creating new institutions that can provide new types of protection.

Next, there are many types of ***rules*** that can be developed to regulate security practices, including rules that prohibit specific types of risky activities, rules that assign liability to various parties for actions (or failures to act) that threaten security and rules that provide mechanism for the enforcement of policies or penalties for violating policies. There are also rules that identify types of behavior that trigger corrective action and others that specify the structure of markets intended to lessen security risks. Finally, there are international treaties that bind different countries into following similar policies related to security protection.

Third, ***money*** represents a potentially powerful policy lever, either in terms of the ability of the government to stimulate particular types of actions through the appropriations process or through the government's ability to promulgate specifications for services it purchases for itself through its procurement process (large companies also have the ability to influence behavior through their procurement policies). And, of course, tax policy is often used by governments to either encourage desired behaviors through targeted incentives or to discourage undesired behaviors by imposing added costs.

Fourth, the government can influence behavior in a less intrusive way by collecting and distributing ***data*** that is helpful in increasing knowledge about the actual dimensions of a problem or the extent of its impact. The government can also collect data that provide benchmarks to enable industry participants to measure their performance against their peers. And data can

Potential Policy Levers

1. Institutions

- Reform of current institutions
- Creation of new institutions

2. Rules

- Prohibitions
- Liability
- Standards
- Enforcement/Penalties
- Triggers
- Market structure
- Treaties

3. Money

- Appropriations
- Procurement
- Tax policy

4. Data

- Collection
- Distribution
- Benchmark
- Trigger

5. Education

- Government
- Non-Governmental Organizations
- Incentives for private sector action

6. Voice

- Framing
- Convening

be used to develop quantitative indicators to trigger remedial action when a particular threshold is reached. The reliability and value of such data can be enhanced by the establishment of standards—either voluntary or regulatory—governing when breaches need to be disclosed.

Education can increase awareness of security issues and/or teach specific security enhancing skills. Education can be provided directly by the government, or it can support educational initiatives by nonprofit non-governmental organizations or it can provide incentives to the private sector to develop educational programs. Several recommendations in this report call for educational campaigns aimed at individual users.

Finally, the government can use its ***voice*** to call attention to an issue by framing it in a way that highlights its importance and urgency. And rather than acting directly, the government can convene groups of key industry players and encourage them to take action to protect security.

With these alternatives in mind, the participants of the Aspen Institute Communications Policy Conference considered what policy initiatives were most urgently needed in the areas of security, privacy and intellectual property to create a new and more effective set of rules for the digital road.

Addressing Security Threats

The starting point for consideration of issues related to security is the premise that the Internet has a vast potential for individuals, for companies and for government to foster innovation, education, free expression, knowledge creation and sharing, commerce and communications. However, that potential is threatened by weaknesses in data protection as well as in the transmission of information and in the functionality of the Internet itself. The importance of the Internet and the realities of its vulnerability provide a strong rationale for action to better protect security of the Net and its users. But what actions?

Departing somewhat from prevailing discussions of cybersecurity, which tend to focus on specific technical fixes, the approach recommended here is designed to be *flexible* enough to evolve with changing circumstances; *simple* enough to be relatively easy to sell to other countries, whose cooperation may be critical to the effectiveness of an initiative; and *graduated*, so that different levels of security can be applied to different levels of threat. Finally, the recommendations are directed at both public and private sector players, rather than focusing solely on government actions in order to avoid over empowering national governments that have the potential of acting in ways that stifle other important values like openness, free speech or innovation in the name of protecting security.

A useful way to determine what types of action are needed is by constructing a "threat matrix" that shows the key categories of users and then identifies the types of security threats that are of greatest concern to each category. The table below provides this type of matrix. Users are divided into three broad categories: first, the government and "critical users" (e.g., operators of the country's power grid or the air traffic control system); second, non-critical business enterprises that depend, to a greater or lesser degree, on the Internet to carry out their activities; and, third, individual consumers who increasingly rely on the Internet for everything from entertainment to communicating with friends and family to managing their financial affairs. The two primary types of security concerns are related to threats to *data* (which is closely linked to privacy concerns addressed in the following section) and threats to the network's *functionality*, which hold the potential to disrupt organizations' or individuals' online activities.

Security Threat Matrix of Problematic Behaviors

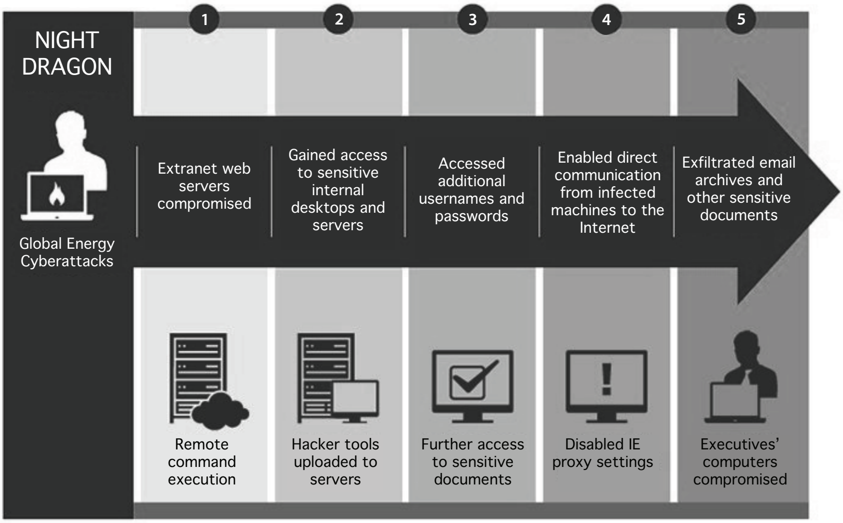
	Government/Critical Infrastructure	Commercial Enterprises	Individuals
Threats to data	Loss of national security data	Loss of business and customer data	Loss of sensitive personal data (e.g., financial, medical)
Threats to functionality	Loss of ability to operate critical infrastructure (e.g., power, financial services, flight control)	Loss of ability to operate or provide vital business functions	Service outage
Ease of use	Not applicable	Not applicable	"Digital hygiene" and Interconnected IDs

This matrix shows that the magnitude of security threats varies considerably according to the type of user. The most serious threats are related to government and critical infrastructure uses where security breaches could damage national security and/or have a major impact on large sectors of society. Fortunately, users in this category are typically large and relatively sophisticated organizations that have the resources and the expertise to take steps to protect their security. In October 2011, for example, the White House issued an executive order calling for a number of actions intended to protect important government data in the wake of the 2010 WikiLeaks release of confidential government documents. The executive order called for such measures as disabling military computers to preclude unauthorized downloading of sensitive information and more active monitoring to detect suspicious activity on classified computer systems—steps described by one security expert as "relatively elementary procedures [that] should have been in place [prior to the WikiLeaks breach] and were not."[25]

Even though these critical parties have substantial resources they can devote to protecting their security, the fact that they are heavily dependent on the Internet to provide them with national and global connectivity means that they do not have the ability to control all aspects of their data communications. In fact, it is with this group of users that the contradiction is most dramatic between the Internet's culture of openness and trust and the needs of responsible public and private sector entities to safeguard highly sensitive information as well as the operation of critical infrastructure systems.

And it is clear that serious vulnerabilities remain. In 2009, Google disclosed that it had been the target of a sophisticated cyber attack dubbed "Operation Aurora" that is presumed to have originated in China. After Google's announcement, a number of other high-tech companies revealed that they had also been targets. In late 2009, the global gas and oil industry was the subject of a broad attack named "Night Dragon" (see figure below). According to the 2011 Georgia Tech review of cyber threats, "The adversaries behind these attacks were able to exfiltrate [i.e., steal] design schematics and sensitive field negotiations, … [which] represent a company's crown jewels."[26]

Anatomy of the Night Dragon Attack, 2009


NIGHT DRAGON
Global Energy Cyberattacks
1
2
3
4
5
Extranet web servers compromised
Gained access to sensitive internal desktops and servers
Accessed additional usernames and passwords
Enabled direct communication from infected machines to the Internet
Exfiltrated email archives and other sensitive documents
Remote command execution
Hacker tools uploaded to servers
Further access to sensitive documents
Disabled IE proxy settings
Executives' computers compromised

Source: Anatomy of the Night Dragon Attack, 2009. Provided by McAfee, Inc. Available at: http://blogs.mcafee.com/wp-content/uploads/2011/02/Diagram_Anatomy_of_a_hack_final-1024x667.jpg

Some experts believe that Internet-based threats to critical data and critical functions are so severe and difficult to defeat that the most prudent strategy is to move these functions off the Internet entirely. Richard Clarke, who served as security advisor both to President George H.W. Bush and President Bill Clinton, points out that the sophistication of "cyberwar" attacks has been increasing faster than our ability to counter them, with the result that "the advantage has shifted to the offense." To counter this threat, he argues that we need to create a new infrastructure for critical applications that is "either physically separated from existing infrastructure or [uses] a different set of protocols from the TCP/IP now underlying the Internet and associated networks."[27] The participants in the Aspen Institute Communications Policy Conference did not endorse this alternative, but they did identify several measures to better protect the security of the nation's critical infrastructure (see Recommended Actions).

