Before the

Federal Communications Commission

Washington, D.C. 20554

In the Matter of Restoring Internet Freedom (sic)

WC Docket No. 17-108

August 30, 2017

**Reply Comments of NetAccess Futures**

NetAccess Futures, through its Principal, Daniel B. Grossman, hereby submits these comments in reply to two responses to the NPRM adopted May 18, 2017, in the above captioned matter.

**Contents**

I. Introduction and Observations 2

A. About these reply comments 2

B. Background 2

C. This proceeding brings disgrace upon the Commission 3

D. The NPRM is unworthy of an independent Federal agency 3

E. The NPRM is based upon false premises 4

II. Outline of Our Position 6

The Internet’s architecture Inherently provides Technical ability – But not necessarily incentives - to violate openness 8

A. Packet Forwarding 8

B. Bandwidth Reservation and Admission Control 11

C. Domain Name Service 12

D. Routing 13

E. Recent Developments 13

III. broadband investment is growing 14

IV. ISPs are more like Telecommunications providers than Information providers 16

V. Conclusion 19

# Introduction and Observations

## About these reply comments

NetAccess Futures (“we”) is an industry analysis consultancy, specializing in broadband access networking technology and strategy. Its Principal, Daniel B. Grossman, has over 35 years of experience in data networking technology and telecommunications. He has been deeply interested in the interaction between communications technology, economics and policy. Past experience also exposed him to the Commission’s Rules and procedures, and instilled respect for their role in maintaining competitive markets.

We have not engaged counsel to prepare these reply comments, which therefore no doubt deviate from normative form. We have not footnoted as extensively as we might, and most footnotes are incomplete. Further, we have not researched or developed all of our arguments as fully as we might have preferred.

Since we must prioritize paid work, we were not able to respond to the NPRM during the comment period, and have had little time to prepare these reply comments. It is not humanly possible for an individual to review the entire record of more than 8 million comments, an unknown number of which are substantive. Indeed, we feel sorry for Wireline Bureau staff, who have had to wade through all of them. Two extensive comments have come to our attention, *Free Press*[[1]](#footnote-1) and the *Joint Comments Internet Engineers, Pioneers and Technologists*[[2]](#footnote-2), which capture our clear understandings and earn our support and elaboration.

We think it valuable to have these Reply comments on the record, not because we expect it to influence Commission actions, but rather in the likelihood that this matter will be revisited on appeal. If any of these comments are of an *ex-parte* nature, we request that they nonetheless be part of the public record.

NetAccess Futures does not presently have any clients who are parties in this matter.

## Background

NetAccess Futures filed extensive comments in Open Internet proceeding[[3]](#footnote-3) We were gratified to note that the Commission adopted many of the ideas proposed in our comments, and indeed referenced them in the Order. The decision to apply Title II to ISPs was a pleasant surprise; we had assumed that the previous Chairman did not have the stomach for the controversy that subsequently came to pass. That said, we assumed that the rules were settled, and that the courts would uphold them.

The disastrous 2016 election upset that, as well as many other apple carts. Chairman Wheeler was forced to resign, and Commissioner Pai was promoted to Chairman. This administration has a penchant for turning gold into manure, and the FCC was not an exception.

## This proceeding brings disgrace upon the Commission

Chairman Wheeler restored the public’s trust in the FCC with the Open Internet order, the Internet Privacy order, and other Commission actions. Prior to the Open Internet order, he was wrongly derided as an industry stooge and a hungry dingo left to mind the baby. Afterwards, he was recognized as a dedicated public servant who put consumer interests first. The Commission basked in its new-found reputation.

Regrettably, Chairman Pai seeks to reverse all that, and bring the Commission back into public disrepute. Regardless of the Chairman’s interior motives, this proceeding stinks of revolving doors, regulatory capture and pay-to-play – business as usual in the Washington swamp. It creates a perception of public corruption, regardless of whether individual Commissioners have violated any law or ethics rule.

Recognizing that public comments in regulatory proceedings are not a referendum, the possibility that the Commission will ignore more than 21 million comments from concerned citizens is troubling. That the Chairman opened this proceeding to reverse a previous rulemaking that enjoyed enormous public support is yet more troubling. By adopting this item, the Commission has thumbed its nose at the concerned public.

## The NPRM is unworthy of an independent Federal agency

In more than 35 years of reading Commission documents, I have never seen anything like this NPRM. It is, bluntly, a partisan hack job, devoid of any semblance of balance or intellectual integrity. The Chairman elected to use inflammatory, prejudicial language and hyperbole, attacking and belittling his predecessor and dismissing any doubt of the righteousness of his cause. It is rooted in an extreme anti-regulatory, unfettered free market ideology which ignores real-world experience.

This document was apparently written from the same style manual used by Kellyanne Conway and Sean Spicer. It confidently revels in contradictions and counterfactuals. It is loaded with pretzel logic. It is the definition of doublethink. The very title, “Restoring Internet Freedom” is Orwellian; it is about freedom only in the sense of “Freedom is Slavery”.[[4]](#footnote-4) We are somehow to believe that restraints against abusive practices by dominant business entities somehow harm the public interest. We are to think that documented abuses by ISPs never happened. To a reader deeply familiar with the subject, its claims are patently devoid of evidence and reason.

The NPRM dismisses Title II of the Communications Act of 1934 as “utility-style regulation”, somehow irrelevant to present circumstances. Regardless of the Chairman’s opinion, Title II remains the law until Congress changes it. The NPRM proposes, in effect, that the Commission abdicate its statutory responsibility to regulate. That a regulatory agency refuses to do its job is not unheard of in Republican administrations, but nonetheless an assault on the Rule of Law.

## The NPRM is based upon false premises

The NPRM is framed around a series of untrue, unproven and risible claims.

