

Exploring Self Regulatory Strategies for Network Management

Flatirons Summit on Information Policy

**Philip J. Weiser
Professor of Law and Telecommunications
University of Colorado**

August 25, 2008

Author's Note

The “Flatirons Summits on Information Policy” brings together academics, public interest advocates, governmental officials, and industry leaders to engage in creative thinking and intellectually honest discussion. Over the last eight years, the Silicon Flatirons February policy conference, which focuses on the “Digital Broadband Migration,” has thrived on account of its ability to elevate policy debates. More recently, we have developed the Flatirons Summits as a means of allowing exchanges of ideas under the “Chatham House Rule”—i.e., individual comments are quoted only with permission as part of a report that encapsulates the discussion and places it in context. Our first such forum, held in the spring of 2007, focused on the challenges and opportunities for spurring the development of a next generation network for public safety.¹ On June 9th and 10th, 2008, we hosted our second “Flatirons Summit on Regulatory Policy,” focusing on the use of self-regulatory strategies to address network management issues.

The focus on network management reflected a confluence of events. First, the Silicon Flatirons Center hosted the 2003 conference where Tim Wu first introduced the concept of “network neutrality” (in a paper later published in our *Journal on Telecommunications and High Technology Law*).² Moreover, Silicon Flatirons has hosted a series of conferences on the topic, including ones discussing FCC Chairman Michael Powell’s “Four Freedoms,” which he outlined at our 2004 February policy conference (and published in our *Journal*).³ Indeed, the allegations that Madison River Communications engaged in the blocking of Vonage’s Voice over Internet Protocol traffic were first reported and confirmed at the 2005 February policy conference. Consequently, addressing issues associated with network management at a Flatirons Summit seemed to be a natural step.

The second principal motivation for evaluating the potential effectiveness of self-regulation is that few commentators or policymakers have examined carefully the institutional issues around how to determine what constitutes “reasonable network management.” Considering that the definition of the term is far from self-evident, the prospect of some entity being charged with interpreting and enforcing that standard appears likely.⁴ Consequently, we believed that a thoughtful discussion among concerned academics, public interest advocates, and industry leaders could shed some light on and help develop thoughtful suggestions on how to address this important public policy issue. Given the pendency of (and subsequent ruling in) the challenge to Comcast’s management of certain peer-to-peer (P2P) protocols (such as BitTorrent) at the FCC,⁵ it seemed clear that this issue would continue to be discussed in the years ahead. Ideally, the report set forth herein will help elevate and inform that discussion.

¹ The report that emerged from that discussion was later published as a paper. See Phil Weiser and Dale N. Hatfield, *In Pursuit of a Next Generation Network for Public Safety Communications* (Univ. Colo. Law Sch. Legal Studies Research Paper No. 08-07), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1032737.

² Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J. TELECOMM. HIGH TECH. L. 141 (2003).

³ Michael K. Powell, *Preserving Internet Freedom: Guiding Principles for the Industry*, 3 J. TELECOMM. HIGH TECH L. 5, 11-12 (2004).

⁴ Indeed, I discuss this very prospect in Phil Weiser, *The Next Frontier in Network Neutrality*, 60 ADMIN L. REV. 2, 22-25 (2008), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1080672.

⁵ Press Release, Federal Communications Commission, Commission Orders Comcast to End Discriminatory Network Management Practices (Aug. 1, 2008), available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-284286A1.pdf [hereinafter *FCC Press Release*]; see also Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly

The success of the Summit reflects the hard work and initiative of a number of individuals. First and foremost, Silicon Flatirons remains indebted to Dale Hatfield on so many levels—his commitment to evidence-based policymaking, intellectual honesty, appreciation for how issues related to technology architecture matter, and personal devotion to Silicon Flatirons are all indispensable to our ongoing growth and development. Indeed, the Flatirons Summits were born of an effort to replicate discussions that Dale participated in during the days when the Annenberg Center in Washington, D.C. was chartered to hold such conferences. It is thus fitting that the Dale Hatfield Scholars and Research Fund, which is supported by friends of Dale to sponsor student internships, regulatory education, and policy research, helped to underwrite this Summit.

The organization and success of this Summit relied on a number of individuals associated with Silicon Flatirons. Dan McCormick, who serves as our Event Manager and as my Research Assistant, invested enormous time and energy to make the event a success, ranging from managing the necessary logistics to organizing the readings to taking notes during the event to helping to write the report. Pierre de Vries, who is a Senior Adjunct Fellow, has taken on the responsibility for helping conceive of and develop our Flatirons Summits and spurred us to hold this event. Similarly, Senior Adjunct Fellow Ray Gifford has thought deeply about this topic and helped us shape the agenda and readings for the event. Most significantly, Anna Noschese, our Program Director, is nothing short of amazing in terms of her dedication and work ethic. We could not have pulled off this Summit without her.

Finally, I must acknowledge the many individuals who came to the event and engaged in a series of thoughtful discussions that, in other settings, are all too often imbued with rhetoric and invective. During the Summit, the level of good will, intellectual honesty and thoughtfulness as well as focus was remarkably high. As to the report itself, it bears emphasis that, unless an individual is quoted, no statements or views should be attributed to individual attendees of the Summit. Rather, the report is written from the perspective of an informed observer and, as the author, I am solely responsible for all statements herein.

Philip J. Weiser
August 25, 2008
Boulder, Colorado

Degrading Peer-to-Peer Applications, *Memorandum Opinion and Order*, File No. EB-08-IH-1518 (2008), available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-183A1.pdf [hereinafter *Comcast Decision*].

Executive Summary

The “hands off the Internet” era is over. The Federal Communications Commission’s recent decision that ruled that Comcast’s use of network management techniques violated its Internet Policy Statement confirms that the federal government is not content to allow broadband providers to operate free from any form of regulatory oversight.⁶ Broadband providers now need to defend their network management practices as “reasonable.” Nevertheless, it remains to be seen what institutional strategy will be effective in answering the no longer hypothetical question of what constitutes “reasonable network management.”

At a Summit that brought together a wide array of academics, public interest group advocates, and industry leaders from a range of disciplines (law, economics, business, and technology), the participants reached a rough consensus on a “Statement of Opportunity.” This statement highlights that a self-regulatory strategy could effectively address the question of how to determine what constitutes “reasonable network management” and whether that standard of conduct was violated in a particular case. While the motivation for establishing such a body may be a combination of the enlightened self-interest of the relevant stakeholders and a fear of politicized intrusion into the development of technology and market relationships, the wide range of Summit participants concurred that a self-regulatory body could superintend a framework that might well operate with greater expertise, flexibility, speed, certainty, and predictability than a public regulatory body.

Relevant stakeholders and public regulators might perceive a self-regulatory strategy as a valuable alternative to either having no institutional form of oversight whatsoever or imposing public regulation. In its earlier days, the Internet’s technical architecture and open standards provided all parties with a means of developing new technologies (whether transmission infrastructure like broadband or applications like email or instant messaging) that could operate effectively. But in a vastly more commercialized Internet environment, where demands for bandwidth and quality of service are ever increasing, the need for coordination between broadband providers and applications developers is greater than ever. Thus, an absence of coordination between broadband providers, applications developers,⁷ and end users could, at a minimum, constrain opportunities for continued development within the Internet. The tools available to “enforce” coordination between Internet stakeholders include private contracts, social norms, public regulation, and a privately developed and superintended self-regulatory framework. The question is what combination of these tools can assure all stakeholders that the Internet will develop—notably, with respect to network management techniques—in a manner than can enable a flourishing of innovation. Participants at the Summit seemed convinced that private contracts, social norms, and public regulation were unlikely, by themselves, to assure such an environment.

The establishment of a self-regulatory framework presents a number of daunting challenges. The success of existing self-regulatory models—such as the ones governing the amateur radio service and frequency coordinators in the spectrum context—provides some encouragement that such a regime can be developed. Ideally, such a regime could avoid both the perils associated with a lack of oversight and stability over the relevant network management

⁶ As the FCC put it: “In the *Internet Policy Statement*, the Commission recognized its responsibility for overseeing and enforcing the ‘national Internet policy’ Congress had established in section 230(b) of the Communications Act of 1934.” *Id.* at ¶ 13.

⁷ This report will use the phrase “applications developers” to refer to the broad cross-section of firms that create Internet-based content or services, ranging from Google and BitTorrent to ESPN.com and Skype.

practices as well as the risks of unintended consequences that sometimes attend public regulation. Consequently, this report outlines the rationale behind and steps necessary for either public authorities or Internet industry leaders to nurture the development of a self-regulatory body to oversee network management issues.

I. Introduction

On June 9th and 10th, 2008, the Silicon Flatirons Center of the University of Colorado hosted a “Flatirons Summit on Regulatory Policy” that brought together academics, public interest advocates, and industry leaders to examine the potential of using self-regulatory strategies to address Internet policy issues in general and network management issues in particular. (A list of the Summit participants is set forth in Appendix A.) Over the course of a day and a half, the participants evaluated the experience of self-regulation in a variety of contexts, discussed its potential applicability to network management issues, and highlighted key issues that would need to be resolved in order to enable this model of regulation to operate effectively.

At the end of the Summit, almost all participants agreed that the potential role of using self-regulation to address network management issues is an opportunity that merits further exploration. To that end, the participants all came together to reach a rough consensus on a “Statement of Opportunity,” which is set forth in Part II of the report. This Statement of Opportunity, although focused specifically on the context of network management, highlights that policymakers would be well advised to examine the use of self-regulation in a variety of Internet policy domains.

Even though the discussion was held in an academic context with a rigorous level of analysis, the issue of self-regulatory strategies for network management became much less academic in the weeks and months following the June Summit. In particular, the FCC announced, on Friday, August 1, 2008, its conclusion that Comcast violated the agency’s Internet Policy Statement, explaining that “Comcast’s network management practices discriminate among applications rather than treating all equally and are inconsistent with the concept of an open and accessible Internet.”⁸ By so doing, the agency made clear that it would enforce the Internet Policy Statement going forward (starting with Comcast) and would thus establish criteria for evaluating what constitutes “reasonable network management.” At the Summit, John Ryan, Assistant Chief Legal Officer at Level 3, envisioned such a ruling, concluding that the need for a new institutional strategy to oversee network management issues became immediately apparent when the FCC opened an investigation into the Comcast/P2P dispute.

The FCC’s Comcast ruling has made it clear that the search for an institutional strategy to address what constitutes “reasonable network management” is anything but an academic exercise. As a number of participants emphasized, developing the appropriate institutional strategy is critical to the development of the Internet because the concept of “reasonable network management” is neither clear nor self-executing.⁹ To that end, Joe Waz, Senior Vice President of

⁸ *Id.* at 2.

⁹ As Paul Ohm, one of the Summit participants, puts it in a forthcoming article:

The phrase “network management” gained prominence through [pronouncements from] successive chairmen of the FCC. . . . Thus far, however, the line of reasonable network management is vague and indeterminate. . . . One reason why “reasonable network management” is so vague is it describes not an engineering principle, but a policy conclusion made by weighing

Comcast, underscored that companies are likely to be frustrated by the lack of any effective forum for developing the “common law of network management” and that the absence of any obvious forum leaves open the important question of “where do we go to get an answer to how does the Internet community feel about network management practices and what’s reasonable and what’s not.” Today, he added, “there’s nowhere to go” to engage in this discussion.

The FCC’s ruling, whether or not it is sustained on appeal, is likely to open up a debate about the proper forum for developing the definition of “reasonable network management” as well as the proper forum for addressing issues as they arise and investigating alleged departures from that standard. In dissenting from the FCC’s Comcast decision, Commissioner McDowell criticized the institutional processes used by the FCC to evaluate whether Comcast departed from the reasonable network management standard. In particular, he suggested that:

The truth is, the FCC does not know what Comcast did or did not do. The evidence in the record is thin and in conflict. All we have to rely on are the apparently unsigned declarations of three individuals representing the complainant’s view, some press reports, and the conflicting declaration of a Comcast employee. The rest of the record consists purely of differing opinions and conjecture.¹⁰

Other commentators have also criticized the FCC’s processes in this case and the level of discourse during the proceeding. Ed Felten, for example, highlighted that, in seeking to defend its network management techniques before the FCC, Comcast invoked Congresswoman Mary Bono as an expert and, in so doing, incorrectly stated how peer-to-peer technology operates.¹¹ In defense of Comcast, its filing (like that of many other parties) reflected the tradition that the FCC’s notice-and-comment proceedings operate more along political lines than judicial ones; consequently, citing the views of members of Congress to make a point is a common practice. Unfortunately, such proceedings are not designed, as McDowell highlighted, to find facts, weigh evidence, and define the parameters of and determine compliance with standards of conduct.