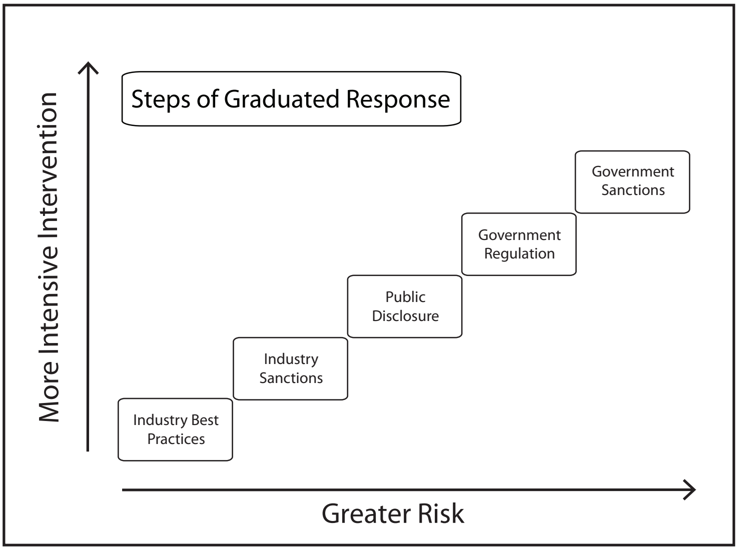
Non-critical enterprises fall in the middle in terms of both the potential consequences of a security breach and their capabilities to protect themselves. Sony and its PlayStation Network would certainly fall in this category, since it would be difficult to argue that the PlayStation Network is part of the nation's critical infrastructure. Even though the actual harm to the 77 million subscribers whose data was compromised by the 2011 break-in remains uncertain, the incident illustrates how large the scale of such breaches can be.

Individual users generally rank lowest in relation to security threats. Reed Hundt, former Chairman of the FCC and Principal at REH Advisors, noted that the prevailing attitude toward individual users, at least in the United States, is "YOYO" ("You're On Your Own"). Using the Internet is still viewed as a voluntary choice, and users are afforded few rights if the systems they use break or are unavailable, or if their personal data is compromised. Still, as more and more of the country's commerce and other vital activities move online, the potential for disruption of one's personal life as the result of the theft (or even the corruption or lack of availability) of sensitive personal information is substantial.[28] And if enough ordinary users should decide to boycott the Internet because of fear of the consequences of security breaches, the impact would be significant.

Moreover, as noted earlier, this category includes a number of particularly vulnerable groups—the young, the elderly, the poor, those with low literacy skills—who may well need special protection. And many individual users, even those who might be generally considered relatively sophisticated, are not particularly knowledgeable about the cyber threats they face; nor are they strongly motivated to take greater responsibility for their online behavior. EPIC's Rotenberg proposed that in protecting the security of individuals, it makes more sense to build in safeguards "under the hood" rather than just putting more information about potential vulnerabilities "on their dashboards." The key point is that more of the privacy safeguards need to be built-in as defaults, as many user settings (the "dashboard") are confusing.

A good way to decide which policy levers are appropriate for a particular security issue is to use a risk management analysis that provides for a series of graduated steps depending on the severity of the threat and the magnitude of the risk involved (see figure below). Such a tiered

Steps of Graduated Response to Threats



scheme would encompass remedies that range from purely voluntary responses to strong government action.

The least intrusive response, appropriate for the least critical threats, would be for industry participants to identify and share best practices in security protection. A more aggressive response would be for industry members to get together and mutually agree to impose sanctions on those entities that fail to adhere to best practice or other standards. Beyond that, a legal requirement for public disclosure of breaches would involve a greater level of government action. Establishing regulations that specify means for security protection or imposing government-enforced sanctions for non-compliance with regulations would represent the highest levels of response, which should be reserved only for the most critical threats.

Recommended Actions

The potential for harm from unchecked security breaches is real and serious. According to Aspen Institute Communications and Society Fellow Blair Levin, if we fail to adequately address these threats, we could find ourselves "in the world of Mad Max"—not a pleasant prospect.

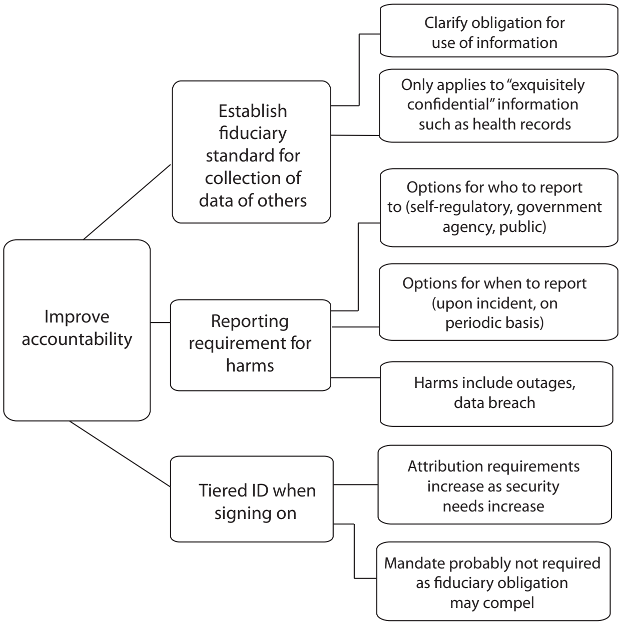
Given the continually changing nature of security threats, the development of policies to respond to these threats is an ongoing challenge. But at this point in time, there are at least six areas where action is called for to strengthen security protection. To a large degree, these recommended actions are intended to address vulnerabilities created by the open architecture of the Internet while attempting to preserve the benefits provided by that openness. While all users are ultimately responsible for their own security, it is realistic to recognize that users need help.

Recommendations for Strengthening Security Protection

1. Improve accountability for security.
2. Facilitate forms of insurance.
3. Increase costs of bad behavior.
4. Improve supply chain security.
5. Improve security of border gateway protocols.
6. Improve consumer ease of use and promote “digital hygiene.”

Recommendation 1: Improve accountability for security. The first set of recommendations is designed to improve the accountability for protecting security through three specific policy initiatives. The first step would be to establish a clear “fiduciary standard” for information about others collected by third parties. The goal of this standard would be to clarify the obligations that third parties have when they have access to information from others. To limit the scope of this obligation—which would certainly entail new costs to the responsible parties—the obligation should apply only to information that is deemed to be “exquisitely confidential,” such as an individual’s personal medical records or important financial information.

Recommendation 1: Improving Accountability for Security

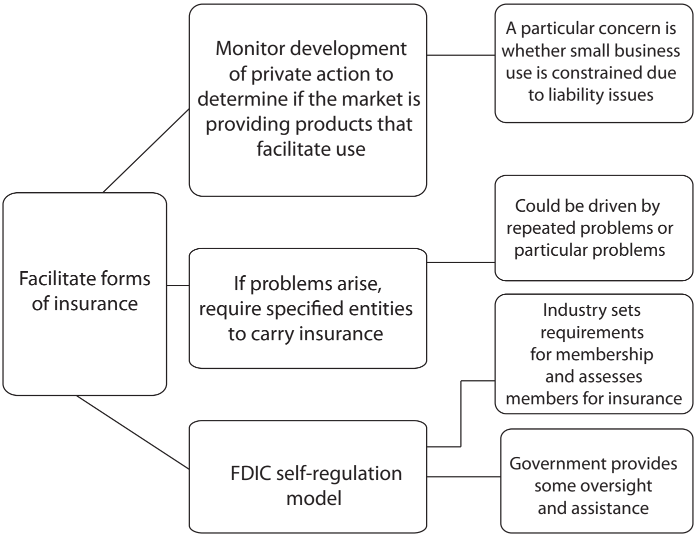

Improve accountability
Establish fiduciary standard for collection of data of others
Clarify obligation for use of information
Only applies to "exquisitely confidential" information such as health records
Reporting requirement for harms
Options for who to report to (self-regulatory, government agency, public)
Options for when to report (upon incident, on periodic basis)
Harms include outages, data breach
Tiered ID when signing on
Attribution requirements increase as security needs increase
Mandate probably not required as fiduciary obligation may compel

The second step for improving accountability would be to require that entities that serve customers on the Internet report any incidents that involve potential harm to users. "Harms" could range from service outages that deprive users of access to important resources to security breaches that result in unauthorized access to personal information about users. This initiative would entail defining who needs to report such incidents and to whom reports must be made (e.g., to customers, to the public, to a self-regulatory body or to a government agency). Rules will also be needed to specify when reports must be issued (e.g., on a regular schedule or immediately following the occurrence of a breach). The need to clarify the timing of disclosures has been demonstrated by controversies over what have been characterized as "delays" in reporting breaches by responsible parties in a number of recent incidents.

The third initiative to improve accountability would be to develop "tiered ID requirements," under which the level of authentication required for users logging onto online services would be directly proportional to the sensitivity of the data or the activity involved. Non-critical services could continue to allow users wide latitude in picking a password (or no password at all), while critical services would need to require safer passwords, more frequent changes to passwords, or even multi-step login procedures. While the first two initiatives would almost certainly require government action, this step would not: if clear fiduciary obligations were established, they would likely compel responsible parties to develop appropriately rigorous mechanisms to prevent unauthorized access to their services.

Recommendation 2: Facilitate forms of insurance. We know that use of the Internet has been growing rapidly. But are the concerns over potential costs that might be incurred by victims of security breaches—particularly among small businesses—preventing the Internet from growing even faster? Given that it is reasonable to assume that security breaches will continue to occur, would the availability of insurance against the risk of security losses inspire greater confidence in the safety of being online, thereby spurring greater growth?

