9-2006

The Benefits and Risks of Mandating Network Neutrality, and the Quest for a Balanced Policy

Jon M. Peha
Carnegie Mellon University, peha@andrew.cmu.edu

Published In
34th Telecommunications Policy Research Conference.

34th Telecommunications Policy Research Conference, Sept. 2006

The Benefits and Risks of Mandating Network Neutrality, and the Quest for a Balanced Policy

Jon M. Peha[1]
Carnegie Mellon University

Abstract

A fundamental issue in the network neutrality debate is the extent to which network operators should be allowed to discriminate among Internet packet streams to selectively block, adjust quality of service, or adjust prices. This paper first reviews technology now available for traffic discrimination. It then shows how network operators can use this technology in ways that would make the Internet less valuable to Internet users, and why a network operator would have financial incentive to do this if and only if it has sufficient market power. A particular concern is that network operators could use discrimination to extract oligopoly rents from upstream markets that are highly competitive. This paper also shows how network operators can use the very same technology to discriminate in ways that benefit Internet users, as well as the network operator. Thus, network neutrality supporters are right to fear unlimited discrimination in some cases, while network neutrality opponents are right to fear a policy that imposes strict limits on discrimination. From this, we argue that the network neutrality debate should be refocused on the search for a *balanced policy*, which is a policy that limits the more harmful discriminatory practices in markets where there is insufficient competition, with little interference to beneficial discrimination or innovation. We apply this balanced policy in a few controversial scenarios as examples. There has been too little attention on the possibility of a nuanced balanced policy, in part because the network neutrality debate is focusing on the wrong issues. This paper argues that the debate should shift towards the complex details of differentiating harmful discrimination from beneficial discrimination, and away from high-level secondary questions like whether discrimination is inherently just, who ought to pay for certain Internet services, how important general design principles are, what abstract rights and freedoms consumers and carriers deserve, or whether network operators can give their affiliates special treatment. Reality is more complex than these questions would imply, and none of them will serve as a basis for a sufficiently specific and effective policy.

[1] Jon M. Peha, Carnegie Mellon University, Associate Director of the Center for Wireless and Broadband Networking, Professor of Electrical Engineering and Public Policy, peha@cmu.edu, www.ece.cmu.edu/~peha and www.epp.cmu.edu/httpdocs/people/bios/peha.html

Section 1: Introduction

As the Internet approaches its 40th birthday, "network neutrality" has suddenly become its most controversial issue. Why now? One reason is that the technology itself has been changing, giving networks extensive abilities to treat some classes of traffic differently from others. As we will show, some forms of this discrimination could harm Internet users, and this has many network neutrality advocates concerned. On the other hand, we will also show that some forms of discrimination enabled by the same technology would benefit users. There is therefore a danger that imposing a broadly-defined network neutrality policy could prohibit carriers from adopting these valuable practices.

The other reason why this controversy is occurring now is that competition for consumer access to the Internet has been declining. After all, if there were rigorous competition, network operators who use discrimination to harm consumers or fail to use discrimination to benefit consumers would lose customers to their rivals. Dial-up access was naturally competitive, but consumers have been switching to broadband, and most consumers currently have one or perhaps two last-mile broadband providers to choose from. At the same, attempts to encourage competition over the same physical connection have largely subsided in the US. Without competition, if there are discriminatory practices that increase carrier profits but harm consumers, then it may take regulation or the threat of regulation to deter these practices. At this point, few people are seriously advocating complete common carrier regulation of these monopoly and duopoly markets, as this could limit innovation and discourage the entry of new competitors. However, under the banner of network neutrality, policymakers could attempt to limit some discriminatory practices, as long as they believe the regulation will do less damage than the discrimination would.

Thus, policymakers face the following fundamental challenge.

Can we limit how network operators can discriminate in a manner that

- **prevents them from fully exploiting market power in ways that seriously harm users, and**
- **does not prevent them from using discrimination in ways that greatly benefit users?**

We refer to a policy that effectively balances these two competing objectives as a *balanced policy*. More specifically, we will argue that the type of discrimination that deserves closest scrutiny in a balanced policy is *discrimination that allows a provider of last-mile broadband Internet access to extract oligopoly rents from upstream competitive markets*.

To address the fundamental question above, we must understand the types of discrimination that are technically possible, their impact on users, the economic incentives carriers may have to use these techniques, and the implications for policy makers. Thus, Section 2 describes what is now technically possible with respect to discrimination. Section 3 shows how these capabilities can be used to benefit Internet users, while Section 4 shows how a network operator with sufficient market power could use the same capabilities to the detriment of users.

Of course, most advocates seem to disagree that policy should revolve around the two-part question above. The network neutrality debate has repeatedly been framed in ways that obscure this question. Instead, we hear about the inherent evils of discrimination, violations of revered

Internet traditions, the basic freedoms of consumers and divine rights of carriers, whether content providers or network operators are carrying an unfair burden, how all forms of regulation are always wrong, vertical integration and unfair alliances, and more. While some of these perspectives are useful, none of them make sufficiently clear how network operators should be allowed to use emerging technology, and all of them have distracted policy-makers from more important concerns. Thus, Section 5 summarizes and critiques some of the common ways that the network neutrality debate has been framed and mis-framed, in light of the basic challenge described above and observations from Sections 3 and 4. Section 6 discusses what an effective balanced policy might allow or prohibit. The paper is concluded in Section 7.

Section 2: The Technical Basis of Discrimination

Unfortunately, engineers, economists, and lawyers have different definitions for discrimination. In this paper, discrimination occurs whenever a network treats some network traffic or some network users differently from others.

In a packet-switched network such as the Internet, information is sent through the network one packet at a time, where a packet consists of some information to be carried across the network and some "header" information used by the network devices to make the transfer. For example, the header might indicate the sender and the recipient of the packet. A single email message or web page may yield many packets that are sent separately and reassembled at the destination. Moreover, networks are "layered" such that a higher-layer packet is stuffed inside a lower-layer packet, like a letter, placed in an envelope, which is placed in a box and mailed. The postal system uses information written on the box, but not "application layer" information inside the envelope. Traditionally, Internet packets were sent with equal priority and "best effort," i.e. with no guarantee of delivery. This is not discriminatory by the above definition.

Times have changed. There are a variety of techniques through which networks can now favor some packets or packet streams over others. We first discuss criteria that networks can now consider when deciding who should get better service. We then discuss methods they can use to give the favored group better service.

Some criteria are easier to use for discrimination than others. Among the easiest are fields in the header of an IP (Internet protocol) packet, because every IP packet contains this information, and it is easy to find within the packet. For example, this information includes the identity (or more specifically, the IP address) of the sender and recipient. Figure 1 shows some of the header fields that reveal useful information for discrimination. If the network places a device where it can monitor traffic entering the network, then that device also knows about the physical location of the source, and information in the link-layer header which could reveal who manufactured the device attached to the network. However, it is difficult to infer much about a packet stream from a single packet, and larger messages have historically only been reassembled at the destination from a series of packets, so until recently more sophisticated forms of discrimination were not practical.

