

Net Neutrality: Implications for the Future of the Internet

W. Scott Nainis, Ph.D.

Net neutrality arose several years ago as a political issue regarding operation of the Internet and the potential for some actors within the Internet, mostly the major network providers, to practice forms of Internet traffic discrimination that could be judged harmful to specific Internet users and to the Internet community overall. [1] Net neutrality refers to the general property of the Internet today insofar as it handles all data traffic in the same manner, i.e., with equal and non-discriminatory priority. The definition of net neutrality is controversial because there is no across-the-board agreement that the Internet operates fully in a neutral or non-discriminatory manner today, and whether or not it is in the best interest of the Internet community that it continue to operate in a fully neutral or non-discriminatory manner today and in the future. Discussions on net neutrality today focus on how neutral the Internet should be, and whether or not attempting to maintain or achieve the strictest form of net neutrality is in everyone's best interests. [2]

Net neutrality covers many important and emerging issues on how the Internet should be operated in the future. Although specific federal legislation protecting net neutrality has been considered for the past three years, there is some risk that premature legislation could overly constrain or wrongly direct Internet development. Perhaps the best approach for now is to continue the network monitoring and multi-community dialogues that are grappling with net neutrality issues as they occur. The Federal Communications Commission should continue and redouble its support and guidance of these efforts.

Introduction

In 2006 and 2007, legislative initiatives were proposed within the U.S. Congress in attempts to design and implement legislation that could control and curb the Internet in order to preserve net neutrality. [3] Though no form of net neutrality legislation passed at that time, a new bill—H.R. 5353, the Internet Freedom Preservation Act of 2008—was introduced in the spring of 2008 by Representative Edward Markey. [4] As this paper will discuss, perhaps there are some needs to protect fundamental aspects of how the Internet operates today so that the benefits it has already provided for society can continue. On the other hand, there are reasons to be concerned with attempts to legislate the operation of the Internet, and that premature legislation could cause more harm than good overall.

The root concept of net neutrality is that the Internet was designed to provide a basic service of transporting and directing data packets of information between *originating* and *destination* users, employing standard protocols that take all packets of information and forward them from one network node to the next network node according to recognized and agreed-upon design and operation principles that do not discriminate on the basis of:

- Sender identity
- Recipient identity
- Amount of data sent

- The nature of the application services by the data packets being sent [5]

Internet design is that these packets are processed and forwarded only on a first-come, first-served, non-discriminatory basis.

What makes the net neutrality issue complex, subtle, and politically sensitive is that it is actually a part of (or perhaps a code word for) a larger-scope issue regarding how the Internet and its related technologies policies, practices, and rules of operation will develop and change in the future. These developments and changes will greatly impact what all Internet users will experience with the Internet in the future and who will benefit and who will lose as part of these changes.

What is the scope of the issues surrounding net neutrality?

The history of the Internet is bound up with an academic view of how information should be exchanged and of its importance in society. [6] The fundamental concepts of Internet Protocol (IP) were designed to place the least structure and restriction on the movement of data, while at the same time giving all users the ability to do what they wanted to do. The concept of allowing packets of information to be transferred across a set of loosely linked networks evolved over time as the most general and open solution. The introduction and development of the higher layer capabilities of the Transmission Control Protocol

(TCP) allowed the demands of applications to be met with the much more general design of the lower-level IP.

The design of the Internet has fared quite well, despite the fact that over its lifetime there have been concerns that it was going to “run out of bandwidth” and be over-subscribed. For the most part, this has not occurred, mostly due to the fact that the Internet has been expanded greatly over time with more fiber optic connections and better and faster router capability. Also, management techniques have been adopted to help keep the Internet under general control. Exactly what these controls should be and how much bandwidth will be needed as traffic continues to grow leads to concerns which inevitably rekindle the net neutrality debate through a variety of questions such as:

- Who will and who must pay for this expansion of the network?
- Who really controls the Internet?
- Will the rights of individual users and fledgling entrepreneurs and other “less powerful” parties be superseded by powerful organizations and their representative groups?

Why has there been a continued call by organizations and individuals to “safeguard” the Internet by proposing and implementing “net neutrality” rules and policies that would impact how the Internet would be specified, designed, implemented, and operated in the future? The answer lies in the potential influence and impact of a variety of groups that are both affected by and have influence over the operation of the Internet. There are numerous groups that can be differentiated on the basis of who they are, what they do, and how they would be impacted by changes to the Internet.

Groups impacted by Internet net neutrality

Users, developers, network providers, and other businesses and organizations have different perspectives on what the Internet represents for them and the opportunities it provides them. What follows is a brief discussion of these various groups and how, in general, their view of the Internet is impacted by their motivations and expectations of the Internet. These groups are not necessarily described in the order of their influence or importance to the future of the Internet. It is possible for any group or community as described to have characteristics, goals, and behaviors deviating from their general class, and to have similarities to other groups in some ways.

Group 1: Academic and technical community

There is a variety of sub-groups and disciplines represented within the academic and technical community. The first sub-

group includes the original developers of the Internet and its major off-shoot application, the Web. These pioneers were part of an early vision that was and still is quite lofty and idealistic in its overall concept. The Internet was conceived, designed, and developed as a common resource for users to move information in a uniformly described, fair, and unimpeded way that gives essentially everyone equal footing and rights to do so. The concept of a connectionless IP layer with datagram packets free to move and be routed from source to destination is the main theme directing the design and operation of the Internet, and many within the early community believe that it should essentially stay this way. These fundamental concepts of the Internet are embodied in what is referred to as the “end-to-end principle,” whereby nearly all the processing and intelligent decision making for Internet transactions occur at the end points of the system. Many from the academic and technical community believe that new technology should be used solely to improve the hardware capability and bandwidth applied to making the original concepts keep working essentially as they have. [7]

Within the engineering community there are some technologists who suggest that although the Internet design and related technologies have worked in the past, the explosion of bandwidth requirements and the changing nature of the applications in use on the Internet make it useful to consider augmentation and greater flexibility in protocol and control technologies.

Academic economists have a range of views on the Internet that can vary towards and away from strict net neutrality, depending on their overall political vantage point. Many economists talk of telecommunications markets and whether or not they are truly competitive, or are monopolistic or duopolistic. In the case of pure competition, many economists indicate that net neutrality principles are not necessary since no one telecommunications provider can control the market and collect supplier “rents” from users due to non-neutral operation of at least portions of the Internet. These arguments are interesting, but complicated by difficulties in fully understanding how Internet telecommunications suppliers are operating in fully competitive or non-competitive markets. In fact, they may be operating in both simultaneously. In terms of the last mile of connectivity for nearly all Internet users, there is typically a monopoly or duopoly situation because there may only be one major telephone-based telecommunications provider and one cable television-based Internet Service Provider (ISP) available to a user or community.