Recommendation 2: Facilitating Forms of Insurance

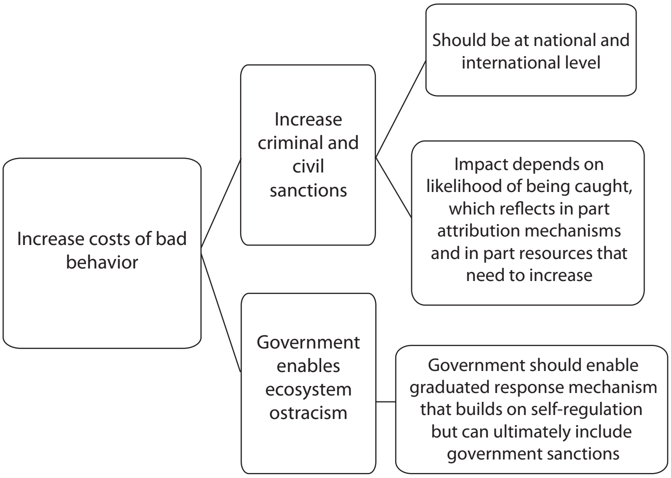

Facilitate forms of insurance
Monitor development of private action to determine if the market is providing products that facilitate use
A particular concern is whether small business use is constrained due to liability issues
If problems arise, require specified entities to carry insurance
Could be driven by repeated problems or particular problems
FDIC self-regulation model
Industry sets requirements for membership and assesses members for insurance
Government provides some oversight and assistance

Since we do not currently know the answers to these questions, a first step should be to monitor developments in the field in order to see if the market, on its own, is responding to this challenge by providing the products necessary to facilitate robust use of the Internet.[29] If the marketplace were functioning well on its own, no action would be needed. If it is not, however—if there is clear evidence that usage is being constrained by the unavailability of insurance—then action should be taken. A good model for such action is the Federal Deposit Insurance Corporation (FDIC), the entity that has protected individual bank accounts since it was founded in 1933. In cases where banks fail or their assets are unexpectedly depleted (e.g., through some sort of fraud), the FDIC stands ready to make up for any losses by account holders up to a specified limit. The FDIC is "an independent agency of the federal government;" its mission is to "preserve and promote public confidence in the U.S. financial system by insuring deposits in banks and thrift institutions." It receives no support from taxpayers but is funded entirely by dues paid by member banks.

Following an FDIC model, if there were a perceived value for offering insurance against damage from security breaches, participants in the industry—with some oversight and support from government—could get together and decide what would be insured, set requirements for membership in an insurance pool, collect fees from members to fund the pool and act as agents to settle users' claims as they arise.

Recommendation 3: Increase Costs of Bad Behavior. Because of the rapid rate at which the Internet has evolved, penalties for unauthorized breaches of security have not kept up with the growing magnitude of the problem. Moreover, laws governing data security are far from consistent domestically and internationally. Given the serious costs of insecurity, there is an evident need to increase both civil and criminal sanctions against damaging security breaches. To be effective, these sanctions will need to be enforced both nationally and internationally. And the effectiveness of sanctions will depend to a considerable degree on the perception among perpetrators of the probability that they will actually be caught—which is likely to remain low as long as the Internet provides few mechanisms to establish the identity of users.

Recommendation 3: Increasing the Costs of Bad Behavior

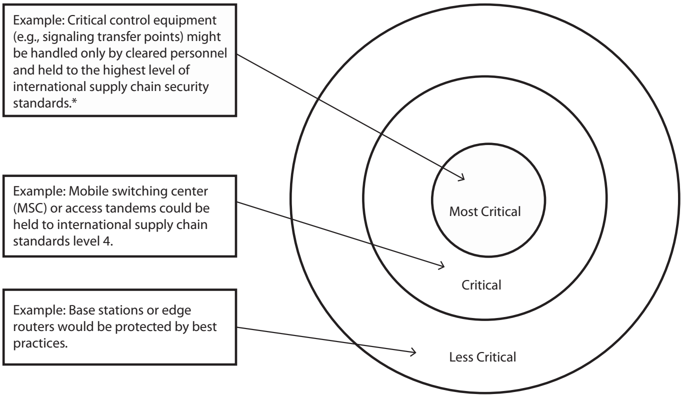

Increase costs of bad behavior
Increase criminal and civil sanctions
Should be at national and international level
Impact depends on likelihood of being caught, which reflects in part attribution mechanisms and in part resources that need to increase
Government enables ecosystem ostracism
Government should enable graduated response mechanism that builds on self-regulation but can ultimately include government sanctions

As is the case with other recommended initiatives, a self-regulatory model is preferable to direct government action. For example, the government could support development of mechanisms that enable "ecosystem ostracism"—that is, the exclusion from the Internet of bad actors by collaborative industry action. The government could regard such actions as the preferred first response to security problems and reserve legal sanctions for the most serious or recurring violations.

Recommendation 4: Improve supply chain security. One way to look at the Internet is as a supply chain that includes multiple parties and systems that play a role in delivering content from a supplier at one end to a user at the other end. As noted earlier, the Internet is not a single entity but rather a "network of networks" that is made up of many independent elements linked through a set of mutually agreed-on standards and protocols. Most of the time, all of the components operate as intended. But the possibility always exists that the security of the network's operation or the integrity of data passing through the network can be compromised through insecurities that are introduced, either intentionally or inadvertently, at some point in the network.

A risk management analysis of the Internet's structure reveals that not all components of the Internet are equally important in maintaining the integrity of its operation (see figure below). A finite set of elements is, in fact, so critical to the functioning of the network that it deserves special attention. These critical elements clearly merit the highest level of protection. As the criticality of elements to the overall functioning of the network decreases, it is appropriate to apply less rigorous methods to protect their security.

Risk-Management Analysis of Internet Supply Chain Components

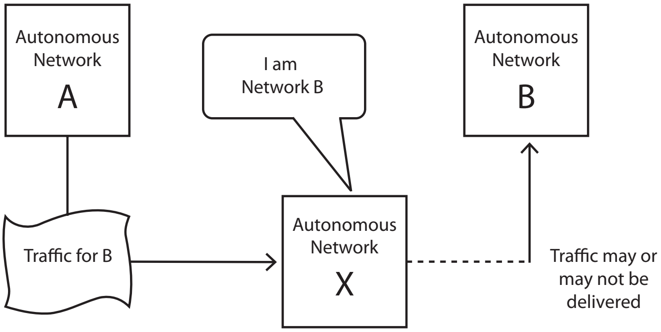

Example: Critical control equipment (e.g., signaling transfer points) might be handled only by cleared personnel and held to the highest level of international supply chain security standards.*
Example: Mobile switching center (MSC) or access tandems could be held to international supply chain standards level 4.
Example: Base stations or edge routers would be protected by best practices.
Most Critical
Critical
Less Critical

**e.g. ISO/IEC 1508, Common Criteria for Information Technology Security Evaluation Level 7*

Thus, in the case of the most critical components, such as network signaling transfer points, it makes sense to restrict access to them to individuals with high-level security clearances and to expect that their management would be held to the highest level of international supply chain security standards (e.g., CC Level 7 of ISO/IEC 1508, Common Criteria for Information Technology Security Evaluation[30]). Less critical elements, such as mobile switching centers or access tandems could be held to a lower standard of security, such as CC Level 4. For the least critical elements of the supply chain, such as components that typically operate on the edges of the network, it may be sufficient to rely on voluntary protection by ensuring that best practices and standards are followed.

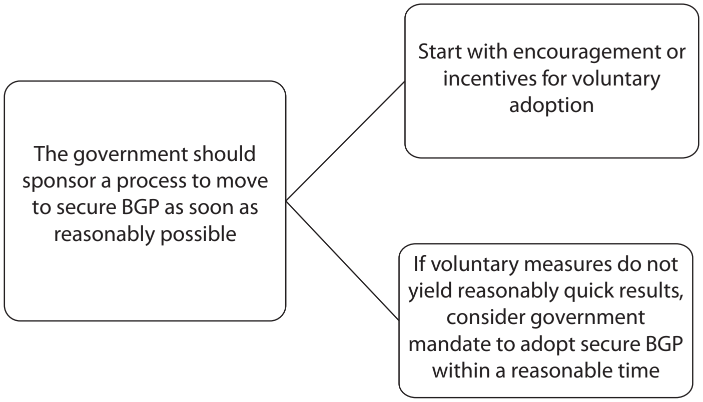
Recommendation 5: Ensure Security of Border Gateway Protocols. As discussed above, the border gateway protocol (BGP) is the set of rules that controls the core routing of traffic on the Internet. Because this routing is based on trust between interconnected but separate networks, it is susceptible to either inadvertent or intentional (malicious) misrouting. In this simplified example, misusing the established BGP, Network X "pretends" to be Network B and hijacks traffic that was intended for Network B, resulting in possible failure to deliver that traffic to its intended destination:

Route Hijacking



Although misrouting of traffic is a potential threat to all Internet users, there is currently little incentive for a competitor to act unilaterally to solve the problem. Securing BGP will require investment in privately held assets by the firms that operate the networks that make up the Internet. But no individual entity wants to be the first to act, and independent action to adopt secure BGP will not, in fact, definitively solve the problem. Because of the decentralized, heterogeneous nature

Recommendation 5: Securing Border Gateway Protocols



The government should sponsor a process to move to secure BGP as soon as reasonably possible

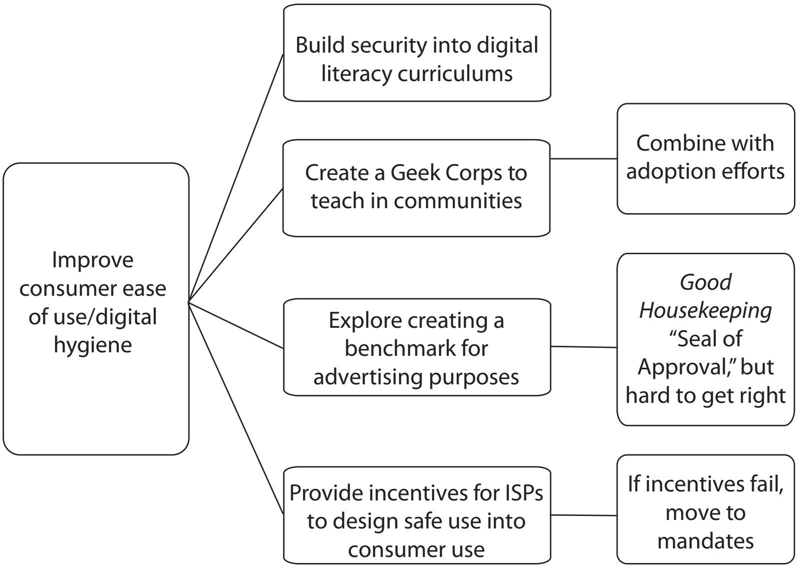
Start with encouragement or incentives for voluntary adoption

If voluntary measures do not yield reasonably quick results, consider government mandate to adopt secure BGP within a reasonable time of the Internet, collective action is required to defeat this kind of disruptive route hijacking.