Protocol	Data Field(s)	Reveals something about
Link layer protocol, such as ethernet (802.11), (802.15), DOCSIS (cable), many more	MAC address of source and destination	Manufacturer of device that is attached to network. (In some but not all cases, MAC addresses are fixed when a device is manufactured, and it is possible to identify the manufacturer from this address.)
IP	IP address of source and destination	Identity of sender, identity of recipient, location of sender, location of recipient. (e.g. was the IP address allocated through an ISP in the U.S.?)
IP	transport protocol (e.g. TCP, or UDP)	Type of application. (Some applications typically use TCP, and some use UDP.)
IP	differentiated service code point in IP version 4 / traffic class in IP version 6	Type of application, priority desired by sender. (Rarely used today. This may change when IP v6 becomes common)
IP	packet length	Type of application. (Some applications generate larger packets than others.)
TCP or UDP	source port, destination port	Type of application (e.g. port 21 for file transfer, 23 for telnet, 25 for email, 80 for web traffic, although some applications choose unpredictable port numbers and evade port filters).

Figure 1: Examples of header data that can easily be used as a basis for discrimination.

New technology has emerged that makes it practical for networks to collect much more information about a packet stream. One is *flow classification*, which is available today (e.g. [1]). By examining the sizes of packets in a stream, the amount of time between consecutive packets, and the amount of time since the packet stream began, one can make reasonable determinations about the nature of the packet stream. For example, a steady 30 kb/s stream of packets that lasts for ten minutes could be voice over IP (VOIP). Note that the network operator learns nothing about the content of the conversation, only the nature of the application. Indeed, this technique works equally well when the voice information is encrypted.

Another approach is *deep packet inspection*, which is also available today (e.g. from Cisco [2], Allot [3], P-cube [4], Packeteer [5]). Deep packet inspection is *stateful*, which means it maintains information about every packet stream going through it. Thus, it can categorize traffic based on the content of many consecutive packets in combination, rather than only what it can learn from the packet it is currently handling. A device using deep packet inspection is also aware of the information at the *application layer*, which means instead of looking only at the information needed to get the packet to its destination, such as what is in Figure 1, the device seeks to understand the data that an application software running at the destination would use. For example, that application could be a web browser, or a VOIP client, or a video display, or an

email user agent. As a result, it is possible to tell whether a packet stream is VOIP, email, web browsing, instant messaging, video streaming, file transfer, or peer to peer file sharing. It is possible to examine in detail the content of the email, or web page, or downloaded file. It is possible to distinguish music files from text from pictures. It is possible to search for keywords within any text.

All of this requires a great deal of processing, which is why cost-effective products were not available until recently, but processors are much faster and cheaper than they used to be. While it still may be challenging to do complex processing at speeds needed in the backbone links with greatest capacity, providers of last-mile broadband service can always use these techniques closer to the edge of the network where links have lower capacity. This requires more devices whose cost must be justified by increased profit, but the technical challenge becomes much easier. For example, my laboratory at Carnegie Mellon University has successfully used deep packet inspection at 150 Mb/s to determine which network applications each computer on campus is running and which remote servers they are accessing as part of an effort to determine what puts a computer at greater risk from dangerous malware. (In our work, we take many precautions to conceal the identity of the users and otherwise protect their privacy, but these precautions make the processing more complex rather than less.)

In a stateful system, every packet may cause the monitoring device to look into a database. It is not difficult to include information in these databases that is not traffic-related, such as billing information or demographic information. For example, the recipient (destination IP address) of the packet may be mapped to something that indicates that this is a premium customer who gets special treatment, or that this is a competitor to the network operator who does not.

Between deep packet inspection and flow classification, it is cost-effective for a network operator to gain unprecedented knowledge about what is happening on the network, and to selectively improve or degrade service for some. Now let us consider what advantages the network might bestow on traffic it wants to favor.

One old and simple way to favor some users is through preferred *interconnection*, i.e. to allow them to connect to the network with a higher-capacity link, or to pay less for the same capacity. This is still an option to discriminate among users, although it alone does not allow the network to discriminate among traffic from a given source.

Finer-grain discrimination is possible if it is embedded in the *traffic control* algorithms, i.e. the algorithms that control the flow of packets through the network. These algorithms can greatly influence the *quality of service* (QOS) of a packet stream. QOS typically involves the amount of time it takes a packet to traverse the network, the rate at which packets can be sent, and the fraction of packets lost along the way. For example, consider a congested communications link. Many packets must sit in a buffer, waiting to be transmitted on that link. The *scheduling algorithm* determines when each waiting packet is actually transmitted, and how often packets from a given stream are transmitted. When the number of waiting packets becomes too large, a *dropping algorithm* will select some to be discarded. A *traffic shaping* algorithm may spread packets out so they do not arrive in a single large burst. An *admission control* algorithm may block entire packet streams temporarily, on the grounds that it would not

be possible to meet QOS requirements for the current streams and the new one if this new stream were admitted. If these algorithms discriminate, they can give favored streams smaller queueing delays, lower loss probabilities, higher data rates and/or lower blocking probabilities.

Discrimination can also be built into the *routing algorithm*, which decides where a packet should be forwarded next. Some packets might be sent over the quickest and most reliable path, while others may be sent the slow way. A particularly undesirable packet may experience "black-hole routing," which has the same effect as dropping the packet entirely. In cases where there are multiple possible destinations, e.g. load balancing across multiple servers, favored packets may go to the server with the shorter line. There are even cases where packets are sent to a destination quite different from the destination specified by the sender. This is *redirection.* For example, if a user attempts to connect to a server that no longer exists, the network might redirect the packets to a different server.

Some network neutrality policies have focused on prioritization, and it is clear how prioritization is at work in the preceding traffic control algorithms. However, there can be discrimination without obvious prioritization. One can simply provide *separate channels* for different classes of traffic. For example, favored traffic may be sent over a lightly used wavelength in a fiberoptic cable, while other traffic goes over a heavily used wavelength. The channel separation can also be logical instead of physical. For example, favored traffic may be sent over a separate virtual local area network (VLAN), or a separate *service flow* in a cable system operating under the Data Over Cable Service Interface Specification (DOCSIS) standard [6]. Traffic flows over the same physical channel, but one logical channel has higher priority when competing for limited resources than another logical channel.

Of course, users care about more than QOS. They also care about *price*. Once a network operator can determine in detail what a user is doing, the operator can charge for that. Thus, a user may pay more depending on which applications she is using, who she is communicating with, or even whether she remembers to include text praising her ISP in every email. This is typically known as "content billing" or "content charging," and it too is already available in today's network products. In many ways, implementing content billing is easier than implementing discriminatory traffic control. For traffic control, one must decide almost immediately which packets to favor. For billing, one merely has to decide by the end of the month, so traffic analysis can be done off line.

Finally, a network operator might discriminate by providing unequal access to various services. For example, favored packet streams might be carried over an efficient multicast mechanism, so the sender does not have to send a separate copy of the content to every recipient [7]. This is particularly useful for those who broadcast video, music, or other content simultaneously to multiple users over the Internet. Also, some users may have better access to information caches, so the content they want can be retrieved locally rather than from a remote part of the network. Others may not be allowed to use caches associated with the network operator, or may be charged more for interconnecting their own caches.