Going forward, the FCC will need to determine whether it will develop appropriate institutional processes to assess compliance with the concept of “reasonable network management.” It might, as McDowell suggests in his dissent, empower its enforcement processes to judge compliance with the applicable standard.¹² Alternatively, the agency might, as McDowell suggested in an op-ed published just before the release of the FCC’s ruling and discussed in his dissent, rely on industry self-regulation.¹³ As Peter Rohrbach highlighted, the

the legitimate technological and business goals of network management with what society deems reasonable in light of many principles including user privacy.

Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance* (forthcoming 2009) (manuscript at 46-47, on file with author).

¹⁰ Dissenting Statement of Commissioner Robert M. McDowell to the *Memorandum Opinion and Order* in Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications, File No. EB-08-IH-1518, WC Docket No. 07-52 7 (2008) [hereinafter *McDowell Dissent*].

¹¹ Ed Felten, *Comcast’s Disappointing Defense*, FREEDOM TO TINKER, Feb. 18, 2008, <http://www.freedom-to-tinker.com/?p=1256>.

¹² *McDowell Dissent*, *supra* note 10, at 8-10.

¹³ Robert M. McDowell, *Who Should Solve This Internet Crisis?*, July 28, 2008, at A17, available at <http://www.washingtonpost.com/wp-dyn/content/article/2008/07/27/AR2008072701172.html>.

two options are not mutually exclusive and, as discussed below, may well mutually reinforce one another. With regard to any possible reliance on self-regulation, there are a series of questions that must be examined, beginning with what existing or new body is available to address such issues. The purpose of this report is to discuss why such an approach might be advantageous, what such a body might look like, and how it might function.

In many regulatory policy discussions, the network neutrality debate (including issues of network management) is often presented as a regulatory battle between potential winners and losers.¹⁴ To that end, reporters are fond of asking whether a proposed regulatory action is “good for Google or AT&T.”¹⁵ In reality, however, there are a series of possible outcomes that are either good for both AT&T and Google or bad for both AT&T and Google. From this perspective, the appropriate resolution of how to address what constitutes “reasonable network management” is not about picking winners and losers in the Internet ecosystem; it is about developing a framework for a thriving ecosystem that enables all players—including end users—to operate effectively. Such a framework, which could take the form of an established self-regulatory organization, could assure all stakeholders that they could adopt business and technology strategies without worrying about negotiating a maze of private contracts with the affected parties.

To appreciate the win-win perspective on developing a new framework for network management issues, it is important to look to the teachings of what is often referred to as “new institutional economics” or, for short, “NIE.” As Ray Gifford, partner at Kamlet, Shepherd & Reichert and Senior Adjunct Fellow at Silicon Flatirons, explained, an NIE perspective can help understand a “multiparty contracting problem.” The problem, Gifford explained, is that very high transaction costs and a lack of trust between the relevant actors (namely, end users, application developers and broadband service providers) create the potential for a breakdown in the relationship. Viewed in this light, the goal of self-regulation—or any effective regulatory framework—is to lower the transaction costs, provide a principled structure to facilitate negotiations, provide some measure of predictability and reliability and channel multiparty contracting problems into a framework that can avoid the escalation and politicization of disputes and misunderstandings.

Without some mechanism to assure all parties of the opportunity to deal fairly with one another and build trust that a stable equilibrium will continue, there are substantial risks to the welfare of end users, applications developers, and broadband service providers. In particular, under high levels of uncertainty, some parties may well resist making certain kinds of investments or choose to engage in strategic behavior aimed at appropriating the value created by the other party’s investment.¹⁶ Notably, this risk is not isolated to either broadband service

¹⁴ The better frame is a competition policy perspective that seeks to evaluate whether or not regulatory policy strategies ensure “competition on the merits.” In that respect, one often noted concern is that unreasonable network management techniques can be used to protect a broadband provider’s own content or services from competition from “over the top” players.

¹⁵ See, i.e., Christopher Stern, *Obama is From Google, McCain is From AT&T on Digital-Age Rules*, BLOOMBERG.COM, July 14, 2008, available at <http://www.bloomberg.com/apps/news?pid=20601087&sid=alsJ22j5BQS0&refer=home>.

¹⁶ For a poignant example of how the threat by a platform provider to appropriate the rents of an applications developer can undermine investment incentives, consider the challenges confronted by Dow Corning after the company invented fiber optic cable. As two commentators related:

providers or applications developers—either party can engage in or be hurt by such behavior. Worst of all, strategic behavior can potentially leave both parties worse off, undermining both of their economic positions, and, in the process, substantially hurting end users. Consequently, from both an enlightened self-interest perspective of the affected companies and a public policy perspective, the question is not whether some established framework will oversee issues like network management practices, but rather, what type of framework can do so most effectively.

In investigating a self-regulatory framework, this report does not evaluate all possible regulatory strategies or suggest that other ones are inappropriate. Rather, it seeks to examine how and why a self-regulatory strategy might well be a complement, or if very successful, a partial substitute to those strategies. Regardless of what institutional framework is developed to oversee network management issues, the core challenge for policymakers is to recognize how decisions about technical architecture and the Internet are related to ongoing innovation and technological change.¹⁷

This Paper proceeds in six parts. Part II sets forth the Statement of Opportunity that emerged from the Summit. Part III outlines the new institutional economics (NIE) perspectives that highlight the potential role for and value of an effective framework that can provide stability and assurance in terms of what network management practices are reasonable. Part IV examines the network management issue and the potential for a self-regulatory strategy. Finally, Part V discusses the specific questions related to the implementation of a self-regulatory strategy to address network management issues. Part VI offers a short conclusion.

AT&T, which owned most of the telephone lines in America at the time [of the invention of fiber optic technology], said it would be 30 years before its telephone system would be ready for optical fiber. And when it was, AT&T planned to make its own fiber. . . . [After AT&T entered into a consent decree with the federal government allowing competition in long distance,] MCI took the risk [of ordering fiber optic technology] and placed a 100,000 kilometer order for a new generation of fiber.

Willard K. Tom & Joshua A. Newberg, *Antitrust and Intellectual Property: From Separate Spheres to Unified Field*, 66 ANTITRUST L.J. 167, 202 (1997) (quoting Testimony of Timothy J. Regan, Division Vice President and Director of Public Policy, Corning, Inc., Before House Judiciary Committee (May 9, 1995)).

¹⁷ It bears emphasis that the Summit, like the regulatory policy debate, focused on network management issues related to the “public Internet” and thus does not relate at all to issues concerned with other uses of Internet technology, including, for example, its use in virtual private networks.

II. Statement of Opportunity

A rough consensus emerged at the Summit around the following statement of opportunity:

- I. The success of the development of Internet broadband delivery platforms and applications can be protected and bolstered by greater levels of (1) effective disclosure to end users, (2) sharing of information between stakeholders, and (3) trust that Internet connectivity will be delivered and used in a predictable and reasonable manner.
 - a. There is an important opportunity for an organizational structure to create a trusted environment for the development of norms that provide all stakeholders with increased certainty and predictability. The creation of such an environment promises to facilitate innovation and technological development on the part of broadband providers, applications developers,¹⁸ and end users each of which can benefit greatly from the ability to invest without the fear of inappropriate interference from public or private actors.
 - b. An established structure could review the reasonableness of “network management” techniques, thereby protecting the four Internet freedoms and the consumer interest in transparency. If no effective framework develops, there is a risk that network management techniques or applications behavior could undermine investment, innovation, and competition as well as leave end users—who are engaged in creative development—confused and frustrated by their Internet experience.
- II. The establishment of a Self Regulatory Organization (SRO) that can operate with independence, credibility, expertise, and legitimacy can build trust that Internet traffic that is generated in a responsible manner will be managed in a reasonable fashion. Such an SRO could also provide an environment for applications developers, broadband providers and end users to engage in constructive discussions concerning appropriate end user, applications, and network behavior (e.g., developing best practices and an increased understanding of one another’s needs). In particular, such an SRO could (1) acknowledge and agree upon clear and enforceable standards of conduct—drawing on the work of other important norm generation bodies; (2) provide “advisory opinions” to broadband providers that particular practices are reasonable; and (3) enforce the relevant standards of conduct as part of a binding contractual commitment to adhere to them.
- III. The advantage of an SRO model over existing regulatory institutions is that it (1) could move more efficiently and effectively to evaluate the reasonableness of network management issues; (2) can be more insulated from political pressures and focused on ascertaining the relevant factual issues through an effective adjudicative mechanism; and (3) could set flexible and adaptable rules that are compatible with technological dynamism.

¹⁸ As stated in note 6 above, this report uses the phrase “applications developers” to refer to the broad cross-section of firms that create Internet-based content or services, ranging from Google and BitTorrent to ESPN.com and Skype.

- IV. The development of an effective SRO raises a series of difficult issues that broadband providers, applications developers, and representatives of end users will need to address. As an initial matter, trust building and dialogue in a norm-generating environment is likely to be a critical prerequisite. Assuming that the interest in such an idea develops, a critical mass of stakeholders will need to structure the membership, financing, participation, and governance of such an organization. To do so, stakeholders should examine past SRO models to assist in developing one appropriate for this context.

III. New Institutional Economics, Multiparty Contracting, and Open Contracts

Before elaborating on the opportunity outlined above, this Part sheds some light on the relevant economic principles that explain the nature of the opportunity (and risk) at hand. In particular, as highlighted in the Introduction, the challenges around addressing the question of what constitutes “reasonable network management” can be understood as a “multiparty contracting problem.” The problem inherent in the network management context is that the relevant actors—broadband providers, applications developers, and end users—need to develop a level of trust and understanding about how the other parties behave. After all, the Internet experience, as Susan Crawford has highlighted, is not created by any single actor and exists because of the level of cooperation of all of them.¹⁹

Under the original Internet architecture, which was engineered in an environment where the Internet operated under a “best efforts” model and communications were generally not real-time or bandwidth-intensive,²⁰ the Internet’s architecture provided an effective guarantee as to how parties could and would behave. Moreover, cooperation in that environment stemmed from strong social norms among a relatively small and sophisticated group of users and a shared reliance on a set of common technical standards which, while voluntary, achieved sufficient acceptance that they came to be thought of as a kind of open contract. In today’s emerging Internet environment, however, there are a series of pressures that are leading broadband providers to upgrade and manage their networks (the need to detect and combat spam and viruses, secure the network against attacks, ensure that particular users do not hog bandwidth, deliver quality of service (QoS), identify and delete child pornography and, in some cases, seek to identify copyrighted works²¹) and opportunities for applications developers (as well as end users) to take advantage of massive levels of bandwidth.²² Unfortunately, when those efforts—instituting network management techniques and developing bandwidth-intensive (or quality-of-service dependent) applications—work at cross-purposes with one another, broadband providers and applications developers may well find themselves in a game of tug-of-war (or cat-and-mouse), with end users potentially suffering as innocent victims.

A. Platforms, Applications, and Multiparty Contracting

¹⁹ See, e.g., Susan Crawford, *The Internet and the Project of Communications Law*, 55 UCLA L. REV. 359, 360 (2007) (noting that all value is not created, nor should be captured by broadband providers).

²⁰ Weiser, *supra* note 4, at 5-7.

²¹ Ohm, *supra* note 9, at 51-53.

²² For a discussion of some emerging bandwidth-intensive applications, see Stacey Higginbotham, *Why We Need Fat Pipes: The Top 5 Bandwidth-Hungry Apps*, GIGAOM, Aug. 12, 2008, available at <http://gigaom.com/2008/08/12/why-we-need-fat-pipes-the-top-5-bandwidth-hungry-apps>.

As a starting point, it merits recognition that, under many circumstances, a platform provider will encourage and embrace development of new applications that will make its platform more valuable. To that end, for example, Comcast CEO Brian Roberts reported that “the increased demand for online video viewing was helping drive sales of cable modems,” stating that “[v]ideo over the Internet is cable’s friend[.]”²³ From the perspective of aspiring applications developers (like Vuze, a P2P applications developer who complained about Comcast’s conduct), there may be suspicion of broadband providers for any number of reasons. Even putting aside the suspicion that a platform provider would act in ways to prevent the applications developer from competing with the platform (such as in the *Madison River Communications* case),²⁴ applications developers may worry about the temptation on the part of platform providers—particularly if they possess monopoly power—to “extract rents” once the application has been developed and successfully deployed. Indeed, if that fear is great enough, applications developers may decline to develop new applications at all or engage in wasteful cat-and-mouse strategies aimed at evading detection by the rent seeker.²⁵ On the other side of the equation, moreover, if platform providers are absolutely prohibited from identifying new revenue opportunities or protecting the performance of their network in the face of bandwidth and QoS hungry applications, that will constrain their available business strategies and ability to succeed.