Given this stalemate situation, the government can play a useful role in sponsoring a process that would move all industry participants to take measures to expeditiously secure BGP. In keeping with a preference for voluntary action, such an initiative could begin with the government acting as a convener or encouraging or providing incentives for such a collaborative action by the private sector. However, if voluntary action does not lead to meaningful results in a reasonable period of time, the government should consider issuing a mandate to the industry to adopt secure BGP within a specified period of time.

Recommendation 6: Improve consumer ease of use and promote "digital hygiene." The final recommendation related to security focuses on the end user. This recommendation includes several specific steps to increase consumers' awareness of security threats and the actions that they can take to protect their own security.

Recommendation 6: Improving Consumer Ease of Use and Promoting "Digital Hygiene"


Improve consumer ease of use/digital hygiene
Build security into digital literacy curriculums
Create a Geek Corps to teach in communities
Combine with adoption efforts
Explore creating a benchmark for advertising purposes
Good Housekeeping "Seal of Approval," but hard to get right
Provide incentives for ISPs to design safe use into consumer use
If incentives fail, move to mandates

Over the years, there have been repeated calls, in Aspen Institute conferences and beyond, for the broader adoption of so-called "digital literacy" curriculums. For example, the 2009 Knight Commission on Information Needs of Communities in a Democracy called for the integration of "digital and media literacy as critical elements of education at all levels."[31]

Although there is no universally accepted definition of digital literacy, it is usually focused on building individuals' skills in finding, evaluating, using, creating and sharing information online. Teaching appropriate "netiquette" is often part of digital literacy curriculums, but these programs do not always give attention to issues directly related to security, such as good practices in picking and protecting passwords or being alert to the dangers of spam-based phishing attacks. As long as the Internet remains an inherently dangerous place, it makes sense to incorporate security into digital literacy curriculums.

Schools and libraries have been the primary venues for digital literacy education. Another frequently made recommendation at Aspen Institute meetings and elsewhere is the creation of a "Geek Corps" or "Digital Literacy Corps" to take this kind of education beyond these institutions into the broader community. Such a corps could focus particularly on reaching the most vulnerable members of the population, including those with low education levels or limited English skills or older adults who were not brought up with the new technologies.

Another useful initiative to raise awareness of security issues would be to create a *Good Housekeeping*-type "Seal of Approval" that could be used in advertising and other communications only by those parties that conform to an agreed-on set of best security practices. Such a seal could be created by an independent entity that wins wide support from industry participants or by a consortium of these participants themselves.

Finally, although consumers certainly bear ultimate responsibility for their own security, it is not realistic to put the entire burden for acting safely on them. ISPs and other Internet participants can play an important role in improving consumer security by making it easier for their customers to follow good security procedures (e.g., making the default choice "opt out" rather than "opt in" to security measures). The government could encourage action by providing incentives—perhaps in the form of tax breaks or credits—to encourage ISPs to build in safe use mechanisms into their services ("security by design"). And if incentives fail to yield enough progress, then government should consider mandating better security measures.

Addressing Privacy Threats

Breaches of privacy can result in various kinds of harm. Misuse of an individual's sensitive personal data poses a risk to that person's economic security. Privacy breaches can also potentially limit political freedom and restrict the ability to speak freely.

Any consideration of recommendations to update privacy protection must also acknowledge that data collection is a vital contributor to commerce, to civic life and to innovation. Proposed policies need to balance protecting against the potential harms that can result from unwanted or excessive data sharing with preserving the real benefits of data sharing.

It is also important to recognize that privacy concerns are not new, but they have been exacerbated by new threats that have been enabled by new technologies. Among these new developments are the increasing speed and extent of information proliferation and the persistence of digitally stored information that may have seemed ephemeral at the time it was created (e.g., postings on social networks). The growing powers of data aggregation and "data mining" that make it possible to connect dots that could not previously have been connected also pose new threats to privacy.

Contributing to concern about privacy is a lack of consumer awareness of what is actually happening to their data—who is being allowed access to their information and how it is being used—and a lack of industry awareness of issues related to protecting privacy. A final concern about the current state of privacy protection is the existence of multiple privacy regimes (e.g., HIPAA for health care, the Gramm-Leach-Bliley Act for banking, FTC regulation of children's privacy) as well as different policies in different states and different countries that can lead to confusion about when privacy is protected, where data can flow and where businesses can operate.

Recommended Actions

The simplest, most straightforward way to address these concerns is through wide adoption of a single comprehensive framework that will provide clarity for individuals and industry members about their rights and responsibilities in terms of privacy protection. A comprehensive framework can help to overcome the troubling fragmentation of privacy protection schemes domestically and internationally.

Fortunately, there is a well-established basis for such a framework. The Fair Information Practices (FIPs) discussed earlier have been developed by a number of different bodies over a period of several decades. The first such set of practices was promulgated nearly 40 years ago in a seminal report titled *Records, Computers and the Rights of Citizens* published in 1973 by the U.S. Department of Health and Human Services. The practices have been refined and extended since then by several federal agencies and international bodies (which often refer to them as Fair Information Practices and Principles or FIPPs)[32].

The following set of practices represents a synthesis of existing FIPs frameworks, based on an initial draft offered by Stefaan Verhulst, Chief of Research for the Markle Foundation.

The FIPs framework is intended to be comprehensive: it is designed to cover all critical aspects of privacy, both offline and online, from how information is initially collected through how the information is protected and used and how compliance is monitored. A fundamental purpose of the practices is the empowerment of individuals to maintain awareness of and control of their own information. While each of these practices is important, the value of FIPs depends on their being seen as a single, coherent package, rather than a collection of separate, individual practices.

Since not all data is equal in sensitivity, there needs to be flexibility in how FIPs are applied. FIPs would apply only peripherally if at all to information that is not personally identifiable or that is widely understood to be publicly available, while information that is "exquisitely confidential" (as described in the previous section) would logically call for the most rigorous application of FIPs.

FIPs can be used in a number of different ways. First, the practices can be used to inform new legislation—to ensure that it takes into

Synthesis of Fair Information Practices: A Comprehensive Framework for Protecting Privacy

1. **Openness and Transparency**

   Is it easy to locate and understand what policies are in place, how they were determined and how to make inquiries or comment?

2. **Purpose Specification and Minimization**

   What is the purpose of gathering these data? Are the purposes narrowly and clearly defined? Are there criteria and procedures for deletion of personal data?

3. **Collection Limitation**

   Are only those data needed for the specified purposes being collected, and are subjects informed of what is being collected?

4. **Use Limitation**

   Will data be used only for the purposes agreed to by the subjects?

5. **Individual Participation and Control**

   Can an individual find out what sensitive/important data has been collected and exercise control over whether and with whom it is shared?

6. **Data Integrity and Quality**

   How are data kept current and accurate? What mechanisms are available for individuals to check and correct data?

7. **Security Safeguards and Controls**

   How are the data secured against breaches, loss or unauthorized access?

8. **Accountability and Oversight**

   How is compliance with the policies monitored, and how is the public informed about violations?

account all of the key aspects of privacy protection. FIPs can also be applied to corporate and industry codes of conduct, either as a guide to formulating such codes or as a checklist to assess their adequacy. FIPs can even be used to guide building privacy protection into the creation of new products and services (so-called “privacy by design”).

To assess the relevance and value of FIPs to the current, rapidly changing information environment, participants developed a list of emerging privacy issues and three of the most critical selected for testing against the practices. Some 15 issues were initially identified. Some of these are quite new (e.g., mobile issues, social media, facial recognition), while others represent the evolution of older issues (e.g., government access to information, secondary use of data).

The 15 emerging issues are:

1. *Evolving definition of personally identifiable information (PII).* To what extent do new technological capabilities expand the definition of PII?

2. *Mobile privacy issues.* Are new privacy rules needed for the new environment created by the proliferation of multifunction mobile devices?

3. *Data analytics/data brokers.* What privacy standards should apply to parties that do not collect data directly but rely on data collected by others?

4. *Data breach notification.* Should standards for notification be uniform nationally or determined by individual states?

5. *Online identification.* Should disclosure of actual personal identity be legally mandated?

6. *Data retention.* What policies should govern retention and deletion of personal data?

7. *Interoperability among companies.* To what degree should privacy practices be uniform across companies?

8. *Government access.* What are the appropriate standards for government access to personal data in the digital age?

9. *Social media.* Are new privacy protection rules or practices required for people (including children) active in social networks?