In summary, network operators have powerful means to differentiate among network traffic, including examining packet headers, deep packet inspection, and flow classification. Once they

have used these techniques to choose what to favor, they can improve quality of service or price for the favored class through some combination of preferred interconnection, discriminatory traffic control algorithms (including scheduling, dropping, traffic shaping, admission control and routing), separate channels, content billing, and access to services like caching and multicast.

Section 3: The Benefits of Discrimination

In this section, we discuss why discrimination is valuable for both users and carriers.

One obvious use of discrimination is security. A network operator may use deep packet inspection to determine whether a packet stream is carrying a virus or a dangerous piece of spyware. A broader examination of traffic patterns may reveal that a given source is participating in a denial of service attack on another user. A network neutrality policy that prohibits networks from dropping dangerous traffic of this kind would damage network security.

Redirection in combination with deep packet inspection can further improve security. My laboratory at Carnegie Mellon University is developing tools that use deep packet inspection to identify spyware. Once detected, it is possible through redirection to send users to a web site with anti-spyware and anti-virus tools that can eliminate the threat. Redirection is also commonly used to provide useful instructions to those who try to connect with servers that are down, or to enable users to pay for wfi hotspots before they begin normal operation.

Another useful role for blocking is to deny service from an unauthorized device. By insuring that only authorized devices are attached to the network, the network can prevent customers from using equipment that will operate in "promiscuous mode" to observe their neighbors' traffic, or that consumes more of the shared resources than is allowed, or that accesses adult-only material contrary to the customer's stated wishes. (The latter might occur, for example, when a child of the customer seeks content that the customer has restricted.)

Instead of blocking packet streams, the network might discriminate with respect to quality of service, price, or both, to insure that resources will be shared fairly and no one will "starve." The ready availability of high-capacity always-on connections to the network has made it possible for a small number of users to generate the vast majority of network traffic on many commercial broadband networks, while filling some communications links to capacity. Today, peer-to-peer file transfers are the primary cause, but other applications may have a similar impact in the future. Moreover, some of these applications are not "TCP-friendly," which means when congestion occurs on these bottleneck links, these applications do not reduce their rate of transmission to allow the congestion to subside. An application like this will send out data as fast as it can, while the TCP-friendly applications deliberately send fewer and fewer packets. One Gb of traffic that is not TCP-friendly therefore degrades performance for its neighbors more than one that is TCP-friendly. Network operators may therefore wish to give traffic from these applications lower scheduling and dropping priorities, or limit the amount of traffic they can send per day, or charge them more for consuming more network resources. This discrimination benefits the applications that might otherwise be starved of network resources.

Discrimination with respect to QOS is also important because different applications have different QOS needs. For example, in a VOIP application, the recipient may play out packets 50 ms after they are first sent across the network. Thus, most packets must be received within 50 ms, as any arriving after 50 ms are useless. Best effort delivery could lead to completely unacceptable QOS for a VOIP application if there is congestion. On the other hand, for a large file transfer, there is no specific maximum allowable delay, but a low average delay is helpful, whereas for email, delay is of little importance. If sophisticated traffic control algorithms take these QOS requirements into consideration, it is possible to give packets high priority when and only when they need high priority to meet QOS requirements, thereby meeting QOS requirements for many more users on a given network. Alternatively, it is possible to serve the same number of customers at the same QOS with less network capacity, making the network less costly. This benefits Internet users and network operators.

Perhaps as a compromise, some network neutrality proposals would allow discrimination with respect to QOS, as long as there is no discrimination with respect to price [8]. Although the policy's goals are laudable, this is not effective, as users would have no incentive to accept anything less than the highest priority. Discriminatory pricing gives users incentive to provide accurate information about their real QOS needs, to avoid wasting resources, and to refrain from transmitting when the network is congested and shift usage to off peak hours. Indeed, by adjusting prices dynamically based on congestion levels, thereby convincing some users to delay their transmissions, pricing actually becomes a form of congestion control that has quantifiable advantages over more traditional technical approaches [9]. Limited resources are allocated most efficiently when price to users is a function of "cost" to network operators. In this case, cost is the opportunity cost of carrying a given traffic stream, since allocating resources to carry one stream means those resources cannot go to another stream. These costs can be quantified [10], and the cost per bit of a stream with strict QOS requirements is greater than the cost per bit when QOS requirements are lax. Moreover, all else being equal, the cost per bit of carrying traffic that arrives sporadically in large bursts is greater than the cost of carrying traffic that arrives in a steady stream, and the cost of carrying traffic that is TCP-friendly is less than the cost of carrying traffic that is not. Since the QOS requirements, burstiness, and back-off behavior of traffic are highly dependent on the application type, the public may be well served by networks that charge different prices per bit for different applications.

Unfortunately, these efficient pricing mechanisms may lead to higher prices and potentially greater profit when the network is congested than when it is uncongested. Thus, although such prices may give users incentives for efficiency, they may give network operators reason to prefer congestion, i.e. to profit from providing inadequate capacity. (More on this in Sections 4 and 6.)

Note that the incentive to discriminate with respect to QOS and price is based on the assumption that there are limited resources. In fact, a network has a choice on that. Networks can deploy far more communications capacity than is usually needed, so congestion is simply not a problem. Their reward is simple traffic control that can be run on cheaper processors, simple billing systems, and pricing that can be easily explained to customers. Alternatively, they can put money into sophisticated traffic control and billing instead of communications capacity. The best strategy depends on whether processing or communications gets cheaper at a faster rate. Throughout the 1990s, as progress in fiberoptics decreased the cost of communications at an

astounding rate, this kind of discrimination made little sense and flat-rate pricing was the dominant model. Some believe this trend will continue [11], but others disagree. Thus, there are risks in embedding this conjecture into our laws and regulations.

Section 4: The Damage From Discrimination

The previous section showed that the technologies for discrimination in Section 2 can be beneficial to users. In this section, we show how a network operator has incentive to use the same technologies to the detriment of users, if and only if it has sufficient market power. (Market power generally comes from lack of competition, although there may be cases where a network operator with competition has this power because it has monopoly control over the termination of a call [12].)

It should be noted that in some cases, Internet users can take countermeasures in response to attempts by the network operator to discriminate, and these may lead to reactions by the network operator. These countermeasures range from use of virtual private networks to conceal information from the network operator to shifting usage from home to work where there may be more competition among broadband providers. Some forms of discrimination are relatively easy to circumvent, and others are nearly impossible. The resulting arms race could affect outcomes. This is largely outside the scope of this paper, but is discussed in a companion paper [12].

Protecting Legacy Services from Competition

The dominant broadband providers are cable companies and telephone companies, who have incentive to protect their traditional offerings from video and voice over IP. In a competitive market, this would be the standard "innovator's dilemma" [13], and in time, either the market leader or an upstart rival would bring the novel IP-based product to market. However, in the absence of competition, the market leaders may prefer to stifle innovation indefinitely. Network operators can simply prohibit these rival services in their user agreements and then block the traffic. Alternatively, it is relatively simple to degrade quality of service of VOIP to the point that it cannot seriously compete with traditional telephony. The same approach is also possible with streaming video, although it is not as effective because video streaming applications can be designed to tolerate QOS that would be unacceptable for VOIP [12]. A third practical approach is simply to detect the voice or video traffic and charge extra for it, so the IP-based services are no longer a competitive threat. Vendors are already building and marketing products to network operators with the stated purpose of determining when customers use "revenue bypass" [14] applications like VOIP, and adding extra charges accordingly for this behavior.