Hardcore free marketers may suggest that the market can be trusted to develop institutional arrangements to anticipate and address the possibility of strategic behavior and to encourage ongoing innovation by both platform providers and applications developers. To be sure, firms may well be able to, in certain cases, anticipate and address “*ex post* opportunism” and, in any event, it is not necessarily self-evident what constitutes “opportunistic” or “strategic” behavior. Nonetheless, as Jim DeLong has explained, “the mantra of ‘do it by contract’ is [flawed insofar as] it requires contract writers with an unlimited legal budget and a level of foresight that would be the envy of a psychic.”²⁶ Moreover, at least in this context, “we are talking long term investments under conditions of great uncertainty, and it is difficult to write the

²³ Vishesh Kumar, *Comcast Reports Strong Results in Web Services*, WALL ST. J., July 31, 2008, at B8. For the economic logic behind the principle that a platform provider welcomes complementary applications, see Joseph Farrell & Philip J. Weiser, *Modularity, Vertical Integration and Open Access Policies: Towards A Convergence of Antitrust and Regulation in the Internet Age*, 17 HARV. J. L. & TECH. 85, 89-100 (2003).

²⁴ See *Madison River Communications, LLC and Affiliated Companies*, Order, 20 FCC Rcd. 4296 (2005), available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-05-543A2.pdf [hereinafter *Madison River*]. There have been some examples abroad as well. See, e.g., Cho Jin-seo, *Cable TV Operators Block HanaTV*, KOREA TIMES, Oct. 22, 2006, available at <http://www.asiamedia.ucla.edu/article.asp?parentid=55961> (reporting that company blocked internet television services). For a discussion of the possible reasons for such behavior, see Farrell & Weiser, *supra* note 23, at 89-90.

²⁵ As Gawer and Henderson note, if the platform provider’s “incentive to engage in *ex post* price ‘squeezes’ is sufficiently strong, complementors may have no *ex ante* incentive to engage in innovation at all.” Annabelle Gawer & Rebecca Henderson, *Platform Owner Entry and Innovation in Complementary Markets: Evidence from Intel*, 16 J. ECON. & MGMT. STRATEGY 1, 5 (2007).

²⁶ James V. DeLong, *Avoiding A Tech Train Wreck*, THE AMERICAN, May/June 2008, available at <http://www.american.com/archive/2008/may-june-magazine-contents/avoiding-a-tech-train-wreck>; see also Paul L. Joskow, *Transaction Cost Economics, Antitrust Rules, and Remedies*, 18(1) J. L. ECON. & ORG. 95, 102 (2002) (“Transacting parties enter into relationships to mitigate [ex post opportunistic behavior,] but cannot do so perfectly.”).

contracts that would be required.”²⁷ And, to make matters even more complicated, as Jonathan Sallet, partner in the Glover Park Group highlighted, the transaction costs in this environment are huge and the difficulties of instituting the necessary arrangements are challenging. Finally, as for the definition of strategic or opportunistic behavior, this report uses Oliver Williamson’s colorful definition of such conduct “as self-interest seeking with guile.”²⁸

The concern with opportunistic behavior is greatest where a set of parties needs to cooperate and where a threat not to cooperate can be used to extract greater “rents” from another party. In general, firms confronting such a scenario will look for means of avoiding the need to engage in repeated bargaining for fear that their ability to bargain effectively will be compromised once they have made “relationship-specific” investments. The study of such relationships and the effort to develop safeguards against “*ex post* opportunism” is the central project of new institutional economics (NIE). Consequently, as explained by NIE, firms search for contractual (or regulatory) guarantees against opportunistic behavior when entering into such relationships.²⁹ In some cases, reputational constraints—and the power of social norms—may be effective; in others, vertical integration may become a necessary step to mitigate against the hazards of *ex post* opportunism; and, in yet other cases, parties may remain vulnerable to the possibility of hold-up, relying on imperfect contractual strategies as their best mode of protection.³⁰

Over the course of modern regulatory history, platform providers and applications developers have often relied on the presence of legal oversight mechanisms to prevent *ex post* opportunism and to facilitate cooperation. Consider, for example, the role played by the rules governing “retransmission consent” arrangements in the cable TV context. These rules, in effect, seek to limit the potential to engage in strategic behavior by a firm—either the platform provider (in this case, the cable or satellite company) or the applications developer (in this case, generally the broadcast network owning local TV stations). The presence of such rules becomes part of the operating environment and is only visible on those rare occasions, such as the famous dispute between Time Warner and Disney, when firms continue to hold out on reaching any arrangement and leave consumers without service as a result. In an unregulated environment, such as the

²⁷ *Id.*

²⁸ OLIVER E. WILLIAMSON, *THE ECONOMIC INSTITUTIONS OF CAPITALISM* 47 (Free Press, 1985).

²⁹ As Paul Joskow explained:

According to [NIE], when exchange involves significant investments in relationship-specific capital, an exchange relationship that relies on repeated bargaining is unattractive. Once the investments are sunk in anticipation of performance, “hold up” or “opportunism” incentives are created *ex post* which, if mechanisms cannot be designed to mitigate the parties’ ability to act on these incentives, could make a socially cost-minimizing transaction privately unattractive at the contract execution stage. A long-term contract that specifies the terms and conditions for some set of future transactions *ex ante*, provides a vehicle for guarding against *ex post* performance problems.

Paul L. Joskow, *Contract Duration and Relationship-Specific Investments: Empirical Evidence from Coal Markets*, 77 *AMER. ECON. REV.* 168, 169 (1987) (citations omitted).

³⁰ As Josh Wright has explained, reputational sanctions and contractual flexibility sometimes go hand-in-hand, but they do not prevent the possibility that “transactors ‘hold up’ their trading partners by taking advantage of unspecified elements of performance and attempting to appropriate the available quasi-rents resulting from relationship-specific investment.” Joshua D. Wright, *Benjamin Klein* 10 (George Mason Law & Econ. Research Paper No. 08-31), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1143568.

Internet backbone, concerns related to “hold out” tactics can arise when firms do not respect the emerging norms of how to exchange traffic. Over the last few years, Cogent has seen fit to challenge those norms on a number of occasions and, when it has played a game of chicken with other backbone operators, it has sometimes left Internet users (both those connected to Cogent and those using the other affected networks) with degraded service as a result.³¹

B. Preventing Hold Out and the Search for Institutional Solutions

In the Internet ecosystem, the contractual environment, the relevant norms, and the regulatory requirements are all in flux. This state of affairs means that businesses and policymakers need to develop an optimal strategy for guarding against opportunism. To be sure, one could suggest that businesses will negotiate a maze of contractual arrangements, but such a path would require both a degree of business acumen as well as regulatory restraint (during the time when such arrangements are developed) that may be too much to expect. Alternatively, the affected firms might see an opportunity to develop a new institutional model that provides for an ongoing reassessment of appropriate norms and standards of conduct that all parties (including regulatory authorities) trust as grounded in good faith and fair dealing.³²

The affected parties may well mutually benefit from the establishment of an enforcement institution for policing compliance with network management standards. By committing to participate in such a regime, firms could demonstrate their good faith and compliance with applicable standards of conduct in an environment where not all parties will be aware whether all firms are complying with the relevant conduct standards.³³ Admittedly, other dynamics—such as

³¹ See, e.g., Alex Goldman, *The Cogent-Level 3 Dispute*, ISP-PLANET, Oct. 7, 2005, available at, http://www.isp-planet.com/business/2005/cogent_level_3.html.

³² In referring to an “institution,” this report uses the concept as described by Douglass North:

Institutions are the humanly devised constraints that structure political, economic and social interaction. They consist of both informal constraints (sanctions, taboos, customs, traditions, and codes of conduct), and formal rules (constitutions, laws, property rights). Throughout history, institutions have been devised by human beings to create order and reduce uncertainty in exchange.

DOUGLASS C. NORTH, INSTITUTIONS, INSTITUTIONAL CHANGE AND ECONOMIC PERFORMANCE 97:

³³ As Douglass North explained:

Without complete information . . . cooperative solutions will break down unless institutions are created that provide sufficient information for individuals to police deviations. There are two parts to an institution’s assuring cooperation. First, it is necessary to form a communications mechanism that provides the information necessary to know when punishment is required. By making available the relevant information, institutions make possible the policing of defections. Typically they economize on information so, for example, players need no longer know the entire past history of any partner. Second, because punishment is often a public good in which the community benefits but the costs are borne by a small set of individuals, institutions must also provide incentives for those individuals to carry out punishment when called on to do so.

Id. at 57. Jonathan Sallet added a similar perspective, suggesting, with respect to the establishment of a self-regulatory organization that:

Isn’t the implicit assumption that there’s no mechanism of contract practice that could fill these lines? To be sure, the transaction costs are very high. But I think it’s worth thinking why contract couldn’t work. Often times we talk about self-regulation by industries that all begin with the same

a party's reputation—could theoretically provide parties with some level of assurance. An effective enforcement institution, however, can both substitute for the need to rely on such proxies and operate where those proxies would not be relevant or effective.³⁴ In short, as a number of NIE scholars emphasize, “institutions matter” and the strategy that emerges to address this issue will have a significant impact on the Internet economy.³⁵

Whatever set of practices, rules, and processes address network management issues, they will collectively constitute an institutional environment. In this sense, it is important to appreciate that institutions “should be understood as the mix of regulatory systems, property and contract rights, and informal norms and customs.”³⁶ Stated differently, a careful institutional analysis appreciates that the reality on the ground does not simply reflect the formal legal rules and processes, but also appreciates the role of informal norms and understandings that can either increase or decrease the levels of trust of the affected parties. As Douglass North put it, “creating an institutional environment that induces credible commitment entails the complex institutional framework of formal rules, informal constraints, and enforcement that together make possible low cost transacting.”³⁷

The development of a new institutional environment is both daunting and promising. It is challenging insofar as parties are likely to maintain past perspectives and attitudes, making change difficult. Nonetheless, whereas the FCC has an established profile and parties are accustomed to dealing with the agency in certain ways, a newly chartered self-regulatory body could develop its own cultural environment. Such an entity, moreover, would be situated within the broader institutional environment of other Internet bodies—such as the Internet Society, the Internet Engineering Task Force, and the Internet Architecture Board—that identify best practices, develop norms, and provide a forum for continuing communication and discussion at the engineering level. Over time, however, any newly chartered institution would take on a life of its own and generate “a self-sustaining system of shared beliefs about a salient way in which the [relevant] game is repeatedly played.”³⁸ To explain the context for such an institution, the next part discusses the history of network management issues and how a self-regulatory institution could operate in this environment.

interest and try to then keep themselves from doing what they shouldn't be doing. The advantage of contract as a way of thinking, is that it suggests not just a single set of homogeneous industry players; rather it contemplates a very creative process among people who, by definition, have diverse interests. It may therefore create a more robust system that achieves consensus between entities that inhabit different parts of the value chain, suppliers, customers and competitors.

³⁴ In the terminology of Oliver Williamson, the use of such an institution would be a means of addressing a particular type of a “contractual hazard” that arises when “incomplete contracts that are supported by nontrivial investments in specific assets are beset by disturbances[,]” such as uncertainty. Notably, such an institution, which could provide a mechanism for addressing changing technological conditions and could provide a level of assurance as to necessary technical cooperation, would constitute a safeguard that would “infuse order and thereby reduce conflict and realize mutual gains.” Oliver E. Williamson, *Why Law, Economics, and Organization?*, 1 ANN. REV. L. SOC. SCI. 369, 379 (2005).

³⁵ See MASAHIKO AOKI, TOWARD A COMPARATIVE INSTITUTIONAL ANALYSIS 1 (MIT Press, 2001) (“[I]t has been increasingly recognized that ‘institutions matter’ for understanding the diverse economic performances of different economies, and when the phrase is cited, the reference is not always limited to markets.”).

³⁶ *Id.* at 1-2 (emphasis in original).

³⁷ NORTH, *supra* note 28, at 58.

³⁸ AOKI, *supra* note 31, at 10 (emphasis in original).

IV. Network Management and Self-Regulation

The concept of network neutrality was outlined in a paper authored by Tim Wu and later embraced, in a speech by Michael Powell, as “Internet Freedom.” In articulating what he viewed as the four essential Internet freedoms—(1) freedom to access content; (2) freedom to use applications; (3) freedom to attach personal devices; and (4) freedom to obtain service plan information—Powell reserved the right to broadband providers to manage their networks. In particular, he recognized “that network operators have a legitimate need to manage their networks and ensure a quality experience, thus reasonable limits sometimes must be placed in service contracts.”³⁹

Whereas Powell’s remarks were informal guidance to industry, Chairman Kevin Martin, Powell’s successor, elevated the importance of this concept when the FCC issued a policy statement that adopted a modified version of these four freedoms. The policy statement was not developed with an eye to regulate broadband providers *per se*, but rather, as a guide for the agency’s “ongoing policymaking activities.”⁴⁰ And like Powell’s speech, the Internet Policy Statement made clear that the “principles we adopt are subject to reasonable network management.”⁴¹ Over the last several years (and the last year in particular), the question of what constitutes “reasonable network management” has become a pressing one, with the attendant institutional question of who should decide that issue. Section A will explain the network management issue and Section B of this Part will address the question of how a self-regulatory strategy for overseeing network management might operate.