10. *Facial recognition.* What issues are raised by the growing power and pervasiveness of facial recognition technologies?

11. *Geo-location.* What issues arise from automatic, real-time tracking of mobile users' locations?
12. *Data portability.* Are rules needed to govern users' rights to extract and move their personal data and content from one site to another?
13. *Intermediary liability.* What obligations and liabilities do intermediaries bear for breaches of users' privacy?
14. *Offline data.* To what extent should rules for online and offline privacy protection be the same?
15. *Secondary use of data.* What rules are needed to protect the privacy of users' data when used for purposes that differ from original intent?

Participants explored the implications of the top three issues on the list in greater depth.

Evolving definition of personally identifiable information. Traditionally, it is the collection of information that can be linked to a specific individual—personally identifiable information (PII)—that triggers the application of FIPs. There is generally little concern about privacy in the handling of information that is truly anonymous or that has been made anonymous by stripping out any PII. Such anonymized data can be enormously useful in areas such as medical or economic research that depend on information on large populations.

However, computerized data analysis techniques are making it possible to carry out personal identifications that were not previously possible. In a study published in 2000, Latanya Sweeney, then a graduate student at Carnegie Mellon University, reported that a large portion of the population could be uniquely identified by a combination of a very small number of widely available characteristics through a simple computerized process of linking supposedly anonymized data with voter registration records. Using this technique, Sweeney found that fully 87 percent of the American population could be identified based on only three pieces of data: gender, ZIP code and date of birth. Even when location is just the community in which a person resides, it was possible to uniquely identify 53 percent of the population. The study concluded that "the practice of 'de-identifying' data [is] not sufficient to render data anonymous because combinations of attributes often combine uniquely to re-identify individuals."[33] The author also noted that legislatively mandated data on medical care that is collected and made publicly available in many states include listings that identify patients' genders, ZIP codes, dates of birth and ethnicities, all of which could be used to "de-anonymize" them.

Under the FIPs framework, data that is truly anonymous, i.e. not personally identifiable, is excluded from consideration. Also, reducing or eliminating the collection of personally identifiable data can reduce the obligation of companies under various privacy laws. This prospect should encourage companies that collect personal data to consider whether data can be anonymized, minimized, or routinely deleted. This also reduces risks that result from data breaches. As Marc Rotenberg of EPIC noted, a critical criterion for deciding what information to ask for should be, "If you can't protect it, don't collect it."

Mobile privacy. As noted earlier, an entirely new data environment is being created based on wireless mobile technology that is rapidly becoming pervasive and virtually indispensable for a majority of the population. Furthermore, the emergence of devices such as smart phones and tablets are blurring the lines between communications and computing, creating a potential source of confusion about what rules and standards should apply to mobile activities.

At present, there is little consensus about the application of FIPs in this environment, especially in terms of deciding where and when privacy protections should be applied and how stringent those protections should be. A complicating factor is the presence in the mobile marketplace of many small developers who are creating small apps for smart phones and tablets (as of July 2011, Apple's online App Store alone contained more than 425,000 apps for its iPhones and iPads). App developers, who may be young individual entrepreneurs, are often unfamiliar with privacy issues and lack the resources to develop and implement effective privacy policies for their apps. The result is the kind of common lapses in privacy protection—including the absence of required privacy notification statements—documented by *The Wall Street Journal.*[34] Further confusion arises from the fact that different app development environments (e.g., Apple IOS, Android, RIM, Windows Mobile) have different approaches to enforcing privacy standards. But even if these differences persist, they should all be based directly on adherence to FIPs.

Given the small screens of most mobile devices and the casual use of many apps, lengthy privacy policies are clearly inappropriate in the mobile environment. The Communications Policy Conference recommended the development of alternative means for disclosing privacy information that is better suited to this environment. One possibility would be a relatively simple, uniform system of icons that represent different levels of protection. Another promising option would be for the mobile industry to take the lead in developing a "privacy in a box" template that is demonstrated to be effective for users and that could be easily adopted by app developers.

Data analytics/data brokers and personal privacy. The increasing aggregation and analysis of data about individuals offer many potential benefits from increased knowledge, ranging from the development of more personalized marketing and advertising techniques to the more efficient delivery of services to the development of more effective medical treatments. But such aggregation and analysis also raise new issues about privacy protections. In many cases, data collected by one entity is shared with or sold to third parties that aggregate huge databases and add value through techniques such as data mining to produce valuable insights. In many cases, these third parties are invisible to users, who are unaware of where their information is going or how it is being used. This situation inevitably leads to concerns about the transparency of such entities and the ability of individuals to access their own data and correct it if it is erroneous—capabilities that are explicitly identified in the FIPs framework.

At a minimum, all entities that collect, analyze and use any type of personally identifiable information should be expected to act as good stewards of that information and to adhere to FIPs where applicable. Specifically, the original collectors of information should provide their users with notice and a choice whenever they transfer personally identifiable (or potentially identifiable) information about those users to data brokers.

Second, the Communications Policy Conference participants recommended the establishment of a portal that lists all data brokers, the kinds of information that they collect, and offers tools that enable consumers to access and correct information about themselves. The level of access and the extent of redress available should be proportional to the sensitivity of the information in question.

Finally, data brokers should be obligated to inform on an annual basis each person whose information they have about that information.

Protecting Intellectual Property

Just as with privacy and security, protecting intellectual property (IP) in the Internet age is a matter of achieving optimal balance between multiple interests and multiple rights: for example, the issue calls for a tricky balancing act between the rights of copyright holders to protect their intellectual property and the values of openness and creativity spurred by new technologies. Also in play are the rights of intermediaries, who may be called on to enforce copyright protection. Almost all remedies that have been proposed or implemented have been criticized either for being so cumbersome as to stifle innovation and speech or for being too weak to provide sufficient protections for IP (or both).

In seeking to identify specific rules of the road to protect IP, the Communications Policy Conference participants adopted a strategy of identifying the most significant gaps in current protection schemes and then proposing responses to address those gaps. As Joe Waz, Senior Fellow at the Silicon Flatirons Center at the University of Colorado at Boulder, noted, the primary rationale for providing protection for IP is to protect the incentive and ability of creators and innovators to create and innovate online. From a practical point of view, potential remedies should be assessed against multiple goals, which include:

- Protecting copyrighted content
- Protecting creativity and fair use (which can generate new IP)
- Enabling innovation (e.g., new business models, new technologies)

- Protecting users' privacy, civil liberties, due process and the principal of openness
- Promoting user understanding and acceptance of protective measures

In fact, devising appropriate remedies is a multidimensional challenge: all of these goals can rarely be served equally by a given remedy, which inevitably involves trade-offs among them. With these caveats in mind, the participants recommended three types of actions intended to address areas of current weakness in IP protection schemes.

Recommendations for Addressing Weaknesses in Current Intellectual Property Protection Schemes

1. Target rogue websites.
2. Improve consumer/user education.
3. Encourage greater availability of digitized content on more platforms.

Recommendation 1: Target rogue websites. The first recommendation focuses on the need for a better set of procedures to deal with "rogue websites," such as The Pirate Bay (see sidebar) that play a major role in enabling illicit sharing of copyrighted materials. Past efforts to combat these sites have been hampered by the lack of tools to effectively block users' access to sites whose primary purpose is to facilitate unauthorized access to legally protected content. To hamper the operations of rogue sites, copyright holders have resorted to efforts to convince third parties—such as ISPs that provide connectivity, banks or credit card companies that provide billing capabilities or agencies that provide advertising—not to offer their services to these sites, thereby depriving them of revenue. In fact, intermediaries like ISPs and banks are reluctant to act as "judge and jury" in deciding which sites should or should not be blocked or have access to their services. As a result, achieving meaningful actions against rogue sites can be protracted and hit-or-miss.

Identifying and sharing best practices in dealing with illicit content sharing would help financial services companies and advertising pro-

The Pirate Bay

Established in Sweden in 2003, The Pirate Bay (TPB) website has been described by the *Los Angeles Times* as “one of the world’s largest facilitators of illegal downloading” and “the most visible member of a burgeoning international anti-copyright or pro-piracy movement.”[35] From a technical standpoint, The Pirate Bay allows users to search for others who are willing to share digital files, including copyrighted materials, using the peer-to-peer BitTorrent protocol.

The site provides access to more than 500,000 music tracks, television programs, movies, videogames and computer applications. Despite repeated legal efforts to shut the site down, including a Swedish police raid on its offices in 2006 followed by criminal prosecution, the site has survived and continues to operate. In fact, as technology has evolved, TPB has become more decentralized, making efforts to restrict its activities more difficult. (Commenting on a recent action to block the site, one presumably contented user described the attempt as “just another useless effort at getting less traffic to TPB, one that will fail for sure.”[36]) As of the fall of 2011, The Pirate Bay was ranked by Alexa as the 82nd most popular website in the world in terms of traffic.

viders as well as content owners to develop a set of standards on when to cease doing business with rogue sites.

A stronger approach would be a process that would allow owners of intellectual property who believe they are being harmed by a specific site to go to a court with competent jurisdiction to seek an order to intermediaries to cease doing business with that site. Such a judicial process, which would require new legislation, would offer the protection of due process to sites that have been targeted for being blocked but would allow for relatively quick action. The recommended process would allow a court to issue the equivalent of a temporary restraining order against offending sites based on a strong prima facie case that 1) the plaintiff owns the copyright; 2) the copyright is being infringed; and 3) the owner is able to identify the infringer. Since this approach involves explicit legal action, it would alleviate intermediaries of the burden of having to decide independently when they should comply with requests from copyright holders to take action against rogue sites.