Charging Oligopoly Rents in the Broadband Market

Obviously, a company who dominates the broadband market can exact oligopoly rents from the broadband market itself, by which I mean the market for transport of bits. Profit is maximized through perfect price discrimination, i.e. where each user is charged precisely what that user is willing to pay. Users here include consumers, businesses, and content and service providers. This implies that the *benefit of the Internet to each user is zero*.

To approach perfect price discrimination, the network operator can divide users into categories, and estimate willingness to pay within each category. The fact that the operator has extraordinary information about what each user does over the Internet, along with external information about credit, housing, and much more, should make this task considerably easier. It is as if a grocery store could adjust the price of any item based on all the food you have ever purchased, when, where, and at what price, as well as your credit history and the value of your house.

Further improvements in discrimination are possible by offering multiple services, such that those willing to pay even more for better service will choose to do so, and those who are more sensitive to price will choose the cheaper services [15]. This can be achieved by intentionally degrading the quality of service for those paying less. Equipment is already being deployed to degrade QOS for this purpose. As one vendor [16] put it, "service providers can sell the same thing to customers with different willingness to pay and therefore catch the consumer surplus." And "to maximize revenues for value added services there must be a clear perceived difference in the performance .... Bottlenecks are the foundation of this differentiation. ... Note though that bottlenecks may be actual resource bottlenecks, or managed gates in the network." Adding managed gates in a network specifically to degrade QOS would push away many customers if there were competitors who did not do this, but can be quite profitable for a network operator with sufficient market power.

Charging Oligopoly Rents in Competitive Upstream Markets

The types of discrimination described in Section 2 are particularly dangerous because a network operator can extract oligopoly rents not just in the broadband market, but in any upstream market, i.e. any market that depends on Internet access for operation. This includes electronic commerce for any and all products, communications services like VOIP and videoconferencing, information distribution markets like video streaming and MP3 music sales, on-line advertising, and network equipment that attaches to the Internet. This strategy works even if the upstream market is highly competitive. For example, there are many online bookstores. A network operator could charge extra for each book sold online by any vendor, effectively pushing total book prices to where they would be if there were only one online bookstore. (This extra charge could be paid by assigned to either consumer or content/service provider.) In the absence of competition or regulation, a network operator's ability to identify distinct upstream markets for this purpose is limited only by what the technology can reveal about the content of network traffic. As we have seen, network operators can consider the sender and recipient of the traffic, the application, the content, the time of day, and much more. Thus, not only can a network operator charge different amounts for 4-MB journal articles and 4-MB MP3 music files, but the operator can charge more for an MP3 song that is currently among the ten most popular in the country than for one that it is not. (And through its monitoring, the network operator may know more about which music is popular than anyone in the music industry does.)

Note that a network operator can effectively extract oligopoly rents from upstream markets without ever entering those markets. For example, it can charge for each iTune downloaded

without affiliating with Apple, and despite Apple's strenuous objections. However, in many cases, it might be convenient for the network operator to either enter the market for given content or service, or to partner with an affiliate who is doing so. If the network operator does have an affiliated partner, then the operator can do more than block rivals; the operator can redirect requests that were intended for one of these rivals to its partner, i.e. the customer typed the name of her favorite ecommerce site, but is instead shown the site of a competitor affiliated with the network operator.

In practice, network operators would probably focus their attention on a few upstream markets with big companies that are generating significant margins. For example, the "Cisco Service Control Solution" is advertised as enabling three steps that allow the extraction of rents from upstream markets [17]. First, analyze network traffic to identify markets to enter as either a competitor or partner to existing players. Second, adjust the QOS of the relevant traffic. This can provide incentives for the current content or service providers to partner with the network operator, even if they might not have done so otherwise. Alternatively, adjusting QOS for current providers could yield a competitive advantage if the network operator decides to compete with the current providers. Third, use content billing to charge for use of the relevant services.

Once network operators have identified the upstream markets from which they can extract greater profits, they can also attempt to match price to willingness to pay in these upstream markets, just as described previously for the broadband market. If perfect discrimination were possible, *network operators could then drive consumer surplus to zero in every upstream market* -- a terrible blow to Internet users.

Again, network operators can exploit all of the information available regarding a user's online behavior, and they have far more information than upstream content and service providers do. For example, a network operator knows more about the location of sender and receiver, and can add a surcharge to every VOIP call that depends on what telephone companies would charge for the same call, or on the credit rating of the parties involved. Even a monopoly VOIP provider would not be able to charge the user this much. Moreover, unlike firms in the upstream markets, network operators have information about multiple markets. Thus, for example, if there is a relationship between a user's interest in streaming video on demand and in peer to peer file sharing, the network operator might increase its profits by charging additional fees to those high-volume customers who do both. Even a monopolist in the streaming video market could not use such a strategy to increase profits, at the expense of Internet users.

As in the broadband market, network operators can also deliberately degrade service where it is helpful in capturing profits in upstream markets. As one equipment vendor put it, the ability to adjust QOS for each upstream market "enables revenue sharing schemes or value-based pricing rather than only 'bit retailing.'" [16]. An alternative to intentionally degrading QOS is selectively limiting applications. For example, Cisco [17] suggests offering a basic service in which all traffic other than email and web browsing is blocked. Users who want peer-to-peer file sharing would pay a surcharge, and those wanting VOIP would pay an even larger surcharge. Thus, people who want additional services would be required to pay more, even when this places no more demands on the network. They further suggest that surcharges would be waived for

content and services that come from providers affiliated with the network operator. Content billing makes all of this easy.

Note that Internet users include both consumers and content or service providers. Many network operators are considering pricing schemes through which both sides of an exchange would pay in some way for the last-mile connection to the consumer. This makes it easier to conceal how the network is differentiating among upstream markets. For example, if there is a greater difference between the monopoly price and competitive price in online book sales than in online CD sales, the network might impose greater charges on book merchants than on CD merchants. This may raise fewer objections than charging consumers who buy books differently from consumers who buy CDs.

This would also allow network operators to separately charge oligopoly prices to both sides. For example, viewers of an online newspaper could be charged based on the value of this specific news content, while advertisers are simultaneously charged based on the value of disseminating the ads to this particular set of readers. Moreover, these advertisers might have considered many online outlets, and that competition could drive down advertising rates. However, if all of these media outlets go over the same network to reach the viewer, then the network operator can charge a monopoly price where one would not otherwise have been possible.

Further Exploiting Upstream Market Failures

Market failures in upstream markets can provide additional opportunities for network operators. This is certainly the case when products in upstream markets are "sticky," i.e. there are switching costs such that once a customer has chosen that product, she will be reluctant to switch to a competitor. An important example is email. There may be little reason to choose one email provider over another, but once a customer has informed people of her email address, it can be painful to switch. Network operators can exploit this by offering an email service that is available only to customers, and then using blocking, QOS manipulation, or pricing to make rival email services inaccessible or unattractive. In a duopoly, network operators could use this technique to reduce effective competition.