A. The Emerging Law of Network Management

Network management is not a term whose meaning is self-evident.⁴² As a broad, working definition, however, “network management” can be understood as referring “to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems.”⁴³ As for what types of network management are “reasonable,” that standard calls for a “policy conclusion made by weighing the legitimate technological and business goals of network management with what society deems reasonable.”⁴⁴ As noted above, network providers are identifying new justifications for monitoring and managing their networks. They include the need to protect their customers from

³⁹ Powell, *supra* note 3, at 11.

⁴⁰ Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, *Policy Statement*, FCC 05-151 (Aug. 5, 2005) available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.doc. The agency did, however, ask merging companies to “voluntarily” agree to be bound by the principles. *See, e.g.*, Verizon Communications Inc. and MCI, Inc., *Memorandum Opinion and Order*, FCC 05-184, ¶ 215 (2005), available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-184A1.doc.

⁴¹ *Id.*

⁴² ALEXANDER CLEMM, NETWORK MANAGEMENT FUNDAMENTALS 5 (Cisco Press, 2006) (“As is the case with so many words, *network management* has many attached meanings.”); DOUGLAS COMER, AUTOMATED NETWORK MANAGEMENT SYSTEMS 26 (Pearson Prentice Hall, 2006) (“Unfortunately, network management covers such a broad range of networks and activities that no short definition can capture the task well.”).

⁴³ CLEMM, *supra* note 42, at 5.

⁴⁴ Ohm, *supra* 9, at 47.

spam and viruses; keep their network secure; prevent particular users from creating network congestion; ensure levels of service quality; identify and delete child pornography; and, in some cases, identify copyrighted works. Consequently, the reasonableness of a network management strategy may well depend on its particular objective (say, addressing congestion concerns as opposed to focusing on child pornography).

Of the different justifications for network management, the need to conserve bandwidth has emerged as a particularly controversial one. At one level, the core challenge is that, in an environment where end users access the Internet with an “all you can eat” pricing plan, there are only minimal incentives to conserve bandwidth. Some commentators suggest that broadband providers should respond to the increased demand by simply provisioning more capacity. In Japan, however, where Internet Service Providers routinely provide bit rates of 50 Megabits per second and above, the challenges around bandwidth management have not disappeared. Indeed, one Japanese trade association reported that 1% of all users consume approximately 50% of the backbone bandwidth by using peer-to-peer (P2P) applications like BitTorrent.⁴⁵ In the United States, broadband providers point to similar challenges, reporting that certain “greedy users”⁴⁶ threaten to undermine the levels of service quality for other users.⁴⁷ Tony Werner, Comcast’s CTO, for example, suggested that P2P applications consume 50% of “our upstream capacity and that’s after network management practices.”⁴⁸

Assuming that providers cannot simply provision their way out of the bandwidth management dilemma and that users will resent being subject to lower service quality levels on account of “greedy users,”⁴⁹ there are two, non-mutually exclusive strategies being developed for protecting non-greedy users from greedy ones. The first option, now being explored by Time Warner, is to impose some form of a “soft bandwidth cap” or usage-sensitive pricing on users, such as assessing a charge (say, \$1 per extra gigabyte) for using bandwidth above a specified amount (say, 40 gigabytes).⁵⁰ A second option is to engage in some form of traffic management.

⁴⁵ JAPAN INTERNET PROVIDERS ASSOCIATION, GUIDELINE FOR PACKET SHAPING 1 (2008), *available at* http://www.jaipa.or.jp/other/bandwidth/guidelines_e.pdf.

⁴⁶ The use of the phrase, “greedy users,” while common, suggests a negative connotation that, at least in some places, is misplaced. Consider, for example, that some “greedy users” are, in fact, “innovative users” who are pioneering and using new applications that, once bandwidth levels increase, may well become more widely adopted and commonly used. Nonetheless, this report will follow popular usage and use the term “greedy users.”

⁴⁷ Chris Bowick, CTO of Cox, for example, noted that one uploader transferred 681 gigabytes of data over a month (888 hours of video) and that another downloader transferred 1.5 terrabytes of data (1,833 hours of video). Cynthia Brumfield, *Comcast CTO: P2P Uses Half of Upstream Capacity*, IP DEMOCRACY, June 25, 2008, *available at* http://www.ipdemocracy.com/archives/003018comcast_cto_p2p_uses_half_of_upstream_capacity.php.

⁴⁸ *Id.*

⁴⁹ This is, admittedly, a big assumption. For telephone company networks, which may offer dedicated capacity as opposed to shared capacity connections, the issue may be far less of a concern. For cable and wireless networks, however, the challenges around bandwidth management are real. In the wireless context, for example, some companies have banned P2P applications altogether. See Ted Hearn, *AT&T Bans Wireless P2P*, MULTICHANNEL NEWS, July 28, 2008, *available at* <http://www.multichannel.com/article/CA6582213.html>.

⁵⁰ Ryan Paul, *40GB for \$55 per Month: Time Warner Bandwidth Caps Arrive*, ARS TECHNICA, June 3, 2008, *available at* <http://arstechnica.com/news.ars/post/20080603-40gb-for-55-per-month-time-warner-bandwidth-caps-arrive.html>.

It is the way in which Comcast implemented the latter strategy that led to the FCC investigation and the decision against them. Nonetheless, as Free Press's Derek Turner points out, there is a third way of addressing congestion concerns—contacting customers directly or restricting available bandwidth at specific times of day.⁵¹ While such strategies may be particularly appropriate if the concern related to congestion arises only during particular times of day, it remains to be seen what strategy, either on its own or in combination with others, will be most effective.

As policymakers begin evaluating—in the wake of the Comcast decision—how to oversee network management issues, they should do so with a clear eyed view of the limitations inherent in any particular institutional strategy. They should appreciate the ultimate impact of restricting too closely network management strategies—providers may well instead gravitate toward bandwidth caps. To be sure, some network neutrality proponents may be comfortable with that result; Tim Wu, for example, explained that bandwidth caps may be “the fairest system going,” noting that “the psychology of knowing that you’re paying for bandwidth may change behavior.”⁵²

The possible advent of soft bandwidth caps or usage charges, whether spurred by FCC network management regulation or other forces, is not welcomed by many technologists and policy observers. Om Malik suggests, for example, that such a system is “the enemy of innovation.”⁵³ Making a similar point, Vint Cerf, Google's Chief Internet Evangelist, has commented that bandwidth caps could “end up creating the wrong incentives for consumers to scale back their use of Internet applications over broadband networks.”⁵⁴ Instead of implementing such caps, Cerf recommends that companies introduce “transmission rate caps, which would allow users to purchase access to the Internet at a given minimum data rate and be free to transfer data at least up to that rate in any way they wish” and that might allow faster speeds when the network is not congested.⁵⁵ Significantly, this model of network management is

⁵¹ Policy Brief by S. Derek Turner, *Blocking or Metering: A False Choice*, FREE PRESS, Aug. 2008, available at http://www.freepress.net/files/Blocking_or_Metering_A_False_Choice.pdf.

⁵² Cecilia Kang, *Comcast Illegally Interfered With Web File-Sharing Traffic, FCC Says*, WASH. POST, July 30, 2008, at D1.

⁵³ See Om Malik, *Why Tiered Broadband is the Enemy of Innovation*, GIGAOM, June 4, 2008, available at <http://gigaom.com/2008/06/04/why-tiered-broadband-is-the-enemy-of-innovation/>. In particular, Chris Albrecht suggested that metered bandwidth could protect legacy video services far better than the network management techniques used by Comcast and objected to by the FCC, highlighting that “[i]f metered access becomes standard, there will come a day when you spend less time watching videos, and more time counting the number of videos you watched to avoid going over your cap.” Chris Albrecht, *Warning Sign: Metered Broadband Already a Hassle*, GIGAOM, Aug. 2, 2008, available at <http://gigaom.com/2008/08/02/warning-sign-metered-broadband-already-a-hassle>. See also Allan Leinwand, *Why Metered Broadband is Bad for Microsoft, Google & Us*, GIGAOM, July 17, 2008, available at <http://gigaom.com/2008/07/17/why-metered-broadband-is-bad-for-microsoft-google-us/>.

⁵⁴ Vint Cerf, *What's A Reasonable Approach For Managing Broadband Networks?*, GOOGLE PUBLIC POLICY BLOG, Aug. 4, 2008, available at <http://googlepublicpolicy.blogspot.com/2008/08/whats-reasonable-approach-for-managing.html>.

⁵⁵ *Id.* As noted above, Cerf's focus on the relevance of peak versus non-peak congestion is important. After all, a pure cap on bandwidth only focuses on total network congestion and does little to address concerns about congestion at particular times of the day.

similar to the approach that emerged from the discussions between Comcast and BitTorrent.⁵⁶ In short, it is clear that the relevant issues are technical, complex, and dynamic, making any broad pronouncements by the FCC potentially dangerous and counseling for a degree of experimentation and flexibility.

However the network management issue ultimately unfolds, the FCC's Comcast decision promises to shape the future discussion of the issue. As Comcast's Joe Waz put it at the Summit, "the common law around what is reasonable network management will probably begin with us." By all accounts, Comcast's initial public handling of its network management practices was not fully transparent and its initial public reaction was clumsy.⁵⁷ Notably, Comcast did not disclose that it subjected peer-to-peer applications to any Internet management techniques, but simply warned consumers against "excess" uses of bandwidth.⁵⁸

The fact that Comcast used a form of network management that targeted P2P applications came to light when an Associated Press story reported difficulties in using BitTorrent to upload a copy of the King James Bible from a single PC equipped with a Comcast cable modem. The Electronic Frontier Foundation investigated the matter further and concluded that Comcast was using a technique that it called "packet forgery" as a means of causing peer-to-peer connections to shut down.⁵⁹ In response, Comcast defended its actions as "reasonable network management" and maintained that the company does not block the use of P2P applications but rather delays P2P uploads based on session limits in its local service areas.⁶⁰ The FCC concluded, however, that

⁵⁶ In announcing the agreement with BitTorrent, Joe Waz from Comcast noted that "no bandwidth caps are planned." More generally, Comcast committed to a collaborative process that would yield, as BitTorrent Chief Technology Officer Eric Klinker put it, "techniques that the Internet community will find to be more transparent." See Anne Broache, *Comcast and BitTorrent Agree to 'Collaborate'*, CNET NEWS, Mar. 27, 2008, available at http://news.cnet.com/8301-10784_3-9904494-7.html. In recent trials, Comcast has sought to address its network management concerns by "focus[ing] on the data (or bandwidth) consumption activity of individual customers who are [. . .] contributing to congestion [on Comcast's network.]" Comcast Frequently Asked Questions About Network Management, <http://help.comcast.net/content/faq/Frequently-Asked-Questions-about-Network-Management#what> (last visited Aug. 14, 2008). The technique measures only aggregate bandwidth consumption, not the protocol or content being used by customers. Recognizing this point, Cerf suggested that:

Over the past few months, I have been talking with engineers at Comcast about some of these network management issues. I've been pleased so far with the tone and substance of these conversations, which have helped me to better understand the underlying motivation and rationale for the network management decisions facing Comcast, and the unique characteristics of cable broadband architecture. And as we said a few weeks ago, their commitment to a protocol-agnostic approach to network management is a step in the right direction.

Cerf, *supra* note 50.

⁵⁷ The FCC's order excoriated Comcast on that score. See *Comcast Decision*, *supra* note 5, at ¶¶ 7-9.

⁵⁸ See Drew Clark, *Comcast and Freedom to Obtain Service Plan Information*, DREWCLARK.COM, Nov. 6, 2007, available at <http://www.drewclark.com/comcast-and-freedom-to-obtain-service-plan-information>; see also *Comcast Decision*, *supra* note 5, at ¶ 53 ("Comcast's claim that it has always disclosed its network management practices to its customers is imply untrue.").

⁵⁹ PETER ECKERSLEY ET AL., PACKET FORGERY BY ISPs: A REPORT ON THE COMCAST AFFAIR 1 (2007), available at http://www.eff.org/files/eff_comcast_report2.pdf.