Other academic groups concerned with net neutrality are within the legal academic community. They are involved with the issue of net neutrality in support of or against the interests of the major telecommunications providers, the major Internet application providers, and those who represent the major enter-

tainment and intellectual property providers, as discussed below. [8]

Group 2: Telecommunications providers

The major telecommunications companies have differing positions with respect to net neutrality, often depending on the detailed nature of their businesses, their planned business model strategies, and the specifics of their telecommunications infrastructure supporting the Internet. For example, a regulated telephone service provider has a different perspective than that of a major U.S. cable television-based Internet provider. The cable television industry developed as a broadcast service, providing television to communities that could not easily receive over-the-air television broadcasts. Over the last 15 years, the U.S. cable television industry has expanded its capabilities to provide digital television with a large degree of additional video programming beyond that developed by the major over-the-air broadcast organizations (NBC, ABC, Fox, CBS, etc.). The bulk of the cable television business and associated revenues have come from shipping video information to its subscribers. Internet connectivity and voice telephone service have come as a more recent addition to the basic mission of the cable providers. Thus, the telecommunications infrastructure of the cable providers has been overwhelmingly designed to facilitate broadcast and download of content to users, and is not designed to support upload of content from users. Under the Data-Over-Cable Service Interface Specification (DOCSIS) 1.1 standard, which is still the predominant operating mode for U.S. cable providers today, upstream bandwidth capabilities are very limited and very vulnerable to increases in user upstream data traffic. [9] These characteristics have led some cable telecommunications providers, such as Comcast, to treat Internet traffic in ways that have appeared to be decidedly “non-neutral.” [10]

On the other hand, major local exchange telecommunications carriers have been spending a great amount of money and effort to increase bandwidth to their customers and have, in general, greater symmetry between upload and download capacity with their customers—though by no means total symmetry. Thus, the motivations and activities of telephone service providers will differ significantly from those of Comcast, Inc. This circumstance has been recently observed to impact telecommunications provider behavior with respect to net neutrality.

In the longer term, many analysts have concluded that the interests of the major telecommunications providers are not aligned with net neutrality in the sense that these providers could economically benefit from providing value-added services and integrating the additional content and applications derived from future triple play and quad play services, with network discrimination a tempting approach to adopt. [11]

Group 3: Internet applications providers

High-profile participants in the Internet include organizations that provide some of the most used applications. *Google* comes to mind with its extremely well-used search engines and mapping services, as well as its *YouTube.com* video playback site. Other major applications include *Apple's iTunes Website*, *Amazon.com*, *Microsoft.com*, and *ebay.com*, which are all major Internet retailers. *Yahoo.com* and the more focused social Websites—*facebook.com* and *myspace.com*—are also some of the larger Website applications. [12] These organizations through their Websites have delivered well-accepted capabilities to service users, provide information, support significant levels of user interaction, and provide products and services, both indirectly and directly. These wide-ranging services have changed the behavior and expectations of users in the U.S. and worldwide. The major Internet application providers have an interest in preservation of Internet net neutrality, and they want the Internet to allow them continued and complete non-discriminated access to their full customer base.

Application providers are businesses and as such have concerns about security and safety for both financial transactions and for user privacy. Net neutrality may be less important to this group if it conflicts with the support of safety and security of transactions.

Group 4: Intellectual property and entertainment providers

There are owners and distributors of intellectual property who use the Internet as their major or sole channel of distribution. However, many were established long before the Internet came to prominence and universal use, and thus have only participated marginally on the Internet compared to other organizations. The major music distribution organizations and the motion picture industry represent the major providers in this sector. Their concerns with respect to net neutrality are focused on protection of their intellectual property rights in a climate which is rapidly changing in terms of its expected distribution modes, and in attitudes, laws, and legal practice regarding how intellectual property is obtained, distributed, and controlled. Some of the major players in the intellectual property provider sector, represented by the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA), are interested in the implications of net neutrality in terms of how it may impact their ability to protect their intellectual property from illegal copying and distribution over the Internet without, in their opinion, adequate control and checks. Recently, both the RIAA and the MPAA have come forward to express their solid opposition to essentially any form of net neutrality legislation. [13]

Other impacted groups

There are many other constituency groups that will be impacted by net neutrality on the Internet. Obviously, the end user public will be greatly impacted through the range of information and applications that the Internet will or will not provide them as a result of net neutrality policy or legislation in the future. The cost of this information and service will also be impacted by whether or not the full range of both innovation and competition can be maintained on the Internet in the future. That is why there are numerous groups focused on support for maintaining net neutrality.

Another group impacted by net neutrality is telecommunications workers, represented by unions promoting their general interests and allowing a degree of focus of their interests within the telecommunications expansion and development sector.

The installation of greater capacity in terms of fiber cable and switching electronics is a goal of the communications workers, since it strengthens the value of their efforts and provides a more robust sector to support the telecommunications workers and their union. Telecommunications workers generally look negatively at proposals that tend to limit or focus the use of the Internet, thus reducing the degree of investment to be made in Internet infrastructure. The telecommunications workers support greater bandwidth capabilities for all Internet users through a stronger and more robust Internet backbone network.

The emerging, but fledgling, Internet entrepreneurs represent an array of individuals and small organizations that are adopting and inventing new applications to take advantage of the Internet and to provide new and inventive applications for users across the Internet. Some of the Internet entrepreneurs of today may become the major Internet applications providers of tomorrow. These emerging entrepreneurs generally count on the open and neutral characteristics of the Internet in order to design and implement their new services. Thus, with few exceptions, these participants within the Internet are supporters of net neutrality for the Internet.

The government sector is involved with the evolution of net neutrality. Key organizations within the federal government are currently charged with the maintenance of net neutrality on the Internet; namely, the Federal Communications Commission (FCC), which, under its general mandate under the Telecommunications Act as amended in 1996, is responsible for the maintenance of net neutrality to the extent that it is consistent with non-discriminatory behavior in telecommunications. All other agencies of the government, including federal, state, and local, are impacted by net neutrality to the extent that their employees are users of the Internet and the applications and services provided over the Internet. In fact, it has been shown that the Internet has significantly impacted the manner, effectiveness, and efficiency with which all levels of government have

operated. [14] Within the government, law enforcement has continuing and expanding requirements for the capability to learn what is being done by individuals and groups on the Internet when it involves the potential for crime and impact on national security. While some sectors of the government actively support measures to ensure net neutrality, policies of other sectors actively support user transparency and data retrieval capabilities that could be at odds with certain aspects of net neutrality—particularly the end-to-end principle. [15]

Discrimination and segmentation

There are two basic concepts that are very useful in making sense of this debate on net neutrality—discrimination and segmentation. Discrimination refers to the ability to differentiate, on one or multiple bases, the availability, price, speed, or other operational characteristics of an Internet-based service. Discrimination would be practiced by some types of Internet providers. Within this context, discrimination in Internet services can be good or bad or neither depending on who is viewing it and under what particular circumstance. Segmentation is an action by Internet providers to design, organize, and operate the Internet with differing capabilities and approaches in order to support chosen types of discrimination. Segmentation, like discrimination, can be either good or bad, depending on individual parties' points of view. Segmentation can be a good thing if it can support a generally beneficial discrimination of users and services on the Internet, while at the same time not introducing excessive complexity and cost to the operation of the Internet overall. It is interesting to note in recent remarks made by Robert Kahn, one of the pioneering founders of the Internet architecture, that strict net neutrality was not as much of a concern as was excessive “network segmentation” not balanced by improvement in overall operations. [16]

There could be many forms of discrimination that are applied to the Internet, and resulting segmentation approaches could be developed to support those selected discriminations. Discrimination can be considered good when it provides an overall benefit to the majority of users, while it discriminates against a minority of users whose actions on the Internet are considered excessive, unfair, or negative in some way. For example, ISP and network providers should all work hard to discriminate against users who desire to infect the Internet with viruses and worms, or launch denial of service (DoS) attacks.

The forms of discrimination that could occur on the Internet include the following.

Price discrimination. Price discrimination is charging a different price for an Internet service or service on the basis of who the user is or what the application is. It is usually applied to situations where the cost of service is not different across

groups. Historically, residential telecommunications customers have been asked to pay less than commercial customers even when the costs of service are essentially the same. When allowed, it is considered a good and profitable business practice.

Service speed or priority discrimination. Varies the speed of Internet service depending on the discriminating characteristics, which could include customer type, application type, or whether the customer has made specific arrangements with the network provider. Many forms of discrimination of this type have been judged to be forms of violation of net neutrality. However, decisions of users to purchase higher or lower amounts of bandwidth are considered net neutral, if the option is available uniformly to all users. If discrimination only occurs when network congestion is present, the discrimination is referred to as minimal discrimination. If this type of discrimination can occur when networks are not congested, it is referred to as non-minimal discrimination.