There are also opportunities in an upstream market where benefits per user increase substantially with the number of users [18], perhaps because of a positive externality or a strong economy of scale. For example, the benefits per user of instant messaging increase as more people join the network. In this case, a network operator may choose to turn an upstream market into a monopoly by blocking or degrading service for rivals. As the winner becomes dominant, benefits of this system grow, and so does the extra revenue that the network operator can extract from this service. The network operator may extract this benefit from users by partnering with the dominant company, but it can extract the benefit through content billing without partnerships.

Network operators can also have incentive to block or discourage online activities that benefit the users involved, but decrease profit of someone else, i.e. for which there is a significant externality. For example, operators may block any anti-spyware software that

removes certain kinds of adware, in return for payment from the adware company and its advertisers. Similarly, network operators may block applications that legally or illegally use or disseminate certain intellectual property, in return for payments from the owner of that intellectual property.

Stifling Free Speech For Fun and Profit

A network operator with sufficient market power clearly has the ability to stifle speech, and sometimes it will have the incentive. This may be particularly important in political spheres, given the Internet's growing role in raising campaign donations, disseminating candidate information, and mobilizing volunteers. Network operators could simply limit access to web sites that are of use to candidates they oppose. This would cost far less than what these companies already spend on lobbying and campaign contributions, and it would probably have more impact.

Such limitations on political speech may seem alarmist, but there is certainly precedent. For example, in 2003, Cumulus Broadcasting and Cox Radio banned the radio play of music from the Dixie Chicks after one member criticized President George W. Bush and the war in Iraq, in spite of the fact that the multi-Grammy-winning artists had the most popular country song in the US at the time, and none of their antiwar sentiments were reflected in their songs [19]. Radio stations have the right to play only what they wish. After all, there are many radio stations, so if listeners are unhappy with the offerings of one station, they can try another. However, users of broadband Internet do not have so many options. Members of the Telecommunications Union in Canada were reminded of this during a labor dispute in 2005, when the ISP Telus blocked access to a web site that was trying to disseminate the union's views [20].

Section 5: Misleading Characterizations of the Network Neutrality Issue

There is no consensus on exactly what network neutrality means in practice, or why the issue might be important. Indeed, the most specific proposals tend to come from those who want network neutrality to sound foolish so they can discredit it. This section reviews a number of prominent characterizations of the issue. We argue that none of these should be used as the primary basis for specific regulation or legislation.

Network neutrality should not be about banning all discrimination.

As was discussed in Section 3, discrimination can be used in ways that benefit users, potentially improving security, improving quality of service, decreasing infrastructure costs, and allocating resources to those who benefit the most from them. Moreover, if discrimination were inherently bad, then it should be banned even in a highly competitive market, but there is no obvious reason for regulatory intervention if such a market existed.

Network neutrality should not be about prohibiting vertical integration or affiliate relationships.

Some discriminatory practices that harm consumers may involve vertical integration, as network operators favor their own businesses in upstream markets. However, as shown in Section 4, broadband operators could achieve similar results without vertical integration, and even without affiliating with another business. For example, a network operator can charge consumers ten cents per minute for each VOIP phone call, or even just for each Vonage VOIP phone call, without permission from Vonage. Thus, simply prohibiting network operators from providing better service to itself and affiliates accomplishes little. Moreover, banning vertical integration can do harm, as there are forms of vertical integration that may yield significant cost savings or other benefits [21, 22].

Network neutrality should not be about protecting the rights or "freedoms" of consumers.

The Federal Communications Commission endorsed four freedoms for consumers [23,24]. Under these principles, consumers should have the ability to access the legal content of their choice, run the applications of their choice, attach the devices of their choice, and receive meaningful information about their service plans. The latter was later changed to a right to competition among network providers, application and service providers, and content providers. This important step in the network neutrality debate gave us useful policy objectives to consider, and variations have been enshrined in a number of proposals for regulation and legislation. However, it is not entirely clear from these freedoms alone how to achieve the stated objectives. For example, what does it mean to have access to content? If it is possible to download a file, but at a painfully slow rate and for an extremely high price, is that acceptable access? If not, on what basis would a regulator decide whether the price is too high or the QOS too poor?

These stated freedoms also do not help the regulator when objectives clash. For example, I exercise my right to choose any application by deliberately launching a denial of service attack on my neighbor, depriving him of his freedoms. Alternatively, perhaps denial of service is not my intent, but that is the effect of my resource-intensive application. On what basis can the FCC decide whether to protect my freedom or to protect my neighbor?

Worse yet, these "freedoms" must really be met by the industry as a whole rather than a specific company. If content becomes inaccessible because two companies cannot agree on the terms of interconnection, how can the FCC decide which company has violated its customers' freedoms by making unreasonable demands? If there is no competition, who should be held responsible? Moreover, in a highly competitive market, these objectives can be met if some network operators support consumer freedoms, so how can the FCC determine who among the competing firms has acted unfairly?

These statements of rights or principles clearly have their place, but if we are to develop (or at least evaluate and discard) regulatory constraints, regulations must be based on the acceptable or unacceptable behavior of network operators rather than the inherent rights of consumers.

Network neutrality should not be about "who pays" for Internet service or infrastructure.

This issue is of great short-term interest to a few prominent stakeholders, but its broader significance is limited. Today, both consumers and content providers pay the network operator that provides last-mile service directly. Thus, if a stream passes through one commercial network, that network is paid by both parties. Otherwise, the consumer pays one network and the content provider pays the other. Some network operators have tried to argue that content providers get a "free ride" because they pay directly for one last-mile connection but not both. Of course, this is no different from cellular telephone calls in the US, where both sender and receiver pay for "air time," and we do not hear similar cries about inherent injustice Some network neutrality advocates would like to permanently enshrine this existing business model for the Internet.

On the other hand, there are network operators who would like content or service providers to pay fees for the last-mile connection to the consumer, in addition to their own last-mile connection. For example, a consumer might pay a monthly fee for her connection to the Internet, and in addition, Amazon might pay for each purchase made by the consumer over that connection. Otherwise, the network will block or degrade service for traffic from Amazon. Some self-proclaimed defenders of Internet users call this "double charging," but there are many business models where costs are shared by multiple parties who benefit. There are also communications services where one side pays disproportionally. For example, callers generally pay the full cost of long-distance telephone calls, and in some countries (other than the US), the same is true for cellular. Again, we do not hear claims that these models are inherently unjust.

Each model has its pros and cons for Internet users, as well as the network operator, and these are largely beyond the scope of this paper. One case where both consumers and content providers may benefit if the latter pays more of the last-mile costs is the distribution of free, advertiser-supported content. This business model makes it easier for the content providers, and ultimately the advertisers, to pay the communications costs. This saves consumers money, and potentially allows advertisers to reach more people. On the other hand, if a consumer *purchases* the content, it should not matter to the consumer whether she pays the network directly, or she pays the content-provider who then pays the network (except where transaction costs are different).

Thus, a shift in who pays is not always bad for Internet users, but in some cases it could be. As demonstrated in Section 4, a network operator with market power may be able to adopt discriminatory pricing models that are more harmful to consumers if that operator has the flexibility to charge both sides whatever the market will bear on a discriminatory basis. For example, a provider of VOIP services might be charged more than a provider of videoconference services, even though the latter clearly requires more network resources. Thus, it is the exertion of market power through discrimination that we must watch for.