⁶⁰ See Grant Gross, *EFF: Comcast Continues to Block P-to-P*, WASH. POST, Nov. 30, 2007, available at <http://www.washingtonpost.com/wp-dyn/content/article/2007/11/30/AR2007113001543.html> (reporting on Comcast's response). In response, EFF suggested that the claim that Comcast's network management

Comcast's choice of techniques was not reasonable because "Comcast's network management practices discriminate among applications rather than treating all equally and are inconsistent with the concept of an open and accessible Internet."⁶¹

The FCC's decision in the Comcast matter represents the beginning of what is likely to be a challenging effort to define "reasonable network management." In its decision, the FCC offered mixed signals as to how it would define this concept, suggesting on one hand that Comcast's failing was that it engaged in discriminatory conduct and used deep packet inspection (DPI), which it labeled as unacceptable behavior.⁶² At the same time, the Commission concluded that Comcast's network management techniques were unreasonable because they were "not minimally intrusive" and seemed to condone the use of network management techniques—including, presumably, deep packet inspection—when used to block "unlawful content such as child pornography or pirated music or video."⁶³ Responding to the concern that the final test of the opinion institutes a highly restrictive "strict scrutiny" standard that would, in effect, ban all network management techniques, Commissioner McDowell condemned the opinion on the ground that it adopted a standard that "all traffic must be treated equally," creating the scenario of "a congested downtown without stoplights."⁶⁴ The decision itself rejects this characterization, terming its analysis as tailored "to the particulars of the dispute at issue" and not calling for "broad, prophylactic rules."⁶⁵ Whether McDowell's depiction of the decision or its impact is ultimately proven out to be the case, he correctly highlights that the decision "generate[s] more questions than it" answers.⁶⁶ After all, it is far from clear what network management techniques

techniques did not block packets is "only true under special conditions, and is certainly not true in general." ECKERSLEY, *supra* note 59, at 5. In support of Comcast, another commentator explained:

We can think of [Comcast's restrictions on peer-to-peer traffic] as a freeway onramp that has lights on it to rate limit the number of cars that may enter a freeway. Those lights aren't there to say people of a certain race can pass through or people of a certain race must wait longer in line; everyone must wait their turn. If you didn't have the lights and everyone tries to pile on to the freeway at the same time, everyone ends up with worse traffic. Comcast doesn't block you from using BitTorrent, it simply limits the number of simultaneous uploads you can perform at once.

George Ou, *A Rational Debate on Comcast Traffic Management*, ZDNET, Nov. 6, 2007, available at <http://blogs.zdnet.com/Ou/?p=852&page=2>.

⁶¹ *Comcast Decision*, *supra* note 5, at 2.

⁶² The FCC elaborated on this point, explaining that :

While Comcast claimed that it was motivated by a desire to combat network congestion, the Commission concluded that the company's practices are ill-tailored to serve that goal for many reasons: they affect customers who are using little bandwidth simply because they are using a disfavored application; they are not employed only during times of the day when congestion is prevalent; the company's equipment does not target only those neighborhoods suffering from congestion; and a customer may use an extraordinary amount of bandwidth during periods of network congestion and will be totally unaffected so long as he does not utilize an application disfavored by Comcast.

Id.

⁶³ *Id.* at 2-3.

⁶⁴ *McDowell Dissent*, *supra* note 10, at 8-9.

⁶⁵ *Comcast Decision*, *supra* note 5, at ¶ 36. The opinion also stated that it did not institute "an inflexible framework micromanaging providers' network management practices." *Id.*

⁶⁶ *McDowell Dissent*, *supra* note 10, at 11.

are “minimally invasive”⁶⁷ or “reflect a tight fit between its chosen practices and a significant goal.”⁶⁸

In McDowell’s dissent, he calls for a self-regulatory approach based on “collaboration” and not “regulation.”⁶⁹ In so doing, McDowell may well underestimate the effectiveness of the current Internet standard-setting bodies and ascribe to them greater levels of institutional competence than they actually possess. He suggests, for example, that “[t]hese groups have remained largely self-governing, self-funded and non-profit—with volunteers acting in their own capacities and not on behalf of their employers.”⁷⁰ This suggestion ignores the fact that these groups are affected by corporate interests and are often unable to reach closure on contentious issues. The IETF, for example, wrestled for years on the appropriate means of ensuring interoperability between instant messaging services and never effectively resolved the issue.⁷¹

The discussion at the Summit underscored the limitations of and the proper role for the IETF. As explained by Doug Sicker, a CU Computer Science professor involved in the IETF, that body is not exactly chomping at the bit to address contentious policy issues. Indeed, as Jim Speta, a Northwestern law professor put it, the political science literature underscores that there is

⁶⁷ *Comcast Decision*, *supra* note 5, at ¶ 42.

⁶⁸ *Id.* at ¶ 46.

⁶⁹ *McDowell Dissent*, *supra* note 10, at 10. Commissioner Adelstein suggested a similar preference in his statement:

As providers craft their network management practices, this Order sends a strong signal about the importance of engaging industry standard setting bodies, such as the Internet Engineering Task Force, the Internet Architecture Board, and the Internet Society, which offer the best forum for resolving network management issues. It is certainly preferable for facilities-based providers and applications providers to work collaboratively, in an open and transparent manner, without the need for government intervention. To the extent that engineers can work out these issues among themselves, it obviates the need for Commission action.

Statement of Commissioner Adelstein, *Comcast Decision*, *supra* note 5, at p. 55.

⁷⁰ *Id.*

⁷¹ As I explained elsewhere,

In 1995, before the Internet became big business, private standard-setting bodies like the IETF could focus on the technical merits of proposed standards without the distorting influence of private companies that would benefit depending on the ultimate outcome. As the stakeholders in the future of the Internet become more diverse and more concerned with the impact of the Internet’s development on their profits, stable, open, and end-to-end-based standards may well become the exception, not the norm. Take the case of instant messaging, for example. Instant Messaging, or IM, relies on the Internet transport protocols and adds a Names and Presence Directory to facilitate real-time communication. Unlike email, IM providers have yet to agree on an open, interoperable protocol that enables all users of the service to reach one another. But with the high stakes in a battle to “win” this new network market, AOL has not been eager to share its network externality with others. AOL claims that its actions reflect legitimate concerns about privacy and security, but others, including the FCC, have concluded that AOL is “dragging its feet” to maintain a dominant position that might suffer in a world where IM was an interoperable service.

an engineering ethos that can prevail when bodies are removed from the setting of quasi-regulatory standards. Finally, as Sicker stated, the pace of IETF decision-making is often “slow and [it] may be getting slower” because the body seeks to reach a “rough consensus” rather than ramming items through a majority vote. Jon Peha, professor at Carnegie Mellon, and Bill Lehr, a Research Associate at MIT, both echoed that point, noting that the increased commercialization of the Internet had led the relevant standard setting bodies to become less effective over time.

B. Models of Self Regulation and Network Management

The discussion at the Summit developed an important distinction as to models of self-regulation. As Marc Berejka, Microsoft’s Senior Director of Technology Policy & Strategy, explained, there are really two forms of self-regulation: “lower case” self-regulatory bodies like the IETF, which provide valuable forums for discussion and help to develop norms; and “upper case” self-regulatory bodies—i.e., “Self Regulating Organizations,” or “SROs”—that are empowered with decision-making authority. Both forms of self-regulation are important, he emphasized, but they serve different roles. In some cases, the lower case self-regulatory institutions can be effective in advancing public policy decision-making if given an explicit mandate to do so, but, in general, such bodies are not constituted for that purpose. Moreover, lower case self-regulation can play a very important role in contexts where social norms and the diffusion of best practices are sufficiently strong that they can constrain behavior.

As Pierre de Vries noted, Ofcom, the UK telecoms regulator, suggests a different typology than that outlined by Berejka. In particular, Ofcom suggests that “self-regulation” can be understood as when “industry administers and enforces its own solution to address a particular issue without formal oversight or participation of the regulator or government.”⁷² By contrast, Ofcom defines “co-regulation” as a form of regulation where the industry wields the initial oversight responsibility, but that responsibility fits within the ambit of a public agency’s regulatory authority. In this typology, pure public regulation would be the most taxing on the public authorities and potentially the most intrusive in terms of setting and enforcing well specified rules. In terms of the choice between a model of public regulation, co-regulation, or self-regulation, Pierre de Vries suggested that “when you have an emerging industry, and everything is uncertain, it makes some sense to have a self-regulatory body without having rules set in stone.”

In terms of the U.S. tradition, the model of co-regulation can be defined as “industry self-policing through an established, independent, and credible body subject to government accountability.” Consider, for example, the Better Business Bureau’s National Advertising Division, which is designed to, and regularly does, act as a self-policing mechanism, often working in conjunction with federal agencies like the Federal Trade Commission (FTC).⁷³ In some cases, such as the MPAA’s rating system, a self-regulatory body can operate effectively under a very minimal form of government oversight—for example, to ensure that the body does not violate the antitrust laws—and establish its independence and effectiveness through its

⁷² OFCOM, INITIAL ASSESSMENTS OF WHEN TO ADOPT SELF- OR CO-REGULATION ¶ 2.17 (2008), available at <http://www.ofcom.org.uk/consult/condocs/coregulation/condoc.pdf>.

⁷³ See Jeffrey S. Edelstein, *Self-Regulation of Advertising: An Alternative to Litigation and Government Action*, 43 IDEA 509, 527 (2003) (explaining the regime and noting that only 5% of cases are referred to the FTC and other government agencies); see also Andrew Strenio et al., *Self-Regulatory Techniques for Threading the Antitrust Needle*, 18-SUM ANTITRUST 57, 57 (calling the National Advertising Division a “notable example of successful self-regulation.”).

structure and operation (as opposed to government oversight of its processes and decisions). In short, there are two key distinctions among self-regulatory bodies: (1) the presence of actual decision-making authority (as opposed to merely offering advice); and (2) accountability to a government agency (a model sometimes called “audited self-regulation”⁷⁴).

As an historical matter, the FCC has not relied on self-regulation in many contexts. Consequently, it is not a great surprise that, in its *Comcast* decision, the FCC did not think to investigate this option as a strategic tool (at least going forward). Notably, even McDowell’s emphasis on the promise of self-regulation did not highlight any past precedents of FCC superintended self-regulation. This may well reflect that the FCC has not embraced self-regulation on a broad scale like that contemplated here. As Dale Hatfield explained at the Summit, however, there are some promising self-regulatory models used by the FCC, but they operate below the radar screen and thus have not attracted much attention.

One notable FCC self-regulatory program is the use of frequency coordinators, which manage voluntary cooperation in the use of point-to-point microwave links and private land mobile radio systems. In that context, the coordinator will evaluate requests for new licenses and will certify that such new licenses will not cause undue interference to established users. Consequently, while the FCC is the authority that grants or denies licenses as a formal matter, it routinely relies on and defers to the judgment of the frequency coordinator, which facilitates cooperation around the use of the relevant licenses. As Hatfield explained, a key reason why this system works so well is that it invites the engineers to “sit down together, solve these problems, and say let’s figure out how to do it.” Notably, this model largely involves a scenario where the FCC has defined (at least to a degree) a standard of conduct (in terms of harmful interference); the network management context, by contrast, would call upon a self-regulatory organization to play a critical role in both fleshing out and adjudicating compliance with a standard of conduct.

The frequency coordination system is not perfect, but it provides an important case study.⁷⁵ Significantly, it is most effective in contexts of repeat dealing—where a refusal to cooperate in one context can later haunt a company in another—and it may be subject to abuse where a party is requesting a license in a single instance and encounters strategic behavior by the established licensees.⁷⁶ Picking up on this point, Peter Rohrbach, head of Hogan & Hartson’s Communications Practice Group, explained that mediation can work as long as there are effective backstop arrangements—say, arbitration panels—for those cases where cooperation is not forthcoming. In response, Hatfield noted that the deadlines in this process require a relatively expeditious process of dispute resolution and that the relevant standards governing what constitutes interference are reasonably well established, enabling the system to work relatively well. Moreover, Hatfield explained, the FCC respects and defers to the judgments of the coordinators, preventing parties from re-litigating the issues at the Commission. In response, Kathy Brown, senior vice president of public policy development and corporate responsibility at Verizon, responded, “If we ever got this network management as smooth as what goes on in this coordination thing, we would say ‘we’re there.’”

⁷⁴ Douglas C. Michael, *Federal Agency Use of Audited Self-Regulation As a Regulatory Technique*, 47 ADMIN. L. REV. 171 (1995).

⁷⁵ For an excellent study of this system, see John Williams, *Private Frequency Coordination in the Common Carrier Point-to-Point Microwave Service* (OPP Working Paper Series, Paper No. 21, 1986), available at http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp21.pdf.

⁷⁶ This idea is developed in Philip J. Weiser & Dale Hatfield, *Spectrum Policy Reform and the Next Frontier of Property Rights*, 15 GEO. MASON L. REV. 549, 589-91 (2008).