Application or feature discrimination. Differentiates the availability of Internet applications or features depending on the nature of the users involved. This form of discrimination is considered net neutral if applied and available uniformly for all users across the board. If applied in a selective mandatory fashion, this form of discrimination would be considered to be not network neutral. One recent example of this type of discrimination was the control of peer-to-peer data file transfer applications like BitTorrent and Azureus by Comcast.

Discrimination amongst users on the basis of the sheer volume of their Internet use is generally accepted as reasonable practice for ISPs, but not accepted by all users. User volumes vary widely and nearly all ISP contract agreements have some form of acceptable use policy which places limits on the amount of data transfer or the types of applications that a user can have through their connection. Commercial users of the Internet who experience much higher data rates and overall data transfer purchase higher bandwidth channels that cost them considerably more per month than smaller commercial and residential users. In Europe there is a greater tendency for ISPs to charge users directly for the amount of data they transfer. Recently, a major U.S. ISP suggested that Internet users be charged a rate of \$1.00 per gigabyte of data they transfer over a specified monthly limit. [17] (To put this price into perspective, consider that a gigabyte of data would allow a user to conduct a high definition television (HDTV) two-way video conference for about 8 minutes with standard compression and transmission technologies.)

When network discrimination and segmentation can be beneficial

Network traffic discrimination and associated network segmentation can provide potential for benefit and improvement. Take, for example, the issue of time/jitter sensitive versus time-insensitive traffic. Figure 1 shows a high-level schematic of the current Internet situation connecting a user/client with a distance user/Website. Here we have the same user/client taking advantage of two Internet services—a time-insensitive application denoted by the solid line, and a time/jitter sensitive application denoted by the dotted line. Under the “net neutral” procedures today, the related traffic reaches the user/client’s ISP. The ISP connects and transports the data to the Internet backbone networks, and the packets traverse various switches until they reach the destination ISP and are forwarded to the user/client or user/Website on the other end. In Figure 1, both types of traffic follow the same path (ISP1 ⇒ S1 ⇒ S2 ⇒ S3 ⇒ S5 ⇒ ISP2).

In Figure 2, the situation is modified in the sense that the two types of traffic are discriminated at the ISP through a segmented approach. The time-sensitive traffic traverses a different path through the backbone networks and with a different algorithm for its control and routing. The segmentation must be carried out throughout the entire Internet and also segmented at the receiving ISPs as shown. Every component within the end-to-end network may have to maintain and handle this new segmentation. Notice that in Figure 2 the time-sensitive traffic traverses a route with fewer “hops.” The intended effect would be to have given the time-sensitive traffic a shorter path with less delay at each router node along the path.

Suggested reasons to deviate from pure net neutrality

Reasons that motivate suggestions to deviate from a purely neutral Internet include the following.

- Providing better quality of service (QoS) for time-critical applications is necessary because a strictly neutral Internet is too costly and inefficient to maintain, or time-critical applications will be negatively impacted at least some of the time.
- There is a strong disparity between those who pay for the Internet and those who use disproportionate resources; when this occurs, it can definitely be unfair.

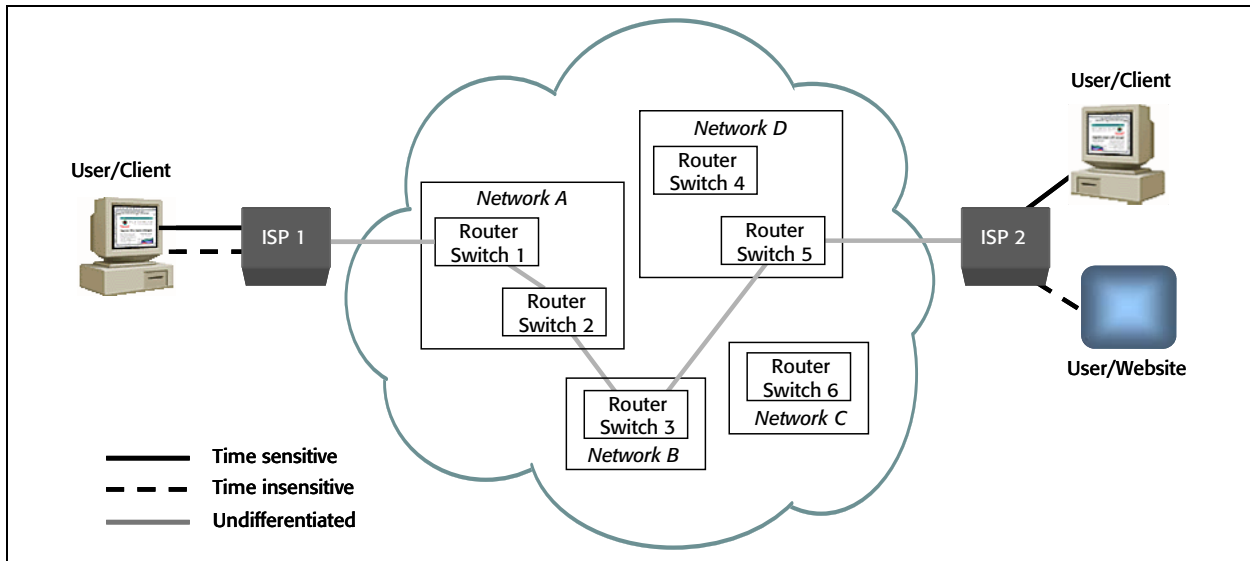


Figure 1. End-to-end topology without discrimination and segmentation

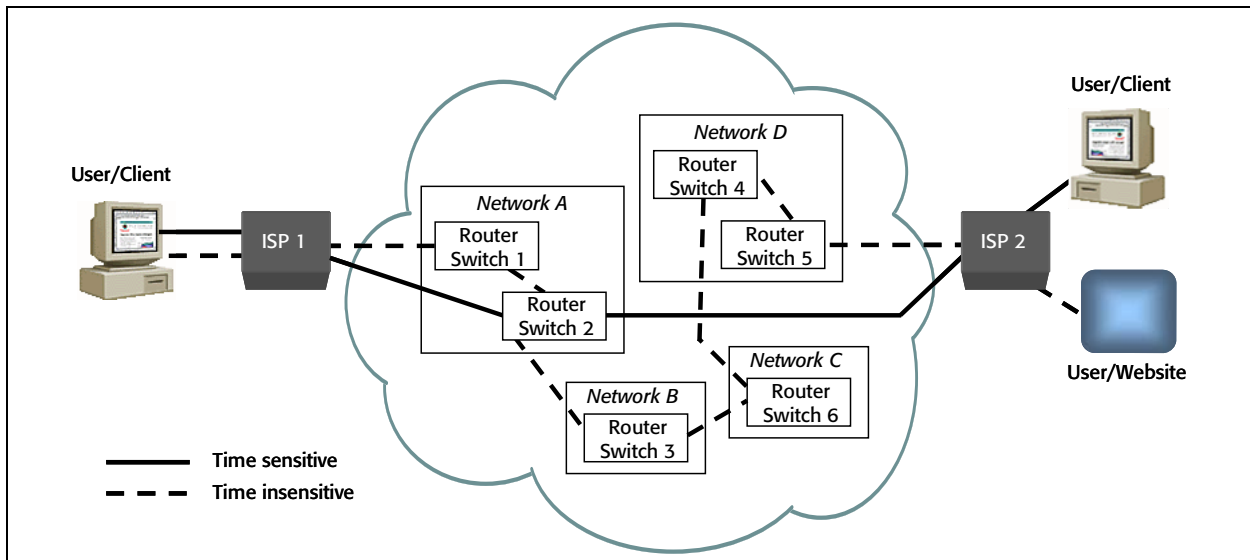


Figure 2. End-to-end topology with discrimination and segmentation

- A strictly neutral Internet makes those who manage and operate the core infrastructure of the Internet pay disproportionately for its operation, while not being able to fully take advantage of the Internet functional opportunities to make revenue and profit from customers who use the Internet.
- A fully neutral Internet obscures the nature of the applications and information flowing across the Internet, thereby allowing individuals and organizations to transmit, copy, and share intellectual property illegally without detection and retribution.