Proposals to treat consumers differently from service or content providers create another risk. They assume that consumers cannot also provide content or services, which may actually sanction network operators to reduce the choices available to consumers. Can't a proud parent run a server that gives the world access to baby pictures?

Network neutrality should not be about whether network operators can differentiate their services.

Differentiation is not a big issue in regions with only one broadband provider, but if rigorous competition were ever to emerge, some fear that a network neutrality policy would prevent a network operator from offering a unique set of services, and this would turn broadband access into a commodity [25]. One partially avoids this problem by adopting a policy that imposes no constraints if competition emerges. Moreover, if a network neutrality policy only limits discrimination that exploits market power in the last mile, there are still ways for carriers in a duopoly to differentiate themselves. For example, offering proprietary content as AOL did in the dial-up market would be allowed, provided that the network does not discriminate in favor of this proprietary content.

Network neutrality should not be about preserving the traditional "end to end design principle."

Under the end-to-end design principle [26], the network provides relatively simple services, while much of the complexity of providing sophisticated services is born by the devices at the edge of the network. This principle has served the Internet well. Among other things, it has facilitated innovation at the edges of the network [27, 28]. However, as discussed in Sections 2 and 3, there has already been a shift away from this principle for sound technical reasons. For example, networks use virus detection mechanisms that improve network security, and caching mechanisms that improve performance. Thus, the shift is not inherently bad. It should become a concern if network operators use this shift to limit the use of new kinds of devices at the edge. Usually, network operators would encourage any innovation that makes broadband services more valuable, but not when they are trying to extract oligopoly rents, as discussed in Section 4. It is therefore the latter that we should watch for.

Section 6: Defining a Balanced Net Neutrality Policy

So what should a network neutrality policy be about? We have argued that it should balance two objectives. Based on the results of Section 4, the policy should limit discriminatory practices that allow network operators to exploit their market power to significantly harm Internet users. Impact on upstream markets is especially important, because it is harder to prevent network operators from extracting oligopoly rents in the broadband market itself without onerous regulation, and because the potential consumer surplus that could be extracted in all of the upstream markets combined is probably far greater than that of the broadband market alone. Based on the results of Section 3, the policy should try not to interfere with the network operators' ability to use discrimination that benefits users.

It remains to be seen exactly how these objectives can be balanced. It may be impossible for a policy to prohibit *all* forms of harmful discrimination and allow *all* forms of beneficial discrimination, but perfection need not be the goal. We can start by preventing the most harmful cases. A reasonable heuristic may be possible from the following observations. To extract oligopoly rents in upstream markets, a network operator will exploit differences in willingness to

pay from one upstream market to another, which means the differences in network prices across these upstream markets will not reflect the costs of providing the service alone. Thus, we might allow discrimination, but seek evidence of prices that are out of line with underlying costs as a possible sign of more harmful forms of discrimination. While it is difficult to quantify the "cost" of carrying a given stream, it is much easier to determine which of two streams would cost more, and regulators can make use of such comparisons This leads us to the following properties, which deserve serious consideration as part of a balanced policy.

A policy designed to protect beneficial uses of discrimination might allow the following.

- Network operators could provide different quality of service to different classes of traffic, using explicit prioritization or other techniques. These techniques can be used to favor traffic with stricter quality of service requirements, and/or traffic sent using a higher-priced service.
- Network operators could charge a different price for different classes of traffic. The higher price would be justified because the traffic requires superior quality of service, consumes more of a limited resource, has a greater adverse effect on other traffic, or is otherwise linked to cost (or opportunity cost).
- Network operators could block traffic that poses a threat to security, or that a reasonable network engineer might believe poses a threat to security.
- Network operators could charge the senders of information, recipients, or both.
- Network operators could offer proprietary content or unique services to their customers (without using their dominant control over the last-mile connection to favor their content or service).
- Network operators could block traffic originating from an attached device that one might reasonably believe is harmful to the network or its users, such as one that does not follow prescribed protocols and algorithms.
- Network operators could use *any* form of discrimination they wish, if the broadband market becomes truly competitive.

A policy designed to limit harmful uses of discrimination would not allow the following if and only if the broadband market is not highly competitive.

- A network operator could not charge more for stream A than for stream B if stream B requires at least as many scarce resources as stream A. For example, one cannot charge more for a steady 50 kb/s VOIP stream than for a steady 50 kb/s gaming application where the QOS requirements are the same. (Such discrimination has occurred when banning virtual private networks from lower-priced services, for example [28].)
- A network operator could not charge one user more than another for a comparable information transfer or monthly service unless the disparity can be justified by a difference in cost (or opportunity cost). This applies whether the user is the sender or receiver, and whether the user is a consumer, content provider, or service provider.
- A network operator could not block traffic based on content or application alone, unless one can reasonably believe that the traffic poses a security threat.
- A network operator could not degrade quality of service for traffic based on content alone.
- A network operator could not block traffic from a properly functioning device, while carrying traffic from devices known to be technically equivalent.

- A network operator could not offer lower quality of service or higher price for traffic that competes with a legacy circuit-switched service than it offers comparable traffic that does not compete with a legacy service.
- A network operator could not offer content or services directly or through an affiliate at a data rate or quality of service that is not available to competitors at a comparable price. It similarly could not make network-level services like multicast available to itself or affiliates and not to competitors.

Some believe we cannot develop rules about what is and is not allowed without basing them on the unfathomable intent of the network operator, but none of the rules above depend on intent.

Note that the above restrictions go beyond the traditional role of the Department of Justice's (DoJ) antitrust division. Today, DoJ would presumably act if a network operator used its market power to limit competition in an upstream market, but probably would not act if a network operator used its market power to extract monopoly rents in an upstream market while allowing competition. For example, a monopoly network operator may be prevented from adding excessive fees to all MP3 downloads that compete with its own service, but not from adding an excessive fee on all MP3 downloads (without a fee on other downloads of comparable size). Either of these policies could have the effect of forcing consumers to pay monopoly prices in the upstream market for music downloads, while the network operator pockets monopoly rents. Of course, DoJ policies can be changed if DoJ is selected as an enforcement agent for network neutrality, or that responsibility could instead be given to the FCC which has a broader "public interest" mandate.

Perhaps the greatest danger from an overly broad network neutrality proposal is that it could undermine security. Many staunch network neutrality advocates have agreed that discrimination for network security should not be prohibited, but further refinement is still needed. For example, one bill [29] would allow discrimination to improve security, provided that it is not based on application, service, or content. However, it is entirely possible that application, service, and content, allow the operator to conclude that a stream contains a dangerous virus or worm. Other proposals [30,31] would allow the operator to drop packets for security if and only if a user opts in to this service. However, it is much more effective to keep a dangerous worm out of the network entirely, rather than let it in and merely try to protect some of the users. Moreover, no matter how the security carve-out is defined, it should protect network operators when they block traffic that they reasonably believe is a security threat, even if they are wrong. There will be false positives and false negatives. If a network operator drops all packets that it believes with 95% certainty are dangerous, should that operator be subject to fines or lawsuits 5% of the time? On the other hand, there must be limits to this flexibility. For example, a network operator should not be allowed to block all encrypted traffic on the grounds that it could conceivably be a security threat.