Another FCC-related case study in self-regulation comes from the amateur (or “ham”) radio context. In particular, the American Radio Relay League (ARRL) has an understanding with the FCC that it manages the relevant enforcement activities related to the use of ham radio. Within the ARRL, particular individuals are appointed as observers and, as Hatfield put it, “their job is to actually monitor the behavior in the amateur bands and if they see something wrong, they send you a postcard that says you were observed operating illegally.” Only in the most egregious cases will such matters ever go to the FCC, with the ARRL reporting such cases to the Enforcement Bureau. A second form of self-regulation that operates in this context is that amateur radio operators adhere to a basic social norm of attempting to minimize interference both among themselves and with consumer electronic equipment.

Unlike the FCC, the FTC has considerable experience working with models of self-regulation. Indeed, after then-Chairman Michael Powell set forth his vision of Internet Freedom at a 2004 Silicon Flatirons conference, Peter Swire, an Ohio State University law professor who served as the Clinton administration privacy czar, identified a promising avenue of potential self-regulation for the FCC based on the model used by the FTC in the privacy context. In particular, Swire suggested that Powell’s call for adherence to a set of principles, which was framed around a suggestion that the Internet Service Providers (ISPs) disclose to their customers relevant terms of service, could be enforced along the lines of the FTC’s privacy initiative. That initiative, both Swire and Paul Ohm explained, involved an effort to push Internet companies to post their privacy policies, with the expectation that the FTC would then be able to sanction any departure from those promises as a misleading business practice.⁷⁷

In relating the FTC’s initial judgment to pursue a self-regulatory strategy, Peter Swire identified three important factors that made that initial framework successful. First, the political climate made clear to the relevant actors—namely, firms operating websites—that, if they did not endeavor to follow the FTC’s vision of posted privacy policies enforced by the agency, more intrusive legislation would follow. Second, the marketplace and technological environment was changing rapidly, raising the risk that government regulation might either impede technological development or become antiquated quickly. Finally, the government had not developed the necessary expertise to superintend a regulatory regime effectively. As Swire related, the second two conditions called for humility in terms of any government regulatory program, but it was the first—the fear of regulation—that spurred the industry to action.

One of the important developments that occurred over the late 1990s with respect to Internet privacy was the commitment of both the FTC and Congress to study the issue closely before developing prescriptive regulations. Thus, not only did the FTC call upon companies to adopt privacy policies, it also conducted an influential yearly study that detailed the quantity and quality of such policies, thereby creating pressure for companies to follow its exhortation and do so in good faith. As Peter Swire related, those reports demonstrated a remarkable level of compliance with the self-regulatory initiative—the number of websites with posted privacy policies rose from 16% to 88% over the course of two years. At that same time, moreover, Congress focused in on the most compelling concern related to Internet privacy—the use of information provided by children—and crafted a law focused on that issue in particular.⁷⁸

⁷⁷ A discussion of this initiative is found in Steven Hetcher, *The FTC As Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041 (2000).

⁷⁸ In evaluating the relevant success of the FTC’s and Congress’ late 1990s Internet privacy protection strategies, it is important to appreciate that success cannot be measured in terms of 100% compliance. Notably, even a comprehensive privacy law would not be fully enforced and thus the relevant question is to

Consistent with its experience in the Internet privacy area, the FTC is much more comfortable with and inclined to examine the potential use of self-regulation.⁷⁹ In the context of network neutrality, for example, former FTC Chair Deborah Majoras has suggested that “self-regulation by broadband providers could be an effective complement to FTC enforcement of the consumer protection laws” and encouraged broadband providers to “consider such a model.”⁸⁰ This suggestion flows naturally from the FTC’s history of working with self-regulatory strategies, such as the one used to police false advertising claims, where the Better Business Bureau’s National Advertising Division—with the aid of FTC oversight—credibly enforces the rules governing false advertising.⁸¹ Similarly, the FTC’s perspective on the concerns related to online behavioral marketing reflect the caution exemplified by the agency’s earlier stance on Internet privacy, suggesting that legislation in this area is premature and that self-regulation is an appropriate initial strategy.⁸²

V. Next Steps for Policymakers and Elements of A Successful SRO

what degree does a particular regulatory regime induce the most substantial and targeted compliance with the relevant policy goals. There is, on that score, some debate as to whether the regime of self-regulation overseen by the FTC has effectively addressed privacy concerns. See, e.g., Chris Jay Hoofnagle, *Privacy Self Regulation: A Decade of Disappointment* 4, EPIC.ORG, Mar. 4, 2005, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=650804 (“Of the five Fair Information Practices endorsed by the FTC—notice, choice, access, security, and accountability—only notice can be said to be present as a result of privacy statements.”).

⁷⁹ Former FTC Chairman Bob Pitofsky explained the agency’s regard for the use of self-regulation as follows:

From a public policy perspective, self-regulation can offer several advantages over government regulation or legislation. It often is more prompt, flexible, and effective than government regulation. Self-regulation can bring the accumulated judgment and experience of an industry to bear on issues that are sometimes difficult for the government to define with bright line rules. Finally, government resources are limited and unlikely to grow in the future. Thus, many government agencies, like the FTC, have sought to leverage their limited resources by promoting and encouraging self-regulation.

Robert Pitofsky, Chairman, Fed. Trade Comm’n, Address at the D.C. Bar Ass’n Symposium: Self Regulation and Antitrust (Feb. 18, 1998).

⁸⁰ Deborah Majoras, Chairwoman, Fed. Trade Comm’n, Keynote Address at the Federal Communications Bar Ass’n Annual Meeting: *The FTC: Working for Consumers In The On-Line World* 13 (June 27, 2007) (transcript available at <http://www.ftc.gov/speeches/majoras/070627fcba.pdf>); see also FTC STAFF REPORT, BROADBAND CONNECTIVITY, COMPETITION POLICY 136 (2007) (recognizing the potential for such an approach, noting that “the Commission applauds industry self-regulation.”) [hereinafter *Broadband Connectivity*].

⁸¹ See Edelstein, *supra* note 73, at 527.

⁸² As one report highlighted, Lydia Parnes, the FTC’s Director of Consumer Protection has called for self-regulation in the area of behavioral advertising, suggesting that a the institutional of regulations would be premature. See Saul Hansell, *The F.T.C.’s Bully Pulpit on Privacy*, BITS.BLOGS, July 21, 2008, available at <http://bits.blogs.nytimes.com/2008/07/21/the-ftcs-bully-pulpit-on-privacy/> (“With a market that is changing as quickly as Internet advertising, there is a danger [. . .] in ‘taking a snapshot of the way the market works at a specific time.’”) (quoting Lydia Parnes, the FTC’s Director of Consumer Protection); see also FTC, ONLINE BEHAVIORAL ADVERTISING: MOVING THE DISCUSSION FORWARD TO POSSIBLE SELF-REGULATORY PRINCIPLES (2007), available at <http://www.ftc.gov/os/2007/12/P859900stmt.pdf>.

At this stage in the Internet’s evolution and policy development, it is clear that there is a considerable debate over what constitutes “reasonable network management” and how to determine compliance with that standard. Highlighting that very point, Verizon’s Kathy Brown added that there are really two separate issues—how to set the relevant standard (i.e., what constitutes reasonable network management) and how to determine compliance with that standard. In the wake of the FCC’s Comcast decision, there is an increasing recognition that both types of judgment calls are not hypothetical and demand some institutional strategy to address them in a way perceived as fair, effective, and legitimate. Part of what makes this question so challenging is that many of our traditional institutions are not wholly up to the task of addressing this issue.

The original Internet architecture provided an important guarantee to all stakeholders that they could “innovate without permission.”⁸³ Notably, the modular design of the Internet enabled developers of applications to create new products and service as well as allowed providers of transmission infrastructure to upgrade their facilities. The challenge for the Internet going forward is how to create institutions that assure continued innovation and the type of cooperation facilitated by the open standards of the Internet protocol suite.

For emerging competition policy issues, it is sometimes tempting to suggest that either Congress should craft a new policy solution or that policymakers should rely on the general applicability of the antitrust laws.⁸⁴ In terms of network management regulation, there are reasons to seriously question this counsel. The challenge for Congress is whether it can legislate in a complex and dynamic area where the relevant concerns are “best confronted with a scalpel, not a sledgehammer.”⁸⁵ As for the role of antitrust law, there are substantial questions about its effectiveness in this context. FTC Commissioner Thomas Rosch, for example, recently remarked that he was not at all confident that an antitrust court would conclude that blocking a rival application violates the Sherman Antitrust Act.⁸⁶ On the remedy front, FTC Commissioner Jonathan Leibowitz suggested that antitrust institutions may well be deficient in terms of

⁸³ As Lawrence Lessig has put it:

The original Internet achieved this architecture of competition unintentionally. The framers of the network’s original design were not economists. They were not focused on building an engine of economic growth. Yet that was a consequence of a technical design intended to facilitate development flexibility. A network designed to enable anyone to develop new applications to run was also a network designed to maximize competition among applications and content.

Testimony of Lawrence Lessig, Senate Committee on Commerce, Science, and Transportation, at 3 (Apr. 22 2008), *available* at http://commerce.senate.gov/public/_files/LessigTestimony.pdf.

⁸⁴ For an argument that the antitrust laws are up to addressing the issues related to network neutrality, see Jonathan E. Nuechterlein, *Antitrust Oversight of an Antitrust Dispute: An Institutional Perspective on the Net Neutrality Debate* iii (Reg-Markets Ctr., Working Paper No. 08-07), *available* at <http://aei-brookings.org/admin/authorpdfs/redirect-safely.php?fname=../pdffiles/phpGw.pdf>.

⁸⁵ Weiser, *supra* note 4, at 5.

⁸⁶ J. Thomas Rosch, Comm’r, FTC, Address at the Broadband Policy Summit IV: Broadband Access Policy: The Role of Antitrust 6 (June 13, 2008), *available* at <http://www.ftc.gov/speeches/rosch/080613broadbandaccess.pdf>. Of course, the FCC concluded that such behavior violates the Communications Act. *See Madison River*, *supra* note 24, at 1.

overseeing more technical matters like interoperability and network management.⁸⁷ Finally, it is far from clear that antitrust oversight applies in broadband markets under the *Trinko* decision.⁸⁸

The three principal institutional strategies that are now in play in terms of addressing network management issues are the role for the FCC in terms of developing rules and enforcing them;⁸⁹ the role for the FCC and FTC in terms of overseeing terms of service and consumer protection;⁹⁰ and a potential role for self-regulation. They are, to be sure, not mutually exclusive strategies and may all well be developed in the years ahead. This Part outlines and evaluates how a self-regulatory strategy built around a new self-regulatory institution would operate in this area and work in conjunction with existing regulatory authority.

A. The Vision of An SRO Focused on Network Management

One point discussed at length during the Summit was the need for any chartered SRO to be viewed as legitimate. This legitimacy, the Summit participants recognized, will emerge from at least four characteristics. First, the body must interface and relate, in some form, with established regulatory institutions (the FCC and/or the FTC). In the self-regulatory models discussed in Part IV, for example, this type of relationship was both standard and important. As Dale Hatfield put it, the presence of governmental oversight “really changes the climate, it makes people behave a little bit better, where they otherwise might not have worked together, they will be more motivated to act in good faith.” Second, the body must cooperate with and be compatible with the existing institutional environment—i.e., established institutions like the

⁸⁷ Jon Leibowitz, Comm’r, FCC, *Concurring Statement Regarding the Staff Report: “Broadband Connectivity Competition Policy”* 1 (2007), available at <http://www.ftc.gov/speeches/leibowitz/V070000statement.pdf> (“while antitrust may be a good way of *thinking* about [consumers’ “Internet Freedoms”], it is not necessarily well-suited to *protecting* them.” (emphasis in original)); see also Philip J. Weiser, *Regulating Interoperability: Lessons From AT&T, Microsoft, and Beyond*, ANTITRUST L. REV. (forthcoming 2009).

⁸⁸ See *Verizon v. Trinko*, 540 U.S. 398, 399, 412 (2004); see also Philip J. Weiser, *The Relationship between Antitrust and Regulation in a Deregulatory Era*, 50 ANTITRUST BULL. 549 (2005) (evaluating the impact of regulation on the role of antitrust in the wake of *Trinko*); see also ANTITRUST MODERNIZATION COMMISSION, REPORT AND RECOMMENDATIONS 22, 340, 360 (2007), available at http://govinfo.library.unt.edu/amc/report_recommendation/amc_final_report.pdf (deeming *Trinko* merely a refusal-to-deal case that “does not displace the role of antitrust laws in regulated industries.”).

⁸⁹ For a discussion of how the FCC could enforce competition policy principles through after-the-fact oversight, see Philip J. Weiser, *Towards A Next Generation Regulatory Strategy*, 35 LOY. U. CHI. L.J. 41 (2003).