Each of these issues deserves some discussion and explanation.

Issue 1: Concerns for QoS for time-critical applications

Some believe the current design of the Internet is ultimately too inefficient for the types of traffic that are developing over the Web. When everyone was limited to file transfers and email, or short non-data intensive Web cruising, the concept of processing and routing incoming packets in order of arrival made sense. Now that applications are becoming very data-intensive and time-critical, the mode of operation of the Internet has to be modified. Meeting QoS goals for certain real-time traffic has a much bigger impact on the resources required to successfully operate the Internet. Thus, the cost of a byte of traffic sent

with a real-time requirement “costs” more than a byte without such stringent QoS requirements. Prioritization approaches that can remember the routing destination for groups of packets, often referred to as a flow, can allow for lower overhead for packet processing. If time-critical packets were given priority over other packets and routers were capable of distinguishing packets by type, it could be possible to provide expedited service for those packets, and reduce their computation impact on the Internet overall.

IPv6 incorporates specific head entry for traffic classes. Eventually when all switches and protocols are migrated to IPv6, it should be possible to institute packet-based priority protocols and individual data packets. Priority queueing and response could be instituted for high priority packets. The initial ISP connection would be given the task of keeping track of customer data flows by datagram class and priority. Billing for end-use customers for both outgoing and incoming high priority class packets could be performed. Packet traffic by priority level could be measured by all backbone network providers, and connected ISPs would be “taxed” by the backbone network providers on the basis of packets sent and received differentiated by priority class. This is just an extension of how the costs of handling traffic are handled today between the ISP and the backbone providers.

Opponents of the type of packet prioritization described above point out that such differentiated schemes and prioritization could lead attempts to discriminate against classes of users in a variety of different ways. For example, an ISP could attempt to differentiate packets to and from particular vendors and their applications if that ISP or telecommunications provider is financially associated with a competing service. In IPv6, there is a location on the packet header that would indicate the type of packet being sent, but it is unlikely that such information would be able to determine which user, vendor, or application with which that packet is associated. Determination of such detailed information would require a deeper inspection of the packet and its contents. This will be discussed further below.

Issue 2: Disparity between those who pay and those who use

Another area of controversy is the degree of cost involved in handling the greater volumes of traffic generated by more and more users, and the proliferation of highly bandwidth-intensive applications such as peer-to-peer (P2P) file transfers and video downloading. Some proponents of net neutrality say that the cost factor for the major telecommunications providers is overstated since they have an excessive amount of fiber in place. In fact, one estimate states that only 7 percent of existing Internet capacity in terms of fiber capacity in place is currently being

used. [18] Such statements are difficult to interpret because capacity measures must be carefully defined and qualified. One potential issue is that some end users are generating a disproportionate share of the bandwidth demand while they are not paying a proportionate share of the cost of the infrastructure needed to handle the demand with enough QoS for the applications used.

Whenever a resource is not directly metered, there is a tendency for individuals to use widely varying amounts of a common resource depending on their individual needs and situation. We all pay taxes to support roads and highways—some of us drive on them more miles per year than others; thus, taxes spent on roads may not be contributed to in proportion to individual usage, except indirectly through gasoline consumption and highway-related taxes paid. A viable solution may be to develop a fair and consistent measure for the amount of bandwidth used by each customer and then charge each user on the basis of the amount of bandwidth they used. One difficulty of this approach is matching the bandwidth used to the real impact on the utilization of Internet resources. A kilobyte of data transferred for a user may have a smaller or larger cost depending on the degree of utilization of the network during that use and the QoS requirements for that service.

Many ISPs have implicit fair use policies that indicate the limits to the amount of data that can be transferred during a period of time, usually each month. An ISP can monitor and track individual Internet accounts and determine whether or not a user is sending an “excessive” amount of data across its network into the Internet. Many agree that ISPs do have the right to limit the total traffic generated by users and/or to charge them in some proportion to their usage. To do so is not necessarily the same thing as being non-net neutral, depending on how such policies are implemented.

Issue 3: Core operation profitability

Some have suggested that the issues of net neutrality represent a battle between those who control edge and interfaces of the Internet versus those who support its core central networks. The organizations that provide the last mile to customers—be they commercial business, residential, or major application providers—are the ones who profit most from the Internet. If a major network provider participates in the Internet only by supplying bandwidth and switching services for IP datagrams, then their revenue and profit is limited to arrangements they make with the other network participants for payments associated with the volume of traffic they handle and route for the other network vendors.

Since the major backbone network providers do not have a direct relationship with the end users, the only way for them to be compensated for their backbone network transportation is

through those funding arrangements. Just as electric utilities generate and transport electrical energy across their transmission networks, the Internet backbone providers do the same, and like the electric utilities, their costs plus adequate profit need to be provided for. Unlike the electric utilities, the degree of regulation and accounting control amongst the Internet backbone and other network providers is not as carefully monitored and regulated by local and national government agencies. To date, the major network providers have worked things out. There are strong pressures from the major providers to ensure that network providers get adequately compensated from their investments and for their operational costs. This should be the case, but it should not be an argument for network providers to move the Internet to a non-neutral operation and be able to generate additional income through non-neutral Internet operations and pricing policies.

If the major network providers want to increase their revenues within the Internet and broadband realm, they must focus their efforts in applications areas not tied directly to their responsibilities for Internet network transport, and also expand their non-Internet broadband services such as television broadcasting including IPTV. Many believe there is a potential for conflict of interest between network providers' desire to provide network transport, and their desire to provide more end user applications and be an incentive for non-neutral network operations and policies.

Issue 4: Transparency for transfer of illegal and copyright-protected materials

A neutral Internet is one that sends packets on a neutral basis for all users without differentiating the level of service depending on the user. In order to operate an Internet-based network in a non-neutral manner, it is necessary to monitor and recognize what the packets of information represent in terms of the type of application being serviced and information related to the identity of the sender and receiver. Such information would be germane to the non-neutral treatment that the data transported. The information that would be collected in a non-neutral Internet serves to support those whose goal is to stem the tide of increasing movement and copying of intellectual property over the Internet. P2P network applications have been used to transport intellectual property illegally; thus detection of such traffic and identification of the sender and receiver are important tools in policing of such practices. Those industries impacted by such P2P traffic have goals and interests that may align with movement towards a non-neutral Internet.

The technology to help determine which applications are potentially involved with illegal file transfers is consistent with capabilities for real-time monitoring and analysis of Internet traffic. Deep packet inspection (DPI) has been developing as a

technology and is now at the point in which it can be effectively used to sample and analyze traffic for ISPs who wish to manage their traffic flows more closely and meet requirements for traffic monitoring and reporting under the federal government's Communications Assistance for Law Enforcement Act (CALEA) program. [19] The increased capability of such equipment, along with the strong financial incentives to utilize this information for legal, security, and commercial reasons, has the potential to threaten network neutrality.

A future scenario and net neutrality: AOL déjà vu

Although concerns of net neutrality proponents could be considered overly alarmist and not realistic for network provider behavior in general, the incentives for the network providers and at times their expressed intentions should be of some concern. This section discusses one path whereby a major network provider might develop its "Internet" network services in a decidedly non-neutral direction.