Such a process has been ordered by a court in Europe. In July 2011, in response to a request from six Hollywood movie studios, a British judge ordered British Telecom, a major ISP, to begin blocking access to a site that was "being heavily used for copyright infringement." According to a news report on the action, "The judge's order relied on the European Union's 2001 Information Society Directive, as implemented by the UK Parliament in 2003, that states that a court can grant an injunction against a service provider, where that service provider has actual knowledge of another person using their service to infringe copyright."[37]

A more controversial recommendation involved a similar process that would allow for temporary restraining orders aimed at major search providers, directing them to block links to sites found to be infringing on IP. In support for this proposal, it was noted that such a system is already in place in some countries for illegal child pornography sites. The supporters of this proposal noted that care would have to be taken to ensure that such a process would not be exploited by governments to limit citizens' free speech.

Google's Davidson noted that Google opposes using search as a mechanism to remove sites from the Internet's index. The company does comply with provisions of the U.S. Digital Millennium Copyright Act by blocking "certain kinds of speech," but it would be reluctant to block entire domains, since that could be construed as a form of prior restraint. Responding to concerns that any such process could be considered a form of censorship, Disney's Attwood commented that the proposal is designed to be "surgical," aimed specifically at sites with predominantly illicit content.

Recommendation 2: Improve consumer/user education. In the early days of personal computers, the casual sharing of software among friends and even business colleagues was relatively common. Eventually, through efforts of groups like the Software and Information Industry Association, the public developed an understanding that commercial software is protected intellectual property and that "software piracy" was, in fact, a crime. Then the Internet opened up an entirely new venue for sharing digital content. A culture grew up that tolerated "sharing" of this content, whether or not it was legally protected, while high-speed broadband connections simplified the process of sharing even very large files, such as full-length movies. And the Internet's tradition of anonymity provided convenient cover for those engaging in this behavior.

Even while legal and/or technologically based remedies to combat illicit sharing are being pursued, an effort to change consumer behavior needs to be part of the solution. The core message of a campaign to curb piracy should be that respecting intellectual property rights is important to maintaining a robust Internet ecosystem and promoting creativity. In fact, the Internet belongs to everyone, and everyone bears a share of the responsibility to keep it in good order. Illegal actions such as piracy threaten the openness of the Internet, which has been responsible for the innovations that have brought so many benefits.

Public media campaigns aimed such things as illicit drug and tobacco use have proved effective, and a similar campaign targeted at online piracy could be equally effective. In addition, media literacy curriculums should incorporate concepts of respect for intellectual property, as well as teaching good security practices. The development of balanced curriculum could be done through a voluntary, collaborative process involving key industry players as well as free speech advocates. The government could play a role in driving adoption of such a curriculum and could also sponsor a public service campaign against piracy. Finally, these topics could be included in the mandate of a Digital Literacy Corps, which was proposed in the FCC's National Broadband Plan[38] and described in a recent white paper issued by the Aspen Institute Communications and Society Program in conjunction with the Knight Commission on the Information Needs of Communities in a Democracy.[39]

Recommendation 3: Encourage greater availability of digitized content on more platforms. One reason that the illicit sharing of music and other types of content online was so rampant for many years was the lack of an alternative that would have made it simple and convenient to purchase content legally over the Internet. That began to change when Apple launched the iTunes Store in April 2003. The store worked well, because it was tightly coupled to Apple's iTunes software media player that was installed in millions of iPods and computers. The store greatly streamlined the process of finding and purchasing music online. (It was easy, for example, to listen to a short sample of any song before deciding to buy it, which then involved just a single "click" to complete the purchase.) The pricing of most songs at 99 cents was low enough to encourage impulse buys. Over time, the iTunes Store has also offered access to other types of digital content, including TV shows, movies, podcasts, apps and games, which now generate significant revenue.

Initially, all music in the store was protected by Digital Rights Management (DRM) software which restricted customers' ability to transfer what they had purchased to other media (e.g., from an iPod to a computer or a CD). However, in response to complaints from users, Apple decided to offer DRM-free music, and by 2009, DRM has been removed from 80 percent of the music in the store, a shift that has been accepted by almost all players in the music industry.

Although the iTunes store has not put an end to digital piracy, it has created a robust market where digital content can be legally sold. As of October 2011, more than 16 billion individual songs had been sold by the store, which has become the No. 1 music seller in the United States.[40] As Apple has introduced more devices capable of purchasing and playing music (first the iPod, then the iPhone, most recently the iPad), and other companies have followed Apple's lead by creating similar products, a thriving ecosystem of media players linked to media stores has grown rapidly and is now providing an attractive marketplace for creators of digital content of all kinds. As of 2010, online music sales by more than 400 licensed sites generated nearly one-third of total income of music publishers, and revenue from the online sale and rental of video content has been increasing steadily.[41]

The Walt Disney Company provides a good example of the value of a proactive response by a major content producer to the challenges and opportunities presented by new technologies. According to Disney's Attwood, the company has long been in the forefront of its industry in believing that greater returns come from embracing, rather than opposing, new technologies. Disney's willingness to pursue new options goes back at least to 1954, when by launching a weekly program titled "Disneyland" on the ABC network, the company was the first to break with the other major Hollywood studios in boycotting television by refusing to produce programs or release films for showing on TV. More recently, Disney was the first in its industry to provide content online and was the first studio to be on Apple's iPad. The value of the company as a role model was captured in a recommendation from the Communications Policy Conference that IP owners should follow Disney's example and "Be Like Mickey" in actively exploring new opportunities in new media.

The lesson from the iTunes and Disney experiences is that the development and use of innovative distribution channels can be among the most effective weapons in combating piracy—and one that can be highly profitable. Unfortunately, members of the creative industries have tended to regard technology with either skepticism or downright hostility. This attitude is one that no longer makes sense. The economics of digital technology dictate that it will continue to become cheaper, more powerful and more pervasive. It is time for content creators to approach technology as a partner, not as an enemy.

Conclusion

A series of events and developments that took place in the months following the Aspen meeting suggests that issues related to security, privacy and intellectual property will continue to pose challenges for the foreseeable future.

The most newsworthy of these developments was undoubtedly the effort by Congress to address protection of intellectual property though the Stop Online Piracy Act (SOPA). This legislation would authorize the U.S. attorney general to seek a court order to block access to foreign websites that make available copyrighted content, using means such as DNS filtering. SOPA would also require online service providers (ISPs, search engines, ad networks and payment providers) to withhold their services from websites that are determined to be infringing copyrights held by American content producers.

The legislation provoked a lively debate. On one side, strongly supporting the bill, were music labels, movie studios and other content producers, who argued that action was needed "to curb online content theft and counterfeiting by foreign rogue websites, which are costing hundreds of thousands of American jobs and billions in lost wages and benefits." On the other side of the issue was a loose but passionate coalition of Internet companies, free speech advocates, academics and technologists who, while acknowledging the problem of piracy, argued that the means proposed by the bill would be destructive to some of the Internet's most important features as well as being ineffective in curbing the abuses it was intended to address. For example, an open letter from a group of Internet engineers asserted that SOPA would "create an environment of tremendous fear and uncertainty for technological innovation, and seriously harm the credibility of the United States in its role as a steward of key Internet infrastructure." Critics of the bill claim that by targeting not just offending content but entire websites, SOPA "will risk fragmenting the Internet's global domain name system (DNS) and have other capricious technical consequences."[42] The intensity of the debate and the sharp polarization of the bill's supporters and opponents demonstrate how difficult it is to reach a broad consensus for action to protect IP.

The issue of privacy seems to come up every time that Facebook makes any change to its interface. These changes typically provoke an outpouring of criticism from users, followed by an apology from Mark Zuckerberg and some revisions from Facebook. The full extent of concern about privacy on Facebook was underlined in November 2011, when the FTC announced settlement of an inquiry into the company's privacy practices that included an agreement that Facebook would undergo regular privacy audits over the next 20 years.

Privacy concerns also arose in late 2011 with the revelation that several major wireless network operators were routinely using a software program—Carrier IQ—preinstalled on subscribers' cell phones to monitor activities such as text messages, phone numbers and Google searches.

Critics charged that by tracking usage without users' knowledge, the Carrier IQ software verged on wiretapping. The operators quickly defended themselves by asserting that the software was being used only to troubleshoot device and network performance in order to "enhance customers' experience." Nonetheless, in the face of outspoken expressions of concern, which included several members of Congress, at least one carrier—Sprint—announced that it was discontinuing its use of the software.

Finally, a recent example of a security issue was a news account following the downing in Iran of an advanced pilotless U.S. surveillance drone. Iranian engineers claimed that they had hacked into the drone's GPS and taken over its guidance system, forcing it to land in Iran rather than returning to its own base. The story cast doubt on the claim and noted that such a feat would be difficult to accomplish. But it also noted that in 2009, Iranians did successfully intercept a live video feed from another U.S. surveillance drone. More recently, a computer virus from an undisclosed source infected the virtual cockpits of Predator and Reaper drone pilots in Nevada.

But as I was completing this report in early December, I encountered two different security issues much closer to home. First, I received an email from a good friend who lives across the country from me, letting me know that he was not in Scotland, had not lost all of his money and had not sent me an urgent request to wire funds to help him out. In fact, I had not received the original phishing message, but if I had, I hope that I would have been careful to check out its authenticity. But since my friend is a frequent and intrepid traveler, the situation was not implausible, and I suspect that my first impulse would have been to respond to his request.