⁹⁰ The role of consumer protection oversight is potentially very significant in overseeing network management issues, particularly as consumers may well be able to adopt tools that enable them to monitor the behavior of broadband providers. See Daniel A. Begun, *Google to Develop ISP Throttling Detector*, HOT HARDWARE, June 15, 2008, available at http://www.hothardware.com/News/Google_To_Develop_ISP_Throttling_Detector/. This report, however, will not address this issue in depth. For discussions of this issue, see Rosch, *supra* note 86, at 4; see also Weiser, *supra* note 4. See also JONATHAN L. ZITTRAIN, THE FUTURE OF THE INTERNET -- AND HOW TO STOP IT (Yale University Press, 2008) (discussing how informed users are part of the Internet ecosystem that have made the technology an important platform for innovation); Link Hoewing, *Consumer Tools for Broadband Connections*, POLICYBLOG, June 17, 2008, available at <http://policyblog.verizon.com/PolicyBlog/Blogs/policyblog/LinkHoewing9/494/Consumer-Tools-for-Broadband-Connections.aspx> (noting that, in terms of consumer protection and disclosure, “we should not forget that the Internet, especially from the consumers’ perspective, includes everything from the connection, to the computer, to the web services and applications consumers want to use.”).

IETF. As the discussion above highlights, the Summit participants recognized that such institutions are not well situated to identify standards of conduct and to oversee their adjudication, but existing Internet standard-setting bodies like the IETF should be empowered, respected, and included in any regime that would oversee network management issues. Third, the body must draw upon the expertise and knowledge in the Internet community so that it is able to render credible judgments. Finally, its legitimacy will come from operating in a transparent, effective, timely, and fair manner. Consequently, once an institution is established, it must be successful in its assigned mission from the outset—lest it fail to build the necessary respect and confidence among the key stakeholders.⁹¹

The legitimacy and effectiveness of an SRO go hand-in-hand. Notably, the ability of a governmental authority to oversee and empower a self-regulatory strategy may well greatly influence both the SRO's legitimacy and its effectiveness.⁹² A critical challenge for both businesses and policymakers is the “chicken-and-egg” question of whether the relevant stakeholders need first to form the appropriate organization or the FCC (and/or the FTC) needs first to call for the establishment of such a body. In the past, both models have worked, with frequency coordinators developing before the FCC formally empowered them and certification bodies stepping into the fray once the FCC called for their involvement to oversee its equipment attachment rules.⁹³ To be sure, both cases are less ambitious initiatives than the one contemplated here, but they nonetheless suggest that self-regulation might work in this context as well.

In terms of a self-regulatory body's charter, the Summit participants were in consensus that the questions related to network management (including the relevant disclosure of terms of service) constituted a sufficient set of issues for a body to address in the first instance. Over the long term, a successful SRO might be able to take on other complementary issues—say, disputes

⁹¹ As Dan Kahan explained, an institution can succeed in channeling disputes and maintaining adherence to social norms if it is regarded as effective. Thus, if firms or individuals

perceive that others are contributing to the collective good in question, then honor, self-respect, honesty, and like dispositions motivate most individuals to contribute to that good as well, even if doing so is personally costly. If, in contrast, they perceive that most individuals are free riding, then pride and resentment will move most people persons to withhold contributions—and even to retaliate, if they can, against perceived shirkers—notwithstanding significant material incentives to do otherwise.

Dan M. Kahan, *Reciprocity, Collective Action, and Community Policing*, 90 CAL. L. REV. 1513, 1514 (2002).

⁹² See *Broadband Connectivity*, *supra* note 80, at 136 (suggesting that “any program of self-regulation is more effective when complemented by strong enforcement mechanisms”); see also Jodi L. Short & Michael W. Toffel, *The Causes and Consequences of Industry Self-Policing*, Harvard Business School Working Paper 15 (2007) (“our findings support a regulatory policy that recognizes the ongoing importance of government regulation and regulators to the success of private-public partnerships”); Neil Weinstock Netanel, *Cyberspace 2.0*, 79 TEX. L. REV. 447, 478 (2000) (reviewing LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* (1999) and ANDREW L. SHAPIRO, *THE CONTROL REVOLUTION: HOW THE INTERNET IS PUTTING PEOPLE IN CHARGE AND CHANGING THE WORLD WE KNOW* (1999) and arguing, based on an Internet privacy case, that self-regulatory programs only work when government oversight mechanisms are in place); Bill Ray, *Three-Quarters of EU Radio Equipment is Non-Compliant*, THE REGISTER (UK), July 10, 2008, available at http://www.theregister.co.uk/2008/07/10/eu_radio_compliance_testing/.

⁹³ See Williams, *supra* note 75, at 1; see also Warren G. Lavey, *Telecom Globalization and Deregulation Encounter U.S. National Security and Labor Concerns*, 6 J. TELECOMM. & HIGH TECH. L. 121, 143-45 (2007).

related to interoperability between users of the Session Initiation Protocol (necessary to enable Voice over Internet Protocol) or Internet backbone interconnection issues. For present purposes, however, the issues related to network management are sufficiently pressing and poised for resolution by a capable institutional actor that the participants suggested a sole focus on such issues was appropriate.

In terms of the role of a newly established SRO, the participants concluded that such a body should be tasked with a three-fold set of discrete duties. First, they suggested that a newly established SRO could acknowledge and agree upon clear and enforceable standards of conduct. In so doing, the participants underscored—as later highlighted in connection with the discussion in the wake of the FCC’s Comcast decision—that developing standards of conduct for network management is a nuanced and complex matter. One option for broadband providers seeking to avoid the legal issues around using network management techniques would be to opt for usage-based pricing strategies for broadband service. As noted above, however, some fear that metered pricing could lead to suboptimal incentives for consumers and, in any event, it is not clear that pricing and bandwidth cap schemes can completely obviate the need for network management techniques insofar as such strategies do not focus on peak versus non-peak congestion. Thus, as Vint Cerf has suggested, there may be an important role for developing nuanced approaches to network management.⁹⁴

As envisioned by the Summit participants, an SRO would need to be sensitive to the importance of and work in conjunction with existing bodies to identify emerging norms and evaluate where standards of conduct can be established. In particular, an SRO in this area would need to appreciate the three-way nature of the issue (i.e., involving broadband providers, applications developers, and end users), as CableLabs General Counsel Lee Zieroth put it. After all, the Internet can only reach its potential if end users, applications developers, and broadband providers are all working cooperatively with one another. To that end, it may be the case that applications will be able to perform better and networks may be more reliable if each party takes particular steps. By providing an effective forum for discussion and codification of conduct standards, such a body can also advise consumers and applications on best practices that will create a better experience for them.

Second, an SRO could be available for issuing advisory opinions. The ability of companies to seek advisory opinions would provide a mechanism for broadband providers (and others) to seek clarification about whether practices were reasonable under relevant conduct standards. By so doing, providers could investigate different options with a level of assurance about their legality and be less likely to turn to bandwidth caps on the theory that such caps are clearly legal (even if, on the views of Vint Cerf and others, they are most unfortunate).⁹⁵

⁹⁴ To that end, Cerf praised the work that Comcast had done in conjunction with recognized standards bodies, like the IETF, and suggested that there are opportunities for developing more nuanced approaches to network management. *See Cerf, supra* note 54.

⁹⁵ As Kevin Werbach explained, for example:

[T]he order seems designed to encourage broadband providers to shift to bandwidth caps and metered pricing, as GigaOm, DSLReports, and others have noted. By acting in this way, the FCC could head off nascent industry collaboration efforts between P2P providers and broadband operators, such as the P4P standard. Rather than forcing a serious examination of the connection between what broadband operators are doing and the legitimate network management challenges they face, this order creates a safe harbor zone for practices that may be more damaging than Comcast’s experimental “throttling.”

Finally, an SRO could be chartered and authorized by the agreement of the relevant parties to adjudicate claims that broadband providers failed to comply with the relevant conduct standards. In theory, the FCC can also act as an adjudicator of competing factual claims, but, in practice, its capabilities to do so are underdeveloped. In the FCC’s *Comcast* decision, the agency employed no real means of ascertaining the relevant facts at issue. By contrast, an arbitration type mechanism could act under specified time periods with technically knowledgeable, independent, and non-political decision-makers. Such individuals would, in contrast to the FCC, be relatively insulated from political pressures and could focus on ascertaining the relevant factual issues through an effective adjudicative process.⁹⁶ To be sure, as noted above, the FCC could theoretically operate in this fashion, but the fact that it did not do so is telling.⁹⁷

Taken together, the three principal responsibilities of a newly chartered SRO—to identify relevant norms and establish standards of conduct, issue advisory opinions, and adjudicate disputes about compliance with the relevant standards—would provide a framework for guiding all involved parties about what forms of network management were reasonable. Unlike a framework superintended by the FCC, such a model would allow for greater levels of flexibility and adaptable rules. Even though not managed directly by the FCC (or the FTC), a self regulatory framework should allow, as a number of commentators have emphasized, for FCC (and/or FTC) oversight.⁹⁸ This oversight would enable the agency to step in if the body departs from enforcing its overarching goals (i.e., the Internet Policy Statement) effectively.⁹⁹ In short, in the absence of government action, an SRO would, as James Assey of the National Cable Telecommunications Association suggested, “institutionalize shame,” telling broadband providers to “cease and desist” from inappropriate behavior.

One issue highlighted by the participants is that such an institution would need to develop a symbiotic relationship with the relevant governmental authorities. As noted above with respect to the frequency coordinator example, it is important that the oversight agency defer to the judgments of a well-functioning SRO and not invite re-litigation of the issues at the agency level, lest it undermine the SRO’s effectiveness. At the same time, as Peter Rohrbach highlighted and the ham radio context demonstrates, the ability of the agency to adjudicate disputes effectively may well prove critical to empowering an SRO because, if the parties know that the FCC could

Kevin Webach, *The End of Network Neutrality?*, WERBLOG, Aug. 1, 2008, available at http://werbach.com/blog/archives/2008/08/the_end_of_netw.html.

⁹⁶ OFCOM, *supra* note 72, at 12.

⁹⁷ Even as far as using the notice-and-comment procedure, it would be a gross understatement to say that the agency does not meet the aspiration for how expert agencies should operate. See, e.g., *McDowell Dissent*, *supra* note 10, at 1 (“Commissioner Tate and I received the current version of the order at 7 p.m. last night, with about half of its content added or modified. As a result, even after my office reviewed this new draft into the wee hours of the morning, I can only render a partial analysis.”).

⁹⁸ Angela Campbell, for example, has stressed the importance of government oversight by suggesting that “[w]here the threat of government regulation receded – as in the case of the National News Council – self-regulation failed. Further, in cases where the credible threat of governmental regulation disappeared, so did the regulation.” Angela J. Campbell, *Self-Regulation and the Media*, 51 FED. COMM. L.J. 711, 758 (1999).

⁹⁹ Doug Michael, Professor of Law at the University of Kentucky, emphasized this point, explaining that “the [oversight] agency must have residual plenary authority to prosecute, to oversee the SRO, to pull the SRO’s authority, to write rules for the SRO.” As he explained, this is the model used by the SEC for how it manages its regulatory oversight of securities markets—as called for by Congress in the Maloney Act, which authorized the creation of the National Association of Securities Dealers, an important self regulatory organization that is now known as the Financial Industry Regulatory Authority (FINRA). See 52 Stat. 1075, 1075 (1938) (codified at 15 U.S.C § 78o (2000) and other scattered sections of 15 U.S.C.).

not or will not adjudicate matters effectively, they might be less committed to ensuring that an SRO is able and willing to do so.

B. The Implementation Challenges in Establishing an Effective SRO

The establishment of an empowered SRO would deal a blow to the respective unrealistic fantasies of both the broadband providers and applications developers. For the applications developers, there is a temptation to view the provision of bandwidth as endless, very cheap (or free), and not their problem, but rather a cost and responsibility that can be dumped on the broadband provider. For the broadband providers, there is a temptation to view the profits generated by the applications providers (or at least a piece of them) as properly theirs (although the risks, on this view, are not shared). In reality, both broadband providers and applications developers need to find a strategy for coordinating their behavior, working out differences of opinions, avoiding opportunistic behavior, and preventing misunderstandings from escalating.

In one sense, the biggest implementation challenge is for the relevant stakeholders to agree on the importance of establishing a body that defines the opportunities available to them. To appreciate just how significant this challenge is, consider the New Institutional Economist Gary Libecap's finding that, when neighboring property owners all are interested in drilling for oil, they are rarely able to cooperate to develop a framework that leaves them all better off; rather, at least as an historical matter, they each act opportunistically, attempting to drill down to reach the same bed of oil and, in the process, all end up worse off.¹⁰⁰ To be sure, there are scenarios where different participants in an overall ecosystem, such as the different companies who owned patents necessary to manufacture DVDs, are able to cooperate.¹⁰¹ It remains to be seen, however, whether that level of foresight will win the day in this context.