Major telecommunications providers in the U.S. are working to connect households and businesses to high-speed Internet ranging in speed from 5 Mbps to over 100 Mbps. [20] The ability for telecommunications providers to offer a full array of "quad play" services, including voice telephone, television channels, video programming, and wireless telephone and data, as well as high-speed Internet access, provides the potential for an ever-expanding array of services at the consumer and commercial level. It is not hard to imagine the internal motivation of the major telecommunications providers to take fullest advantage of their position to help make the potential services happen in a way that would be most attractive to their customers and at the same time give the telecommunications providers a very strong and growing base of revenue on which to continue to build their networks and to make further penetration into their geographically-focused customer base.

Because the major telecommunications providers are strong in network development, management, and expansion, they are in a position to be able to move services and information close to their customers. The information that customers want highly overlaps what the Internet offers today and will offer in the future. The telecommunications providers can imagine offering those services and products directly to their customers over the networks they more closely manage. By working closely with "business partners," the major telecommunications providers can offer within-network services and information that can have some advantages over those offered over the Internet. This potential is reminiscent of the "walled garden" world created by AOL for its customers in the early 1990s. AOL operated chat rooms and provided resources to its users directly. Product offerings were available and AOL presented a

special world of interaction opportunities totally within their own networks and direct control. Access to the Web was relegated to a button in the corner. AOL was conceived in a prior world of dial-up connection speeds and was not able to keep its customers satisfied with the limited offering it had.

To succeed in such a strategy, a large telecommunications provider would have to offer an experience to the user that was superior to what the Internet offers today or in the future. This could be accomplished by interjecting controls and gate-keeping interventions on the Internet to “slow it down” and make it look relatively less attractive. On the other hand, the local telecommunications provider needs to develop the differentiation more subtly by investing heavily in its own “private” network, developing software modules and “plug-ins” to expand the capabilities of its own network offerings, and then letting the Internet suffer in comparison to its own offerings along with its partners. Fears of Internet security and privacy could also be used to help coax the users towards the telecommunications provider’s services and products and away from the Internet. All of the network provider’s walled-garden services could be “guaranteed” to be safe and secure. Again, using triple and quad play convergence could be a strong tool for doing that for those customers ready to take full advantage of that convergence.

Given the broadband world offered by major telecommunications providers today, it is not clear whether such attempts by the telecommunications providers would follow the route of AOL or could be part of a path that broadband access will go in the future—a path in which the essential characteristics of the Internet for achieving its growth, innovations, and ultimate success are threatened by a non-neutral and closed cyberspace world where flexibility as well as risk are locked down and controlled. This is one aspect of the net neutrality debates that continues today. [21]

Preserving net neutrality on the Internet

An article written by David Weitzner in 2006 provides a good overall description of four fundamental properties of the Internet that embody the neutrality of operation that are the cornerstones of the Internet’s ability to provide great value to users and significant opportunity for the growth of new concepts and operations that made the Internet the most important phenomenon of the last 15 years. [22]

Non-discriminatory routing of packets

This fundamental property expresses the concept that traffic should be treated equally based on its class or type, but not treated differently due to the identity of the sender or receiver, or the specific application being used within that class of traffic

type. Traffic types or classes could be differentiated by basic characteristics related to the need for low, real-time latency or lower levels of jitter, as characterized by Voice over IP (VoIP) telephone service or real-time gaming.

User control and choice over service levels

This concept follows from the discussion of the first, above. If there are differentiated classes of service, then every sender and receiver should be able to avail themselves of these classes or types of service. If there are differentials in the price of such service, then all users should be able to avail themselves of these different services at similar prices.

Ability to introduce new services and protocols without prior network operator approval

New developers and those with new ideas for innovative applications have not had to obtain pre-approval to introduce new Internet technologies and related applications. The expectation is that as long as the protocols and agreements generally made by Internet users and developers were maintained, new applications using new services and protocols were welcome. In a world where it is not possible to determine the full extent of the impact of sub-technologies and new procedures on the operation of the Internet, there is an implicit understanding that if a new application or protocol caused damage to other users that the community of users would work together to make the modifications and compromises necessary to establish stability in Internet operations.

Non-discriminatory peering of backbone Internet networks

The Internet backbone is comprised of a number of networks which all agree to work together under a set of principles developed by the Internet Engineering Task Force (IETF) and the general guidance of the Internet Society (ISOC) and the Internet Architectural Board (IAB). The agreements governing how the backbone networks work together and interact are partially directed by IETF and IAB Request for Comments (RFC) documents; however, many of the agreements are specific to the backbone members and those network providers that connect to them including the ISPs. In order for the Internet to ultimately remain neutral and not to discriminate unfairly among the range of users, the peering arrangements among all networks must be done in a reasonably level playing field. All organizations are not prepared to be backbone network providers, but those that can act at that level of performance and scale should be allowed to participate.

Weitzner clarifies that these four proposed principles are intended for the Internet and not necessarily telecommunications providers’ networks overall. This in itself can be an issue.

Historically, TV, radio, and voice telephone were all non-Internet/non-TCP/IP-based capabilities; today all of these telecommunications channels have embraced TCP/IP technology. The distinction between the Internet and a broadband network may not be as distinct given that customers are becoming truly indifferent to the source of the service and only remain focused on the specific nature and level of that service. The point is that net neutrality issues are appearing increasingly across all communications modalities and will not be limited by vendor modality.

Deep packet inspection and privacy for users

DPI has developed as a means to deal with a number of issues related to the operation of the Internet. When a packet arrives at a router, the first information captured from that packet is located within the header of that packet. The packet header includes information about the source and destination of the packet along with other identifying information. In order to route a packet only header information is required. Figure 3 shows the information associated with an IPv6 version header. DPI is the effort to capture *additional* information contained within a packet at the point in time when that packet traverses a router within the network. [23] Routers are designed to read the header information and to determine how they will route the packet. Equipment that can perform DPI is able to scan and analyze information located within the data fields of the packet. By looking “deeper” into the packet, it is possible to learn more about the nature of the data being sent.

Figure 4 shows the situation with “shallow” packet inspection used to determine the routing of packets across the Internet. Packet header information is examined and this information is used to determine the destination for that packet and where the packet should be sent next. Within the data region of the packet, there is much more that can be learned. What type of application is being supported with the packet payload? What is the intended port for the payload application? Some DPI capability can perform statistical analysis of the data within the packet in order to determine specific software applications associated with the packet and to determine more information about the information being sent within the packet.

Figure 5 depicts how DPI inspects much farther or “deeper” into the packet structure and looks inside its data or payload area. By correlating what is found within the data area

of the packet and using knowledge of the nature and structure of common client and server applications, it is possible to learn a great deal about the nature of the traffic that passes through a DPI point. DPI can occur at any location within the Internet or even with an organization’s local area network (LAN), but most DPI activities are being performed by ISPs.

DPI technology has increased in sophistication. Not only does it look into the payload area of each packet inspected, but it can keep track of what has been learned from packets over time, and use information from a sequence of packets to infer information about the nature of the information within the packet. In the case of CALEA-based law information, data messages from specific individuals can be sought out and retrieved.

In the context of ISPs and their network management activities, the type of “stateful” inspection and analysis processing of DPI technology can be used to determine what applications are being used. Such information can be used by network operators to implement strategies of network management and control such as performed by Comcast.