A few days later, when I stopped to pick up a gallon of milk at my local supermarket, part of a medium-sized chain of stores in Northern California, I discovered a printed notice at the checkout stand that informed me that credit/debit card readers in more than 20 of their stores had been tampered with in order to obtain information on customers' bank accounts and credit cards. Most alarmingly, the notice stated that there had been approximately 80 employee and customer reports of either compromised accounts or attempts to access account data. According to a news story about the incident, at least one customer reported that money had been withdrawn from her checking account by an unknown party. I realized that I might well have shopped at some point at one of the compromised locations. In addition, the company was not certain that all tampered terminals had been found. And the action recommended by the stores was not very helpful: they strongly recommended that customers who used a self-checkout lane in the affected stores contact their financial institutions to close existing accounts and seek further advice. In other words, customers, you are basically on your own! Should I take the precaution of closing my bank account or at least changing the PIN on my debit card?

What is striking about these issues related to security, privacy and IP is how diverse and multifaceted they are. They range in scale from international and national to local and even intensely personal. In virtually every case, they raise difficult questions about what actual harm is and what the most appropriate solutions are. These issues are a reminder that the stakes in finding effective rules for the digital road are high, and that all of us have a stake in this game.

Endnotes

1. The four locations linked by the original Arpanet were computer centers at UCLA, UC-Santa Barbara, the Stanford Research Institute (SRI) and the University of Utah.

2. The ability of the Internet to scale from humble beginnings to its present size has surprised even experts. In December 1995, Robert Metcalfe, inventor of Ethernet, famously predicted in a column in *Infoworld* magazine that the Internet would suffer a "catastrophic collapse" in 1996 due to unsustainable growth. He was so sure he was right that he offered to eat his words if he was wrong, which he did publicly in early 1997. See Bob Metcalfe, "Eating my Collapse Column," April 16, 1997. Available at: www.merit.edu/mail.archives/nanog/1997-04/msg00192.html.

3. Somini Sengupta, "Update Urged on Children's Online Privacy," *The New York Times*, September 15, 2011. Available at: www.nytimes.com/2011/09/16/technology/ftc-proposes-updates-to-law-on-childrens-online-privacy.html?_r=1&scp=1&sq=update%20urged%20on%20children%27s%20online%20privacy&st=cse.

4. Musaque Ahamad and Bo Rotolini, *Emerging Cyber Threats Report 2012*, Georgia Tech Cyber Security Summit 2011, Georgia Tech Information Security Center. Available at: gtisc.gatech.edu/doc/emerging_cyber_threats_report2012.pdf.

5. Paul Roberts, "Bredolab Botnet Crackdown Could Have Wide Impact," Threat Post, October 26, 2010. Available at: http://threatpost.com/en_us/blogs/bredolab-botnet-crackdown-could-have-wide-impact-102610.

6. Musaque Ahamad and Bo Rotolini, *Emerging Cyber Threats Report 2012*, Georgia Tech Cyber Security Summit 2011, Georgia Tech Information Security Center. Available at: gtisc.gatech.edu/doc/emerging_cyber_threats_report2012.pdf.

7. See, for example, Mitchell Zuckoff, "The Perfect Mark: How a Massachusetts psychotherapist fell for a Nigerian e-mail scam," *The New Yorker*, May 15, 2006. Available at: www.newyorker.com/archive/2006/05/15/060515fa_fact?printable=true#ixzz1ZC4IsIJZ.

8. "Did China Hijack 15% of the Internet: Routers, BGP and Ignorance," OmniNerd, January 5, 2011. Available at: www.omninerd.com/articles/Did_China_Hijack_15_of_the_Internet_Routers_BGP_and_Ignorance.

9. Aleecia M. McDonald and Lorrie Faith Cranor, "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society*, 2008 Privacy Year in Review issue. Available at: www.is-journal.org.

10. Association of Academic Health Centers, *HIPAA Creating Barriers to Research and Discovery*, June 2008. Available at: www.aahcdc.org/policy/reddot/AAHC_HIPAA_Creating_Barriers.pdf.

11. See, for example, "Physicians' Use of Text Messages Sparks HIPAA Compliance Concerns," iHealthBeat, October 21, 2011. Available at: www.ihealthbeat.org/articles/2011/10/21/physicians-use-of-text-messages-sparks-hipaa-compliance-concerns.aspx#ixzz1bRffFvtC.

12. Scott Thurm and Yukari Iwatani Kane, "Your Apps are Watching You," *The Wall Street Journal*, December 17, 2010. Available at: http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html.

13. Liana B. Baker and Jim Finkle, "Sony PlayStation suffers massive data breach," Reuters, April 26, 2011. Available at: www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUS-TRE73P6WB20110426.

14. "Sutter Health Informs Patients of Stolen Computer," Sutter Health Media Line, November 16, 2011. Available at: www.sutterhealth.org/about/news/news11_notice-to-patients-of-stolen-computer.html.

15. Jason Green, "Stanford Hospital & Clinics vows to fight $20M class action," *San Jose Mercury News*, October 4, 2011. Available at: www.mercurynews.com/ci_19035601?IADID.

16. *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, Internet Policy Task Force, U.S. Department of Commerce, December 10, 2010. Available at: www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf.

17. State Security Breach Notification Laws, National Conference of State Legislatures, October 12, 2010. Available at: www.ncsl.org/default.aspx?tabid=13489.

18. It has been estimated that the BitTorrent peer-to-peer sharing platform has more users than Hulu and Netflix combined and that this type of activity is responsible for generating a substantial portion of all Internet traffic. See Austin Carr, "BitTorrent Has More Users Than Netflix and Hulu Combined—and Doubled," *Fast Company*, January 4, 2011. Available at: www.fastcompany.com/1714001/bittorrent-swells-to-100-million-users.

19. Stephen E. Siwek, "The True Cost of Copyright Industry Piracy to the U.S. Economy," IPI Policy Report # 189, October 2007, Institute for Policy Innovation. Available at: www.ipi.org/IPI\IPIPublications.nsf/PublicationLookupMain/A2C29ADF66FD941186257369005A052D.

20. Isabelle Groc, "The Price of Piracy," *PC Magazine*, October 10, 2007. Available at: www.pcmag.com/article2/0,2817,2193332,00.asp#fbid=YacdnXPU_hA.

21. *IFPI Digital Music Report 2011*, International Federation of the Phonographic Industry. Available at: www.ifpi.org/content/library/DMR2011.pdf.

22. *The Cost of Movie Piracy*, L.E.K. Consulting, 2005. Available at: www.archive.org/stream/MpaaPiracyReort/LeksummarympaRevised_djvu.txt.

23. See, for example, the discussion of "how much regulation" in the report of the 2010 Aspen Institute Forum on Communications and Society (FOCAS): Richard Adler, *News Cities: The Next Generation of Healthy Informed Communities*. Available at: www.aspeninstitute.org/sites/default/files/content/docs/cands/News_Cities_The_Next_Generation_of_Healthy_Informed_Communities.pdf.

24. According to an analysis of 32 million actual user passwords from a list that, ironically, was posted on the Internet as the result of a data intrusion by an unknown hacker, "The most common password was '123456,' followed by '12345' and '123456789.' The other passwords rounding out the top five were 'password' and 'iloveyou.'" Jaikumar Vijayan, "Users still make hacking easy with weak passwords," *Computerworld*, January 21, 2010. Available at: www.computerworld.com/s/article/9147138/Users_still_make_hacking_easy_with_weak_passwords.

25. Eric Schmitt, "White House Orders New Computer Security Rules," *The New York Times*, October 6, 2011. Available at: www.nytimes.com/2011/10/07/us/politics/white-house-orders-new-computer-security-rules.html.

26. Musaque Ahamad and Bo Rotolini, *Emerging Cyber Threats Report 2012*, Georgia Tech Cyber Security Summit 2011, Georgia Tech Information Security Center. Available at: gtisc.gatech.edu/doc/emerging_cyber_threats_report2012.pdf.

27. William Jackson, "Clarke: Outdated cyber defense leaves US open to attack," Government Computer News, September 19, 2011. Available at: http://gcn.com/Articles/2011/09/19/Richard-Clarke-US-outdated-cyber-defense.aspx?Page=1.

28. An article by James Fallows in *The Atlantic* magazine describes his wife's traumatic experience with having her email account hacked, which resulted in the disappearance of some six years of professional and personal correspondence. The article describes the couple's dismay at discovering how little help was available, at least initially, for repairing damage from the attack. The article concludes with specific suggestions for how individuals can better protect their email and other online activities. See James Fallows, "Hacked," *The Atlantic*, November 2011. Available at: www.theatlantic.com/magazine/archive/2011/11/hacked/8673.

29. For a report on how the marketplace is responding to a need for insurance against cyber attacks, see Nicole Perlroth, "Insurance Against Cyber Attacks Expected to Boom," *The New York Times*, December 23, 2011. Available at: http://bits.blogs.nytimes.com/2011/12/23/insurance-against-cyber-attacks-expected-to-boom.

30. These standards are maintained by the Common Criteria Recognition Arrangement, an international consortium that is made up of representatives of more than two-dozen countries. The Common Criteria, which are used to certify the security of computer products and services, were created through harmonization of separate security standards maintained by the United States, Canada and Europe.

31. See *Informing Communities: Sustaining Democracy in the Digital Age*, The Aspen Institute, 2009. Available at: www.knightcomm.org/wp-content/uploads/2010/02/Informing_Communities_Sustaining_Democracy_in_the_Digital_Age.pdf. See also the Knight Commission White Paper, Renee Hobbs, *Digital and Media Literacy: A Plan of Action,* The Aspen Institute, 2010. Available at: www.knightcomm.org/digital-and-media-literacy-a-plan-of-action.