In some cases, the balancing act is more difficult. For example, Section 4 shows how network operators with market power have incentive to intentionally degrade QOS for some traffic, even when there is excess capacity to provide excellent QOS. If one thinks of the network capacity as fixed, this practice is clearly bad for the user whose QOS is unnecessarily poor. On the other hand, if network operators were prohibited from this practice, they might

have incentive not to increase the capacity of the network, which could harm consumers in the long run.

There will also be more subtle tradeoffs. For example, if a network operator charges more for packet stream A than for stream B when the streams are identical in every way except that one is VOIP, then this is clearly a violation of network neutrality. However, if a network operator can present a reasonable technical explanation as to why it should charge more for the VOIP stream, but the VOIP service provider alleges that it is charging too much more, then the matter is more complicated. The question of how a network neutrality policy could resolve issues like this requires much closer scrutiny. It may even be impossible to resolve that kind of dispute without plunging into detailed price regulation. Nevertheless, even if a network neutrality policy can prohibit only the more obvious abuses of market power, that policy may still have significant benefit.

Network neutrality policies also differ in the extent to which regulatory decisions are made in advance or only after complaints about the alleged misdeed. The above list implies that some decisions should be made through an ex post complaint process. For example, if it is important to allow network operators to use discrimination against traffic that they reasonably believe is a security threat, but not against anything they claim is a security threat, then someone must decide what is reasonable. This probably occurs after a complaint about a network's security policy. Nevertheless, we should strive towards producing and continually updating a set of unambiguous a priori principles that describe what is and what is not allowed, so the complaint process yields few surprises. Companies need regulatory certainty before they can make significant investments. This applies to providers of cable modem and DSL services, potential broadband wireless or broadband-over-powerline competitors, content providers, service providers, and e-commerce merchants.

In fairness, we must note two potential counterarguments to the "balanced policy" suggested above. First, some may question the objective of not harming Internet users. Others might instead try to maximize social welfare, which would include the profits of network operators as well as the benefits to users. All else being equal, it is certainly good to increase these profits, but we assume that transfers from consumers to monopolists would not be considered to be in the public interest.

Even among Internet users, there are winners and losers that one could consider. For example, if video streaming over the Internet becomes popular, a policy that allows a network operator to charge much more for this application will harm companies that distribute video and consumers who enjoy their content, but it may allow network operators to provide less expensive service to consumers who want nothing but email access. One can even define scenarios where one group of consumers wins, one loses, and overall consumer surplus increases [15]. Further research is required to determine whether such scenarios are likely to occur often in practice. However, as a general trend, the more a network operator can discriminate on characteristics that are somehow correlated to a user's willingness to pay, the more that operator can increase profit at the expense of consumer surplus.

Others may object to this balanced policy because their goal is to encourage network operators to extend their broadband networks to more of the nation, which is also a worthy goal. Imagine that all consumers are placed in one of three categories: those in regions that will have broadband regardless of whether there is a network neutrality policy, those in regions that will not have broadband regardless of whether there is a network neutrality policy, and those in regions that will have broadband only if there is no network neutrality policy. Consumers in that first category could be better off with an effective and balanced network neutrality policy, if one can be crafted. Consumers in the second category are unaffected by network neutrality. Consumers in the third category are harmed by network neutrality. In effect, network operators will serve these latter customers only if the operators can extract oligopoly rents from upstream markets. This reduces the value of broadband Internet to users, but at least they have it. Thus, network neutrality could help consumers in the first category, and hurt those in the last, at least in the short run. Given that broadband is spreading, it may be more accurate to say that the consumers in the third category get broadband service earlier if there is no network neutrality protection, but once broadband arrives, it will always be less valuable as a result. This could be a high price to pay in the long run.

Section 7: Conclusion

Technology has emerged that will give network operators unprecedented ability to discriminate among network traffic based on sender, recipient, content, application, attached device, demographics, and many other characteristics. Network operators can use this information to selectively block traffic, degrade quality of service, and increase prices. This technology is not hypothetical or futuristic; it is here today, and equipment is being marketed explicitly for these purposes.

People following the network neutrality debate know that content and service providers like Google and Vonage may have to pay more if policy-makers do not limit discriminatory practices, but even network neutrality advocates are not discussing some important broader dangers. While it is obvious that an unregulated monopoly in last-mile broadband Internet access can bring monopoly prices to the broadband market, it is not obvious that an unregulated monopoly could have the ability and incentive to bring monopoly prices to every upstream market, including electronic commerce for any and all products, communications services like VOIP and videoconferencing, information distribution markets like video streaming and MP3 music downloads, on-line advertising, and network equipment, even when these markets are actually competitive. If perfect discrimination could be achieved, then the network operator could drive consumer surplus to zero in the broadband market and all upstream markets, meaning that all Internet users including consumers, content providers, and service providers would derive no value from the Internet. Network operators may even limit political discourse, at least as it pertains to their business. Luckily, perfect discrimination is not achievable, the equipment to support discrimination is not free, and duopoly competition in the larger markets will inhibit some of these practices, as should the fear of future actions from policy-makers. Nevertheless, there are real dangers that have been somewhat overlooked in the debate, including dangers that are not addressed under existing antitrust policy.

At the same time, we should not underestimate the dangers of imposing a network neutrality policy, especially one that is broad. Network neutrality policies could limit or even prohibit discrimination, and many forms of discrimination are beneficial to Internet users. Discrimination can be used to improve security, to increase quality of service, to allocate resources to those who need them the most, to prevent starvation, and to decrease total infrastructure costs. If a network neutrality policy were to prohibit such practices, as many current proposals do, then there would be collateral damage that deserves serious consideration. We must be sure that we do not adopt a cure that is worse than the disease.

We should try to devise a *balanced policy*, which does not limit the more useful forms of discrimination or constructive innovation, but that prevents a network operator with great market power from using the forms of discrimination that are especially harmful to users. Policy-makers should pay particular attention to any attempts to protect legacy services (telephony, video distribution) or to extract oligopoly rents from upstream markets.

Unfortunately, the network neutrality debate has repeatedly been framed in ways that obscure this central issue. Attempts to describe discrimination as inherently wrong are dangerously unproductive, both because discrimination can be beneficial, and because discrimination is not a problem in the absence of market power. Attempts to clarify the rights and freedoms of consumers and of network operators are useful when describing policy objectives, but these rights cannot serve as a useful basis for enforceable regulation, as it is often unclear who is at fault when someone's rights are violated, or what to do when rights come into conflict. The questions about who should pay for services, vertical integration, differentiation among network operators, and the end-to-end design principle are all noteworthy, but these secondary issues have distracted policy-makers from the more central concerns of a balanced policy.

Misframing the issue inevitably leads to problematic policy proposals. For example, because the critical role of market power has sometimes been absent in the debate, some network neutrality proposals might apply to any broadband service, which according to the FCC is any service of 200 kb/s or more. Thus, someday data services in a 3G cellular market could be subject to severe limits on discrimination even if that market proves to be highly competitive. Also, because some stakeholders stress their concerns about competition from network operators and their affiliates, some network neutrality proposals would only limit discrimination that favors network operators or their affiliates. Because network operators have ways of increasing their profits at the expense of users without these affiliations, such policies would not achieve their intended goals, and these policies may limit some beneficial practices. Finally, because network operators and content and service providers are so focused on whether the latter will have to pay more to the former for "access" to consumers, both sides often forget to debate whether those extra payments can be discriminatory, which is what makes them most dangerous.