DPI can be used to learn about the proclivities and habits of ISP users in order to direct-market these users. Recently, Ed Markey expressed the idea that Internet customers should be able to “opt-in” to allowing ISP advertising intrusions based on individual user Internet activities as monitored through DPI. Clearly, an ISP obtaining such knowledge about its users can be considered an invasion of privacy and should be disclosed. [24] Not surprisingly, users are starting to push back against ISP incursions into privacy. The concept of “trip wires” was developed by a group of students and faculty at the University of Washington. [25] In their research, they have set up Websites deliberately designed to be sought out by search engines and users in order to spread user monitoring code called trip wires onto client machines. Through this mechanism, they have been able to obtain information regarding the percentage of time that packet transmission between the client and servers are modified or augmented as they pass through ISPs and other networks. About 40 percent of the time there is a change or augmentation to the series of packets transferred. Some of these are due to client-side software-based changes such as internal security software, but nearly half of the modifications are changes or augmentations added by the ISP and intermediary networks.

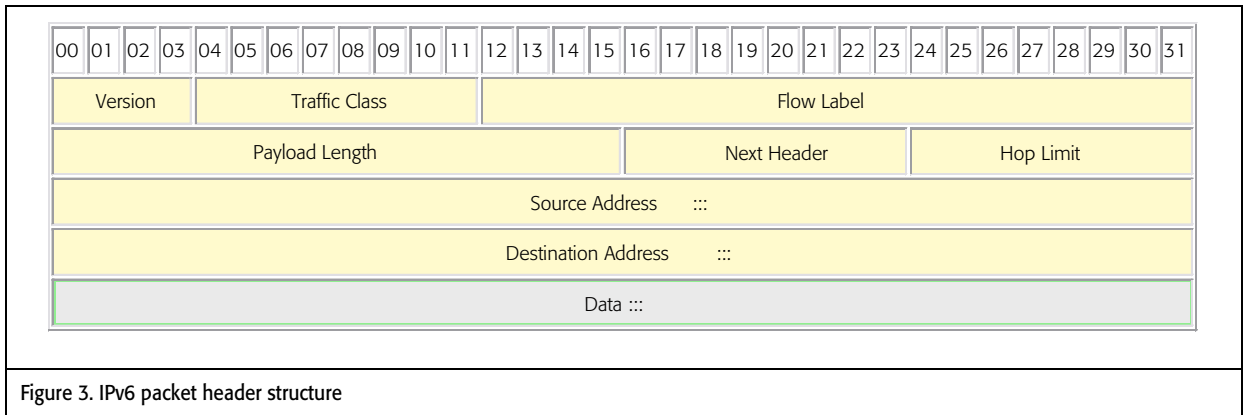


Figure 3. IPv6 packet header structure

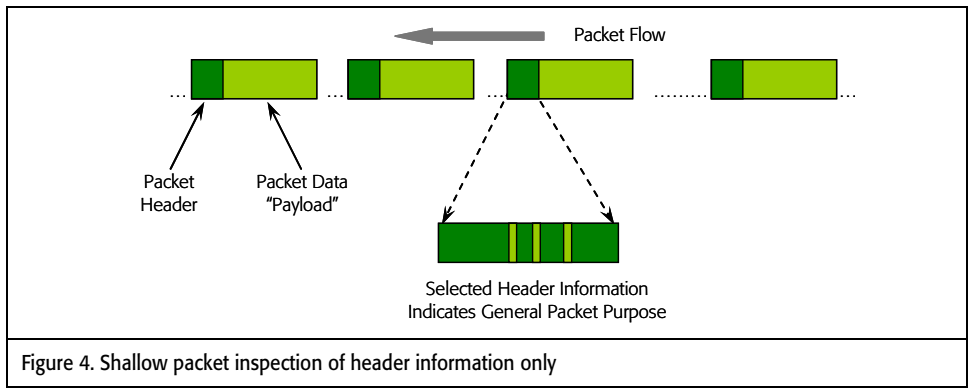


Figure 4. Shallow packet inspection of header information only

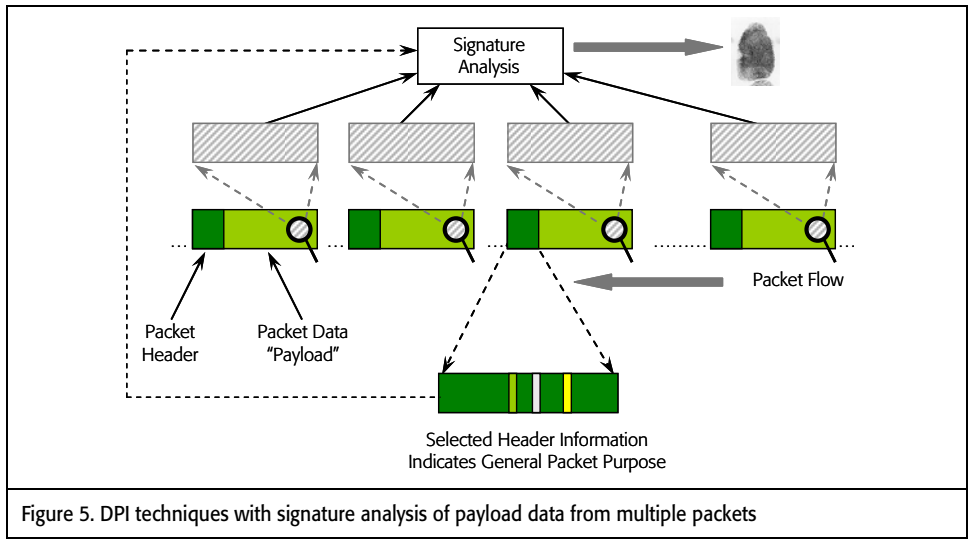


Figure 5. DPI techniques with signature analysis of payload data from multiple packets

In numerous occasions, adware and additional information is added to provide additional messages and advertisements on client Webscreens. Many would believe that such additional information added to the normal payload packets constitutes a form of non-neutral network response, if not an invasion of privacy.

DPI can easily move into the regime of privacy violation if not carefully controlled. At this time there are specific legal

prohibitions about obtaining and divulging private information taken from unencrypted packet payloads, but few if any details are legally described about the rights and privileges of both the senders and receivers versus the transporters of the packets.

[26] One area where there is some definition of the rights and protections for packet inspection is under the CALEA legislation which has been recently extended to explicitly allow the telecommunications providers to gather sender/receiver data

from interactions over the Internet for the purposes of investigating crimes, particularly those associated with threats to national security. [27]

The main point of DPI is that the technology is present and improving to allow network operators at any point within the Internet to detect what is being sent, by whom, to whom, and for what purposes and applications, including detailed information from unencrypted payloads. Such capability can provide the means and the motivation for those telecommunications providers who would like to benefit their operations due to the control of the flow of Internet data and to in some way differentiate, control, tax, or modify the movement of those packets according to what might be considered a “non-neutral” policy. The impact of DPI can be generally avoided through the use of encryption, and this is done automatically for sensitive traffic such as bank or credit card transactions. At present, few users bother to encrypt other packets.

Network complexity—network management

One issue that concerns network operators is protection from traffic overloads and security threats. Sometimes discrimination of traffic is necessary to prevent overloads from causing harm to users. Network managers are concerned that viruses and other potentially harmful payloads must be detected and handled before they can cause damage either to the network or to end users. The question is whether these activities performed by network operators are discriminatory or provide capability for network operators to misuse techniques such as those for non-neutral treatment of users.

A key point that is often missed in the debate about net neutrality is that the Internet is really not a monolithic and centrally-managed system or entity. The greatest utility to be derived collectively from the Internet occurs when all the participants using the Internet abide by a set of common agreements and modes of conduct in their use of the Internet.