32. According to a brief history of FIPs provided by the Federal Trade Commission, "Fair information practice principles were first articulated in a comprehensive manner in the United States Department of Health, Education and Welfare's seminal 1973 report entitled Records, Computers and the Rights of Citizens (1973) [hereinafter "HEW Report"]. In the twenty-five years that have elapsed since the HEW Report, a canon of fair information practices has been developed by a variety of governmental and inter-governmental agencies. In addition to the HEW Report, the major reports setting forth the core fair information practice principles are: The Privacy Protection Study Commission, Personal Privacy in an Information Society (1977); Organization for Economic Cooperation and Development, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980); Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information (1995); U.S. Dept. of Commerce, Privacy and the NII: Safeguarding Telecommunications-Related Personal Information (1995); The European Union Directive on the Protection of Personal Data (1995); and the Canadian Standards Association, Model Code for the Protection of Personal Information: A National Standard of Canada (1996)." Available at: www.ftc.gov/reports/privacy3/endnotes.shtm#N_27.

33. Latanya Sweeney, *Simple Demographics Often Identify People Uniquely*. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh, 2000. Available at: http://dataprivacylab.org/projects/identifiability/index.html.

34. Scott Thurm and Yukari Iwatani Kane, "Your Apps are Watching You," *The Wall Street Journal*, December 17, 2010. Available at: http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html.

35. David Sarno, "The Internet sure loves its outlaws," *Los Angeles Times*, April 29, 2007. Available at: www.latimes.com/entertainment/news/la-ca-webscout29apr29,0,1261622.story?coll=la-home-entertainment.

36. The Pirate Bay Blog, accessed October 24, 2011. Available at: http://thepiratebay.org/blog/195.

37. Timothy B. Lee, "British Telecom ordered to blacklist Usenet search engine, " Ars Technica, July 28, 2011. Available at: http://arstechnica.com/tech-policy/news/2011/07/british-telecom-ordered-to-blacklist-usenet-search-engine.ars.

38. Bobbi Newman, "FCC Proposes Digital Literacy Corps," Libraries and Transliteracy, March 16, 2010. Available at: http://librariesandtransliteracy.wordpress.com/2010/03/16/fcc-proposes-digital-literacy-corps.

39. Peter Levine, *Civic Engagement and Community Information: Five Strategies to Revive Civic Communication*, Aspen Institute, 2011. Available at: www.knightcomm.org/civic-engagement-and-community-information-five-strategies-to-revive-civic-communication. See also Renee Hobbes, *Digital and Media Literacy: A Plan of Action*, Aspen Institute, 2010. Available at: www.knightcomm.org/digital-and-media-literacy-a-plan-of-action.

40. "Apple: 16 billion iTunes songs downloaded, 300 million iPods sold," Engadget, October 4, 2011. Available at: www.engadget.com/2011/10/04/apple-16-billion-itunes-songs-downloaded-300-million-ipods-sol.

41. *IFPI Digital Music Report 2011,* International Federation of the Phonographic Industry. Available at: www.ifpi.org/content/library/DMR2011.pdf. However, IFPI argues that piracy continues to have a large negative impact on music sales. For example, the association's annual report notes that "total sales by debut artists in the global top 50 album chart in 2010 were just one quarter of the level they achieved in 2003."

42. "An Open Letter From Internet Engineers to the United States Congress," December 15, 2011. Available at: www.eff.org/sites/default/files/Internet-Engineers-Letter.pdf

APPENDIX

The Twenty-Sixth Annual Conference on Communications Policy

Rules of the Digital Road: Privacy, Security, Intellectual Property

Aspen, Colorado
August 16-19, 2011

Conference Participants

Richard Adler
Research Associate
Institute for the Future

Greg Amadon
Investor and Entrepreneur

Rebecca Arbogast
Managing Director
Stifel Nicolaus

Robert Atkinson
Founder and President
The Information Technology and Innovation Foundation

Dorothy Attwood
Senior Vice President, Global Public Policy
The Walt Disney Company

Jamie Barnett
Chief, Public Safety and Homeland Security Bureau
Federal Communications Commission

Catherine Bohigian
Senior Vice President, Federal Affairs
Cablevision Systems Corporation

Julie Brill
Commissioner
Federal Trade Commission

Rudy Brioché
Senior Director of External Affairs and Public Policy Counsel
Comcast Corporation

Helen Brunner
Director
Media Democracy Fund

Jeffrey Campbell
Senior Director, Americas Region
Global Government Affairs
Cisco Systems

Jonathan Chaplin
Director
Credit Suisse

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

John Clippinger
Visiting Scientist
MIT Media Lab

Mignon Clyburn
Commissioner
Federal Communications Commission

Alan Davidson
Director of Public Policy, Americas
Google

Gary Epstein
General Counsel and Managing Director
Aspen Institute IDEA Project

Charles M. Firestone
Executive Director
Communications and Society Program
The Aspen Institute

Richard Green
Director
Liberty Global, Inc.

Leslie Harris
President and Chief Executive Officer
Center for Democracy & Technology

Dale Hatfield
Senior Fellow
Silicon Flatirons Center, and
Adjunct Professor
University of Colorado at Boulder

Reed Hundt
Principal
REH Advisors, and
Chairman
Aspen Institute IDEA Project

Robert Jarrin
Senior Director, Government Affairs
Qualcomm Incorporated

Julia Johnson
President
NetCommunications

Cameron Kerry
General Counsel
U.S. Department of Commerce

Karen Kornbluh
United States Ambassador to the Organization for Economic Cooperation and Development
U.S. Department of State

Edward Lazarus
Chief of Staff
Federal Communications Commission

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

Blair Levin
Fellow
Communications and Society Program
The Aspen Institute

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

Brent Olson
Vice President, Public Policy
AT&T Services, Inc.

Thomas Power
Chief of Staff
National Telecommunications and Information Administration
U.S. Department of Commerce

Marc Rotenberg
Executive Director
Electronic Privacy Information Center (EPIC)

Charles Salem
Managing Director of Public Policy
Microsoft Corporation

Gigi Sohn
President
Public Knowledge

Steven Teplitz
Senior Vice President, Government Relations
Time Warner Cable

Nicol Turner-Lee
Vice President and Director
Media and Technology Institute
Joint Center for Political and Economic Studies

Stefaan Verhulst
Chief of Research
Markle Foundation

Joe Waz
Senior Fellow
Silicon Flatirons Center
University of Colorado at Boulder

Bruce Wolpe
Senior Advisor
Representative Henry Waxman
U.S. House of Representatives

Staff:

Sarah Eppehimer
Senior Project Manager
Communications and Society Program
The Aspen Institute

Ian Smalley
Program Associate
Communications and Society Program
The Aspen Institute

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

About the Author

Richard Adler is a Research Associate at the Institute for the Future, in Palo Alto, California. He is also President of People & Technology, a consulting firm located in Silicon Valley.

Adler has written a number of Aspen Institute reports, recently including *Solving the Dilbert Paradox* (2011), *News Cities: The Next Generation of Healthy Informed Communities* (2011), *Leveraging the Talent-Driven Organization* (2010) and *Talent Reframed: Moving to the Talent Driven Firm* (2009). Other Aspen Institute reports Adler has written include *Media and Democracy* (2009), *m-Powering India* (2008), *Minds on Fire: Enhancing India's Knowledge Workforce* (2007), and *Next Generation Media: The Global Shift* (2007). He is also the author of *Healthcare Unplugged: The Evolving Role of Wireless Technology* (California HealthCare Foundation, 2007) and is co-editor of *Texting 4 Health* (Stanford Captology Media, 2009).

Adler is Fellow of the World Demographic Association and serves on a number of local and national boards. He holds a BA from Harvard, an MA from the University of California at Berkeley and an MBA from the McLaren School of Business at the University of San Francisco.

Previous Publications from the Aspen Institute Communications Policy Project

Spectrum for the Next Generation of Wireless, by Mark MacCarthy

The report resulting from the 2010 Aspen Institute Roundtable on Spectrum Policy explores possible sources of spectrum, looking specifically at incentives or other measures to assure that spectrum finds its highest and best use. It includes a number of recommendations, both private and federal, of where and how spectrum can be repurposed for wireless use, including a discussion of incentive auctions, overlay auctions, flexible use, a spectrum innovation fund and spectrum fees, among other strategies. 2011, 68 pages, ISBN Paper: 0-89843-551-X, $12.00

Rewriting Broadband Regulation, by David Bollier

The report of the 25th Annual Aspen Institute Conference on Communications Policy in Aspen, Colorado, considers how the United States should reform its broadband regulatory system. Participants looked at international models and examples, and examined how data and communications should be protected in the international arena. The resulting report 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.

Participants also 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. 2011, 52 pages, ISBN Paper: 0-89843-548-X, $12.00

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 spectrum 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 policymakers 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* or by sending an email request to *publications@aspeninstitute.org.*

About the Aspen Institute Communications and Society Program

www.aspeninstitute.org/c&s

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

The Program's projects fall into one or more of three categories: communications and media policy, 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 video regulation), the impact of advances in information technology (e.g., "when push comes to pull"), advances in the mailing medium and diversity and the media. The Program also convenes the Aspen Institute Forum on Communications and Society, in which chief executive-level leaders of business, government and the nonprofit sector examine issues relating to the changing media and technology environment.

Most conferences use 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 also are available to the public at large through the World Wide Web at *http://www.aspeninstitute.org/c&s.*

The Program's Executive Director is Charles M. Firestone, who has served in that capacity since 1989. He also served as Executive Vice President of the Aspen Institute for three years. He is a communications attorney and law professor who formerly was 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.