This paper has indicated what an effective balanced policy might allow or prohibit in a few cases if such a policy can be defined, and the results differ greatly from most current policy proposals. However, many cases still have not yet been addressed in detail, here or elsewhere. It may ultimately be difficult to both prohibit harmful applications of discrimination and allow beneficial applications. This will disappoint both those who want to prohibit every theoretically possible form of harmful discrimination and those who want to protect any unlikely but

conceivable form of welfare-enhancing discrimination. There may still be plenty of room for reasonable compromise. We will not know what is possible until more detailed proposals are considered by the broader community.

Those Members of Congress who have placed network neutrality onto the legislative agenda have forced the community to address an important issue, and warned network operators that some forms of discrimination may lead to sanctions. This is a great service. The same can be said for the FCC Commissioners who supported the consumer freedoms [23,24]. However, much work remains before an effective and enforceable policy is defined. Success depends on moving the debate from vague principles to specific details about what practical forms of discrimination should and should not be allowed, and where one can prohibit the harmful without prohibiting the beneficial.

References

[1] Caspian, *Caspian Media Controller QOS Operation,* April 2006, www.caspiannetworks.com/PDF/QoS_Overview.pdf

[2] Cisco Systems, *Deploying Premium Services Using Cisco Service Control Technology*, 2005, www.cisco.com/application/pdf/en/us/guest/products/ps6150/c1031/cdccont_0900aecd8025258e.pdf

[3] Allot Communications, *NetEnforcer Overview*, www.allot.com/index.php?option=com_content&task=view&id=45&Itemid=44

[4] P-Cube, *Service Control White Paper: The Next Step in Networking for Cable Operators*, 2003, www.p-cube.com/doc_root/products/Engage/WP_SC_Cable_MSOs_110202.pdf

[5] Packeteer, *Gaining Visibility into Application and Network Behavior,* 2006, www.packeteer.com/resources/prod-sol/VisibilityDrillDown.pdf

[6] Cable Television Laboratories, Network Data Management - Usage for IP-Based Services, Service Specification - DOCSIS 1.1 Service Flow Metering, Sept. 2002, www.ipdr.org/service_specs/DOCSIS(TM)/DOCSIS(TM)1.1-3.1-A.0.pdf

[7] A. S. Uluagac, J. M. Peha, "IP Multicast Over Cable TV Networks," *Lecture Notes in Computer Science,* B. Stiller et al. (Eds.), LCNS 2816, Springer-Verlag, pp. 168-180, 2003.

[8] Rep Edward Markey, *Network Neutrality Act of 2006,* H.R. 5273, May 2, 2006.

[9] J. M. Peha, "Dynamic Pricing and Congestion Control for Best-Effort ATM Services," *Computer Networks,* Vol. 32, 2000, pp. 333-45, www.ece.cmu.edu/~peha/pricing.html

[10] Q. Wang, J. M. Peha, and M. A. Sirbu, "Optimal Pricing for Integrated-Services Networks," in *Internet Economics,* Joseph Bailey and Lee McKnight editors, MIT Press, 1997, pp. 353-76, www.ece.cmu.edu/~peha/pricing.html

[11] G. R. Bachula, Testimony Before the Senate Commerce Committee, Feb. 7, 2006, http://commerce.senate.gov/pdf/bachula-020706.pdf

[12] W. Lehr, J. M. Peha, M. A. Sirbu, S. Gillett, "Scenarios for the Network Neutrality Arms Race," *Proc. 34th Telecommunications Policy Research Conference (TPRC)*, Sept. 2006.

[13] C. M. Christensen, *The Innovator's Dilemma,* Harper Collins Publisher, New York, 2000.

[14] Sandvine, *Sandvine Network Demographic Management,* www.sandvine.com/general/getfile.asp?FILEID=15

[15] H. R. Varian, "Versioning Information Goods," 1997, www.sims.berkeley.edu/~hal/Papers/version.pdf
[16] Operax, *Efficient Network Resource Control - A Source of Competitive Advantage*, Sept. 2005, www.operax.com/docs/efficient_network_resource_control_claes_sept2005_final.pdf
[17] Cisco Systems, *Cisco Service Control: A Guide to Sustained Broadband Profitability,* www.democraticmedia.org/PDFs/CiscoBroadbandProfit.pdf
[18] B. Van Schewick, "Towards an Economic Framework for Network Neutrality Regulation," *Proc. Telecommunications Policy Research Conference*, Sept. 2005, http://web.si.umich.edu/tprc/papers/2005/483/van%20Schewick%20Network%20Neutrality%20TPRC%202005.pdf
[19] S. Renshaw, Testimony, Senate Commerce Committee Hearing on Media Ownership, July 8, 2003, http://commerce.senate.gov/hearings/testimony.cfm?id=831&wit_id=2340
[20] J. Windhausen, *Good Fences make Bad Broadband*, Attachment N, Public Knowledge White Paper, www.publicknowledge.org/pdf/pk-net-neutrality-attach-20060206.pdf
[21] J. Farrell, P. J. Weiser, "Modularity, Vertical Integration, and Open Access Policies: Towards a Convergence of Antitrust and Regulation in the Internet Age," *Harvard Journal of Law and Technology,* Vol. 17, No. 1, Fall 2003.
[22] C. S. Yoo, "Beyond Network Neutrality," *Harvard Journal of Law and Technology,* Vol. 19, No. 1, Fall 2005.
[23] M. J. Powell, *Preserving Internet Freedom: Guiding Principles for the Industry*, Feb. 8, 2004, http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-243556A1.pdf
[24] Federal Communications Commission, *New Principles Preserve and Promote the Open and Interconnected Nature of Public Internet*, August 5, 2005, http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-260435A1.pdf
[25] J. G. Sidak, Testimony, Senate Commerce Committee Hearing on Network Neutrality, Feb. 7, 2006, http://commerce.senate.gov/pdf/sidak-020706.pdf
[26] D. D. Clark, M. S. Blumenthal, "Rethinking the Design of the Internet: The End to End Arguments vs. The Brave New World," *Proc. Telecommunications Policy Research Conference*, August 2000, www.tprc.org/abstracts00/rethinking.pdf
[27] L. Lessig, Testimony, Senate Commerce Committee Hearing on Network Neutrality, Feb. 7, 2006, http://commerce.senate.gov/pdf/lessig-020706.pdf
[28] T. Wu, "Network Neutrality, Broadband Discrimination," *Journal of Telecommunications and High Technology Law*, Vol. 2, pp. 141-78, 2005
[29] Rep. Jim Sensenbrenner, *Internet Freedom and Non-Discrimination Act of 2006,* H.R. 5417, May 18, 2006.
[30] Sen. Ron Wyden, *Internet Non-Discrimination Act of 2006,* S. 2360, March 2, 2006.
[31] Sen. Olympia Snowe, *Internet Freedom Preservation Act,* S. 2917, May 19, 2006.