A number of participants suggested that the key force that might well motivate the establishment of such a body is the threat by government to establish a regime of public regulation in the absence of any self-regulatory initiative. In the case of network management, that threat is clearly not a hypothetical one, as the FCC has already acted in this area. Nonetheless, as Brad Bernthal, an Assistant Clinical Professor at CU noted, regulation by raised eyebrow can operate in this very manner. To that end, David Sohn, the Center for Democracy and Technology's Senior Policy Counsel, noted, the awareness of possible public outcries may well create pressure for a forum to assess whether a company's policies are reasonable. Although it may well take a considerable amount of focused pressure (or encouragement, as it were) from public authorities to spur the development of an SRO,¹⁰² there is—as underscored in Part III above—a powerful enlightened self-interest rationale for the companies to create such an institution. After all, such a body could be very effective in preventing the types of hold-up

¹⁰⁰ James Surowiecki, *The Permission Problem*, THE NEW YORKER, available at http://www.newyorker.com/talk/financial/2008/08/11/080811ta_talk_surowiecki.

¹⁰¹ *Id.* For the antitrust business review letter approving the creation of this patent pool, see U.S. Department of Justice Antitrust Division, Koninklijke Philips Electronics, N.V., Sony Corporation of Japan and Pioneer Electronic Corporation of Japan Business Review Letter (1998), available at <http://www.usdoj.gov/atr/public/busreview/2121.htm>.

¹⁰² Ofcom, for example, has cited that factor as particularly important, stating that “the most likely case [for establishing an SRO] is in response to fear by industry that government or a regulatory [body] will intervene in the market place[,] curbing commercial activity and raising costs for companies. Ofcom’s own research has found that most self-regulatory schemes have been established, at least in part, in response to a perceived threat of state intervention.” OFCOM, *supra* note 72, at ¶ 2.23.

behavior that could undermine the ongoing development of the Internet, thereby affecting all Internet companies.¹⁰³

Assuming that the desire to cooperate exists, one fundamental question is what form of governance will be established. It is natural that a form of governance will need to take account of the financial commitment of different players, but any system viewed as legitimate will need to ensure that those who support the organization financially are not able to control it. To that end, the individuals charged with developing standards of conduct for approval and adjudicating particular matters must be drawn from the Internet community and viewed as not partial towards particular companies or industry segments.¹⁰⁴ Moreover, as Geoff Manne, Academic Relations Manager at Microsoft, noted, the individuals who manage the body must be restrained by the body's charter so that they do not engage in mission creep.

Once the necessary commitment to establish the organization is demonstrated and a critical mass of participants has agreed to participate in and abide by the decisions of the body, the next step will be to gain the blessing of the FTC and/or the FCC. This step would also include obtaining a business review letter from the Department of Justice to establish that the organization was established in a manner unlikely to raise any antitrust concerns. In particular, the organization would need to establish its commitment to transparency, open participation (at least on specified terms), periodic exit rights for members, and, of course, a showing that the benefits of the SRO exceed any potential anticompetitive effects.¹⁰⁵

Over time, as in the frequency coordination and ham radio context, the newly established SRO will be able to develop a culture of its own. Ideally, this culture will be sensitive to the broad Internet community and welcome the type of feedback typical of the Internet's user-based culture (or wiki-nomics, as it sometimes is called¹⁰⁶). There are, to be sure, a number of particular strategies that can advance this overarching goal, including a commitment to seek comment on proposals for particular standards of conduct and the establishment of advisory committees of technical authorities. In practice, however, such steps will develop over time and will emerge to reflect new challenges and opportunities.

¹⁰³ Oliver Williamson, a leader in new institutional economics, highlights the type of mindset necessary to appreciate the value of such an institution in relating that “[i]n contrast to Machiavelli’s myopic advice to ‘get them before they get us,’ the farsighted view of contracting is to ‘give and receive credible commitments’—by providing better information and added security features that serve to infuse confidence and realize mutual gains.” Williamson, *supra* note 34, at 388.

¹⁰⁴ As Ofcom put it in discussing the potential benefits of self-regulation (or co-regulation):

There is a clear tension between the desirability of autonomous schemes and the objectives of drawing on the experience, expertise, resources and engagement of the industry within them. The benefits of self-regulation may only be realized if the scheme is respected by other stakeholders including consumer and citizen groups, government and parliamentarians. Consequently a system involving a mixture of independent lay and industry members will be appropriate in both the scheme's governing body and further operating committees.

OfCOM, *supra* note 72, at 15.

¹⁰⁵ When self-regulatory bodies are created with antitrust concerns in mind, “antitrust only rarely limits opportunities for genuine self-regulation.” Pitofsky, *supra* note 79, at 1.

¹⁰⁶ DON TAPSCOTT & ANTHONY D. WILLIAMS, WIKINOMICS: HOW MASS COLLABORATION CHANGED EVERYTHING 4 (Portfolio, 2006).

Ideally, this body will develop a reputation for independence and credibility. During the time when this body develops, it may well be a concern, as Jack Zinman, an attorney with AT&T noted, that not all of the relevant players will participate in and be subject to the body's oversight. Over time, however, this concern should dissipate if regulators provide a greater level of oversight to those who do participate in the body or if the fact of participation itself signals a level of consumer-friendliness. On that latter front, it could easily become, as Paul Glist, Co-Chair of Davis Wright Tremaine's Communication, Media and Information Technology Practice Group, highlighted, a marketing advantage for companies who commit to follow the standards of conduct on network management and consumer disclosure embraced by the SRO.

Stated more broadly, many participants emphasized that the ultimate effectiveness of the SRO will depend on its ability to ensure a broad array of participation and develop effective solutions for how to address network management. To be sure, regulatory policy can help facilitate this result by encouraging and empowering an SRO (in addition to creating incentives through the fear of alternative forms of oversight). But ultimately, it will be up to the SRO and its participants to develop strategies for overseeing bandwidth usage that will strike applications developers, broadband providers, and end users as fair, reasonable, and effective.

One point that generated some debate is how the body itself should be constituted and who should be members of the SRO. Paul Glist took the position that an SRO will be far more likely to succeed if it can create a climate of shared responsibility for capacity consumption that motivates both edge providers to develop applications that behave responsibly and broadband service providers to design their networks to perform predictably with respect to "well behaved" applications. Dissenting from this view, Peter Rohrbach suggested that facilitating an environment of shared responsibility among diverse players would be extremely difficult—both with respect to developing a consensus on rules and even more so with respect to enforcing such rules by and among a diverse set of members. In his view, SROs are more likely to succeed if they have a singular identity of membership and an alignment of interests, whether brokers, lawyers, real estate agents, or, in this case, broadband network operators. This perspective, he suggested, counsels against any effort to include diverse third parties who would need to formally approve relevant standards of conduct or participate in enforcement actions. Challenging Rohrbach's suggestion, a number of participants highlighted that his proposed model would face its own difficulties—notably the need to find ways to incorporate the concerns of applications developers and end users. To be sure, such challenges might be overcome through the role of FCC oversight (and threat of more intrusive regulation if the SRO-based regime was viewed as ineffective), advisory bodies, or a process sufficiently open and transparent as to welcome input and invite confidence in its decision making processes. Nonetheless, the exclusion of applications developers and end users as formal participants would hardly be a risk free proposition.

The importance of the body's role with respect to assuring consumers about the quality of their Internet experience also generated considerable discussion. Notably, Jon Peha, Professor at Carnegie Mellon emphasized that the companies who subjected themselves to the oversight of this body would commit not only to being transparent with their consumers about their terms of service, but also to being held accountable for any departures from those representations or network management standards deemed reasonable by the SRO. As Jim Speta, a law professor at Northwestern, explained, this is the model used by Underwriters Laboratories, where compliance with the applicable requirements is enforced through an ongoing certification process that enables the UL symbol to be displayed on the relevant product. On that point, Corryne McSherry, Staff Attorney at the Electronic Frontier Foundation, underscored that consumers "don't just want to feel safe, they want to be safe; they don't just want to know about what the applications are, but

they want to be able to do the things they want to do.” Insofar as this body provided important assurances to consumers, McSherry concluded, it could serve a very valuable function for the Internet community as a whole.

A final determinant of an SRO’s success will be its ability to both attract and adjudicate effectively complaints that companies have engaged in unreasonable forms of network management. David Sohn noted that it took some time before Comcast’s practices came to light, and it might be a perennial challenge for outsiders to identify a company’s network management activities. In principle, companies could be asked to certify to their use of reasonable network management through regular audits, but there are no guarantees that such a system would be fully effective.¹⁰⁷ Thus, the most promising strategy for identifying questionable practices may well be the ability of informed users (and applications developers) to employ tools that reveal whether, for example, their traffic is subject to being throttled. To that end, Rick Whitt, Google’s Policy Counsel, suggested that the amateur auxiliary analogy might be a promising one insofar as self-appointed users could police the behavior of broadband providers effectively using applications made available by Google and others.¹⁰⁸

VI. Conclusion

The appropriate strategy for Internet regulation continues to raise challenges for policymakers. The accepted, but often unspoken, fact that the “hands off the Internet” era is over only underscores the challenging questions ahead. That the federal government is rightly concerned about the Internet’s development only begs the question of what policy tools should be used to oversee an increasingly important—and perhaps our most important—platform for delivering to consumers all forms of information, communications, and, increasingly, entertainment. The government, however, is not alone in seeking solutions for vexing Internet challenges. Indeed, part of why the government may end up getting more involved in overseeing issues like network management is that the relevant parties—applications developers, broadband providers, and end users—may fail in their efforts to develop fair, reasonable, and effective solutions to such issues.

The opportunity to develop an SRO focused on network management issues is one that, in all likelihood, will arise only if a government agency strongly encourages this step or a set of relevant parties begin building the trust and comfort level necessary to establish an institutional framework for addressing the set of issues related to network management. Such an institution, if designed and managed appropriately, holds great potential as a tool to improve regulatory policymaking and oversight in this area. By setting out the opportunity and rationale for such an institution, this report seeks to lay the groundwork for future discussions in this area. Indeed, whether or not policymakers or stakeholders pursue a self-regulatory model in the network management context, the considerations discussed in this report also highlight why they would do well to consider such a model in other dynamic contexts where establishing well specified rules raises the risk of giving rise to unintended consequences or ineffective regulations. A virtue of testing the model in this context, however, is that the issue is ripe for some institutional framework that, if it can build trust and credibility among the relevant stakeholders, could be replicated, adapted, or extended to address other issues as well.

¹⁰⁷ See, e.g., Ray, *supra* note 92.

¹⁰⁸ See Begun, *supra* note 90; The Electronic Frontier Foundation also has a tool called the Switzerland Network Testing Tool, available at <http://www.eff.org/testyourisp/switzerland>.

APPENDIX A: Conference Attendees

James Assey	Executive Vice President, National Cable & Telecom. Association
Marc Berejka	Senior Director of Technology Policy & Strategy, Microsoft
Brad Bernthal	Associate Clinical Professor, the University of Colorado Law School
Kathy Brown	Senior Vice President of Public Policy Development and International Government Relations, Verizon
Pierre de Vries	Senior Adjunct Fellow of the Silicon Flatirons Center at the University of Colorado, Boulder
Kyle Dixon	Partner, Kamlet Shepherd & Reichert, LLP
Ray Gifford	Partner, Kamlet Shepherd & Reichert, LLP
Paul Glist	Partner and Co-Chair of the Communication, Media and Information Technology Practice Group, Davis Wright Tremaine
Dale Hatfield	Adjunct Professor, the University of Colorado, Boulder
Bill Lehr	Research Associate, the MIT Communications Futures Program
Tom Lookabaugh	CEO of Polycipher
Geoff Manne	Academic Relations Manager (Law & Economics) for Microsoft
Corrynne McSherry	Staff Attorney, the Electronic Frontier Foundation
Doug Michael	Edward T Breathitt Jr. Professor of Law, the University of Kentucky
Paul Ohm	Associate Professor of Law, the University of Colorado Law School
Jon Peha	Professor, Department of Electrical and Computer Engineering at Carnegie Mellon
Peter Rohrbach	Partner, Hogan & Hartson
John Ryan	Assistant Chief Legal Officer, Level 3 Communications
Jon Sallet	Partner, Glover Park Group
Doug Sicker	Associate Professor, Computer Science at the University of Colorado at Boulder
David Sohn	Senior Policy Counsel and Director of the Project on Intellectual Property and Technology, Center for Democracy & Technology
Jim Speta	Professor of Law, Northwestern University Law School

Peter Swire	C. William O'Neill Professor of Law, Moritz College of Law at Ohio State University
Joe Waz	Senior Vice President of External Affairs and Public Policy Counsel, Comcast
Phil Weiser	Professor at Law and Executive Director of the Silicon Flatirons Center, University of Colorado Law School
Rick Whitt	Washington Telecom and Media Counsel, Google
Lee Zieroth	Senior Vice President and General Counsel, CableLabs
Jack Zinman	General Attorney, AT&T