In order to manage their networks for secure and smooth operation, network providers must perform network management and implement priority setting. Priority setting allows some types of data packets to be processed and routed before other packets, and may not be considered a violation of net neutrality; in fact, many have argued that priority setting in data packet processing is a good and even necessary occurrence. [28] Delays are a by-product of data packet priority setting, but delays can also be used to hold data packets at points within the network waiting for a period of less network traffic congestion. Priority setting and delay are two ways to look at the same phenomenon—data waits if it is not given the priority to go first. The generation of resets, as was recently reported to be performed by Comcast for P2P data traffic found on its net-

work, is another form of discrimination. Unlike setting low priority for packets and delaying or dropping them, modification of a data packet to include a “synthetic” reset indication is used to slow down traffic flow at the source and to actively work to reduce the traffic load.

To the extent that telecommunications software and Internet-based applications build “fair use” into their software, the entire user community benefits. However, some users can still act to impose much higher demands on network providers. A good case in point has been the issue of P2P software such as BitTorrent and Azureus that support multi-P2P file sharing. When faced with network congestion, many of these software applications continued to press for high data transmission rates rather than backing off in their transmission requirements as part of a network-sharing protocol response. This behavior of some of these applications caused further congestion, mostly in the edge connectively networks along such ISPs as Comcast who typically use DOCSIS 1.1 cable IP’s to connect their customers. The limited shared up-load bandwidth in this “last mile” connectivity was sensitive to such P2P applications that could easily overload the local network connections.

Comcast responded by taking actual datagram packets being sent by P2P applications and modifying the data within the packet to change the reset bit within the flow label portion of the header. [29] This had the effect of temporarily ending the virtual connection between the P2P interactors, and thus reduced the traffic load. It would take a significant amount of time for the P2P applications to restart and begin attempting to send data again. Comcast spokespersons indicated that this method of packet modification was justified because dropping or delaying packets would not have slowed down the traffic given the nature of the P2P applications. Some critics have accused Comcast of being too heavy-handed in its response to P2P applications, and have likened what they did to the equivalent within the voice telephone arena of impersonating a talker’s voice and telling the listener “goodbye,” in order to disconnect the conversation. In its defense, Comcast claims that reset changes within a packet fall within reasonable network management policy. By a 3 to 2 majority, FCC decided recently that Comcast’s actions went beyond reasonable network management and violated net neutrality. [30] The FCC chose not to punish Comcast, however.

Encryption as a counter-measure

Given the degree of datagram packet inspection with its issues of privacy invasion, security, and impetus for non-neutral network management activities and policies, many applications and their developers have suggested moving in the direction of packet encryption as a form of protection from any major deviations in net neutrality and other abuses. Because only the

data payload can be encrypted, it can only offer limited protection. Since the header must be sent in the clear, non-net neutral discrimination could be based on header information. Second, DPI can be used to determine general characteristic of even encrypted payload information because the statistically repetitive nature of many types of applications can be determined even with encrypted payload data. [31] Add to the fact that encryption usually increases data payload requirements and adds more delay in processing most applications, this makes encryption a less effective mechanism for preventing or discouraging any non-neutral policies and actions on the Internet.

Role of the FCC

The FCC, under the Telecommunications Act of 1934 as amended in 1996 under 706 of the Public Law 104-104, [32] has jurisdiction over net neutrality. The FCC is responsible “to preserve the vibrant and competitive free market that presently exists for the Internet, ... and to promote continued development of the Internet.” Thus, the FCC has the responsibility to decide the technical and operational boundaries as to when a network provider’s action constitutes reasonable network management behavior and when those actions constitute unacceptable non-network neutral behavior.

In 2005, the FCC promulgated a set of broadband network principles. In their words:

“As a result, the Commission has jurisdiction necessary to ensure that providers of telecommunications for Internet access or Internet Protocol-enabled (IP-enabled) services are operated in a neutral manner. Moreover, to ensure that broadband networks are widely deployed, open, affordable, and accessible to all consumers, the Commission adopts the following principles

- *To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to access the lawful Internet content of their choice.*
- *To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to run applications and use services of their choice, subject to the needs of law enforcement.*
- *To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to connect their choice of legal devices that do not harm the network.*

- *To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to competition among network providers, application and service providers, and content providers.”*

These are obviously high-level, policy-oriented principles and not designed as detailed regulations or constraints. These principles are less direct and potentially less controversial than Weitzner’s four principles. What they imply is that the FCC must continue to work with an active policy and within a regulatory arena to keep assessing the actions of the telecommunications industry and to continuously judge whether the actions of all the players are consistent with their four principles. Others, such as Weitzner, Wu, and Lessig, have suggested additional and potentially more restrictive principles for the FCC to follow. Perhaps the FCC will expand and detail their approach in the future, but the author believes that the most prudent approach is not to rush to a detailed technical solution or prohibition prematurely. The community of telecommunications providers, application providers, intellectual property owners, and end users has much more to learn. On the other hand, as many have pointed out, the Internet with its end-to-end open and flexible technologies have allowed for the creation of immense value and economic growth for use through the Internet over the last 20 years. We should be very careful before we allow any of its capabilities to be transformed away as the Internet evolves.

Conclusions

This paper has described the issues surrounding concept of net neutrality for the Internet. Multiple sides of this issue were presented. While it should be clear that this is an important and complex issue, it is not clear exactly what should be done to respond to this issue. Proponents of net neutrality believe that federal legislation should be enacted to attempt to define and protect net neutrality. While some may oppose net neutrality for somewhat self-serving reasons, there is a very legitimate concern that prematurely enacted and poorly developed net neutrality legislation could well be counter-productive and actually cause more harm than good. Among those who suggest something should be put into law, there is some disagreement over how net neutrality should be enforced. [33] For example, should the FCC be given the continued mandate and extended powers and resources to enforce a net neutrality prescription, or should the federal courts take up the charge of enforcing a net neutrality regulation as an amendment to the Clayton Anti-Trust Act?

It is this author's contention and those of others [34] that it is probably premature for a definitive net neutrality regulation to be developed along with significant penalties or total sanctions except for the most egregious behaviors by the telecommunications providers. There is a need to learn more about the full range of issues facing the Internet and its future and to establish needs and priorities for the role of the Internet in the future. Given the mandate already established for the FCC in this regard, and with a modest degree of resources allocated to discussion of how the Internet should evolve, a workable approach can be found. It is important that those who are observing and watching what is happening to Internet resources, policies, and practices be given a highly visible forum to inform both the public and the policy makers. As time goes on, telecommunications providers and others who have a stake in the Internet must articulate their policies and present a clear indication of their actions that impact net neutrality. As long as the topic is of mutual concern and the FCC has the clear mandate to adjudicate issues related to net neutrality behavior for all parties, the chance for better working solutions and better policies and practices down the road will be greatly enhanced. ■

Notes and references

1. Wu, Tim, "Network Neutrality, Broadband Discrimination," *Journal of Telecommunications and High Technology Law*, vol. 2, pp. 141, 2003; http://papers.ssrn.com/sol3/papers.cfm?abstract_id=388863.
2. Ou, George, "A Rational Debate on Net Neutrality," *Real World IT – ZDNET*, July 4, 2007; <http://blogs.zdnet.com/Ou/?p=512>.
3. Wikipedia, "Network Neutrality Legislative Proposals Introduced in Congress" (under section on Attempted Legislation), August 2008; http://en.wikipedia.org/wiki/Network_neutrality_in_the_United_States#cite_note-1.
4. Representative Edward Markey, "Internet Freedom Law Will Keep Internet Open for Future Innovators," Office of Congressman Markey, February 13, 2008; http://markey.house.gov/index.php?option=com_content&task=view&id=3268&Itemid=141.
5. Shuler, Rus, "How Does the Internet Work?" *The Shuler Website*, 2005; http://www.theshulers.com/whitepapers/internet_whitepaper/index.html.
6. Leiner, B. M., V. G. Cerf, D. D. Clark, R. E. Kahn, L. Kleinrock, D. C. Lynch, J. Postel, L. G. Roberts, and S. Wolff, "A Brief History of the Internet, ver. 3.32," *The Internet Society*, last revised December 10, 2003; <http://www.isoc.org/internet/history/brief.shtml>.
7. Peha, Jon M., "The Benefits and Risks of Mandating Network Neutrality, and the Quest for a Balanced Policy," *International Journal of Communication*, vol. 1, pp. 644–668, 2007; <https://www.dpaket.org/articles/benefits-and-risks-mandating-network-neutrality-and-quest-balanced-policy>.
8. Bailey, Charles W. Jr., "Strong Copyright + DRM + Weak Net Neutrality = Digital Dystopia?" *Information Technology and Libraries*, September 2006; <http://www.lita.org/ala/lita/litapublications/ital/252006/number3september/bailey.pdf>.
9. Reardon, Marguerite, "Comcast Denies Monkeying with BitTorrent Traffic," *CNet News.com*, August 21, 2007; http://news.cnet.com/8301-10784_3-9763901-7.html.
10. Svensson, Peter, "Comcast Defends Internet-Filtering Practices," *MSNBC Website: Technology and Science/Security*, February 12, 2008; <http://www.msnbc.msn.com/id/23136119/>.
11. Wu, Tim, "Why You Should Care About Network Neutrality: The Future of the Internet Depends on It!" *Slate Website*, May 1, 2006; <http://www.slate.com/id/2140850/>.
12. "Top 100 Websites in the United States," *Alexa: The Web Information Company*, August 2, 2008; http://www.alexa.com/site/ds/top_sites?cc=US&ts_mode=country&lang=none.
13. Broache, Anne, "RIAA: Don't Let Net Neutrality Hurt Piracy Fight," *CNet News.com*, May 6, 2008; http://news.cnet.com/8301-10784_3-9937153-7.html?part=rss&subj=news&tag=2547-1_3-0-20.
14. Zapardiel, Juan A. and Fernando García, "Why Should a Government Invest in the Internet? The Experience of the Ministry of Economy and Finance of Spain," *Proceedings of the Internet Society*, June 8, 1999; http://www.isoc.org/inet99/proceedings/3a/3a_1.htm.
15. Saint Sauver, Joe, "Converging Campus Technologies—Evolution or Intelligent Re-Design?" *NWACC Annual Conference*, June 9, 2006; www.uoregon.edu/~joe/convergence/nwacc2006.ppt.
16. Hahn, Robert W. and Robert E. Litan, "The Myth of Network Neutrality and the Threat to Internet Innovation," Publication 06-33, *The Milken Institute Review*, First Quarter 2007; <http://www.milkeninstitute.org/publications/publications.taf?function=detail&ID=586&cat=mir>.
17. Radizeski, Peter, "TWC Metering Bandwidth," *TMCnet*, June 5, 2008; <http://blog.tmcnet.com/on-rads-radar/2008/06/twc-metering-bandwidth.html>.
18. Odlyzko, Andrew M., "Internet Traffic Growth: Sources and Implications," *Proceedings of the International Society for Optical Engineering*, vol. 5247, October 16, 2003; http://www.dtc.umn.edu/publications/reports/2003_10.pdf.
19. Gidari, Albert, "The Communications Assistance for Law Enforcement Act (CALEA)," Office for Information Technology Policy, American Library Association, January 2007; <http://www.ala.org/ala/washoff/woissues/techintelle/calea/caleajan07.pdf>.
20. "Broadband Penetration Grows to 57% in US Homes," *WebSiteOptimization.com*, April 21, 2008; <http://www.websiteoptimization.com/bw/0804/>.
21. Zittrain, Jonathon, *The Future of the Internet and How to Stop It*, Yale University Press, April 2008.
22. Weitzner, Daniel J., "The Neutral Internet: An Information Architecture for Open Societies," *MIT Computer Science and Artificial Intelligence Laboratory*, June 20, 2006; <http://dig.csail.mit.edu/2006/06/neutralnet.pdf>.
23. Wilson, Carol, "DPI: The Good, The Bad, The Stuff No One Talks About," *Telephony On-Line*, July 18, 2008; <http://telephonyonline.com/iptv/news/dpi-scorned-but-thriving-0721/index.html>.
24. Puzanghera, Jim, "House Panelists Seek Opt-In Rule for Web Tracking," *Los Angeles Times*, July 18, 2008; <http://www.latimes.com/business/la-fi-techblog18-2008jul18,0,7684928.story>.
25. Reis, C., S. D. Gribble, T. Kohno, and N. C. Weaver, "Detecting In-Flight Page Changes with Web Tripwires," *International Computer Science Institute (ICSI)*, February 29, 2008; <http://www.cs.washington.edu/research/security/web-tripwire.html>.
26. "Deep Packet Inspection and Privacy," Electronic Privacy Information Center, August 4, 2008; <http://epic.org/privacy/dpi/>.
27. Anderson, Nate, "Deep Packet Inspection Meets Net Neutrality, CALEA," *Ars Technica*, July 25, 2007; <http://arstechnica.com/articles/culture/Deep-packet-inspection-meets-net-neutrality.ars/1>.
28. Wu, George, "Why Network Management is Essential to the Internet," Testimony before the Federal Communications Commission, Washington, DC, WC Docket No. 07-52, In the Matter of Broadband Industry Practices Hearing, Stanford University, April 17, 2008; http://www.fcc.gov/broadband_network_management/041708/ou-stmt.pdf.
29. Metz, Cade, "Comcast Admits it Can Do the Impossible—'We Will Stop Busting BitTorrents,'" *The Register*, March 28, 2008; http://www.theregister.co.uk/2008/03/28/comcast_to_stop_busting_bittorrents/.
30. "FCC Rules Against Comcast Agency: Blocks on Video Files Hamper 'Open' Internet," *Chicago Tribune* (through *New York Times News Ser-*

vice), August 2, 2008; <http://www.chicagotribune.com/business/chi-sat-internet-fcc-comcast-aug02,0,1442111.story>.

31. Dusi, M., M. Crotti, F. Gringoli, and L. Salgarelli, "Detection of Encrypted Tunnels Across Network Boundaries," *2008 IEEE International Conference on Communications (ICC 2008)*, May 2008; <http://www.ing.unibs.it/~gringoli/pub/PID578397b.pdf>. [also] Orion, Egan, "Encryption Might Not Protect Net Neutrality Comment—A See-Saw Cat-and-Mouse Game Looms," *The Inquirer*, 30 June 2008; <http://www.theinquirer.net/gb/inquirer/news/2008/06/30/encryption-might-protect-net>.
32. Federal Communications Commission (FCC), "Policy Statement: Appropriate Framework for Broadband Access over Wireline Facilities," Document FCC-05-151, August 5, 2005; <http://www.publicknowledge.org/pdf/FCC-05-151A1.pdf>.
33. Rosch, J. Thomas, FTC Commissioner, "Broadband Access Policy: The Role of Antitrust," Broadband Policy Summit IV: Navigating the Digital Revolution, Washington, DC, June 13, 2008; <http://www.ftc.gov/speeches/rosch/080613broadbandaccess.pdf>.
34. Lessig, Lawrence, "Net Neutrality Blog Archives—April 2003–April 2008," *Lessig Blog*, <http://lessig.org/blog/netneutrality/>.

About the author



W. Scott Nainis is a senior principal at Noblis where his experience includes information systems, telecommunications systems, and business process planning, design, and evaluation for a wide range of federal and state agencies. He has extensive experience in analysis and modeling in support of the energy, environment, and manufacturing/logistics sectors for both commercial and government clients. He received his doctorate degree in systems engineering with a minor in operations research from Case Western Reserve University. Contact him at snainis@noblis.org.