### It claims that the application of Title II to ISPs has hurt investment. This is at best an untestable hypothesis, and contrary to all evidence and our professional experience. We discuss this below in support of the comments of Public Knowledge.

### It misrepresents the workings of the Internet. We discuss this below in support of the comments of the Internet Engineers.

### It conflates the consumer broadband access market with the Internet applications and content market.

### It claims that broadband access is a competitive market, despite the FCC’s own data to the contrary. [insert numbers from this year’s broadband report here]

### It claims that the Open Internet order reverses a bipartisan consensus that broadband access should be treated as unregulated Information Services. This is based on a twisted view of history, and a blatant misrepresentation of the present debate. We challenge the Chairman to identify one minority member of the Commissions’s oversight committees who supports this action.

### It assumes that “utility style regulation” is somehow a relic, irrelevant in the Internet era. First, the dog-whistle phrase is misleading; common carriage and public utility are not synonymous. Nothing in the Open Internet order comes even close to the level of micromanagement that arises from utility regulation. The order deliberately eschewed any price regulation, much less rate-of-return regulation. Common carriage is the appropriate status for ISPs. Indeed, the conditions that led to the communications act – a natural monopoly in transmission over bottleneck facilities and resulting lack of market discipline – hold every bit as much for the fiber and coax of the first third of 21st century as they did for twisted pairs in the 20th century.

### It treats the very minimal demands of the Open Internet order as an insurmountable burden on ISPs. In fact, they do not apply to the Tier-3 carriers with fewer than 250,000 subscribers, which typically lack a regulatory support infrastructure. Tier-1 and Tier-2 carriers need only file a minimum amount of reports and affidavits and, more important, abide by the Rules. They suffer only if they want to do something contrary to the Rules, which they should not be permitted to do in the first place, and which they claim they have no interest in doing.

### It suggests that industry might self-regulate against abusive practices. In other words, the fox can guard the hen house. This idea is so risible as not to deserve a response.

# Outline of Our Principles

In our comments on the Open Internet order, we expressed the following thoughts, which we excerpt for the convenience of Commission staff and future plaintiff’s attorneys.

1. We take the societal value of the Internet as a given that requires no elaboration. The Internet’s supporting facilities are critical infrastructure and a utility (with a small ‘u’).
2. There is insufficient competition in local broadband access markets to assert market discipline. Broadband providers have (but do not necessarily act upon) perverse incentives, supported by lack of market discipline. Specifically, they are in a position to engage in anti-competitive and anti-consumer practices, extraction of monopoly rents, self-dealing and (arguably) suppression of public discourse. The Commission’s Rules and enforcement process must therefore substitute for market forces in prohibiting such abuses.
3. “The Internet” represents a value chain of consumers, network providers, edge providers, content providers and others. Allocation of consumer revenue among the rest of the value chain is a zero-sum game. The Commission will frequently be called upon to adjudicate tussles over cost and revenue[[5]](#footnote-5).
4. The Internet is a Network of Networks. While nobody “owns the Internet”, some entity owns each of its constituent networks. Those entities are often for-profit corporations. Capital and operating expenses for building, operating, maintaining and upgrading networks – particularly access network infrastructure – are immense. The Internet’s business model must support adequate return-on-investment to incent these investments.
5. The Internet’s architecture is not engraved on stone tablets, according to some platonic ideal, forever immutable. It evolves in response to identified engineering and business problems. The way the Internet actually works is very different from the way it is generally perceived to work.
6. Point-of-view based blocking and degradation of traffic is odious and unacceptable. The Commission must be vigilant against anti-competitive blocking and degradation.
7. The Internet is a content agnostic platform for all forms of communications. However, the technical and economic characteristics of various communications varies widely. Traffic handling behaviors are optimal for some applications, content and protocols, and are sub-optimal (or even inadequate) for others. The Internet can and should handle traffic in the most optimal fashion.
8. The Internet’s canonical and default traffic handling behavior is “Best Effort”, with flat rate charging.
9. Best Effort service must treat traffic from all sources to all destinations roughly “fairly”, without commercial discrimination. Excess delay and packet dropping should occur only during periods of congestion.
10. The Internet’s dynamics are complex, incompletely understood, and often counter-intuitive. Differentiated traffic handling can, in some circumstances, improve overall performance.
11. The Commission should be vigilant against egregious practices and be empowered and prepared to take enforcement action when needed.

The Open Internet order fulfilled these principles. The NPRM seeks to undermine them.

# The Internet’s architecture Inherently provides Technical ability – But not necessarily incentives - to violate openness

In our previous comments, we sought to clarify the record as to the technical mechanisms that might be abused by ISPs for this for anti-competitive purposes and monopoly rent-seeking. Note that they concur with the comments of the Internet Engineers. We reiterate them here.

## Packet Forwarding

The Internet’s architecture requires that each router along the path from source to destination to undertake a prescribed series of steps[[6]](#footnote-6), some of them mandatory and some optional, to forward packets. Of particular interest are:

1. Classification of individual packets by fields in the packet headers, including IP Source and Destination Address, Protocol, Differentiated Services Code Point, and Port Number. Classifiers match to patterns of Boolean strings within these fields. Further classification using application data, or deep packet inspection (DPI) is also used. A classifier database contains a set of patterns, and for each pattern, an outgoing link and a set of one or more action to be taken by the router upon packets that match the pattern.
2. Identification of flows of packets, based upon results of classification. A flow is a series of packets from a source to a destination which are inferred to be related to a single or aggregated instance of communication.
3. Traffic conditioning of flows (or groups of flows). Traffic conditioning can take the form of rate shaping (i.e., retaining packets when the flow exceeds a configured rate, and metering them out according to that rate), rate policing (i.e., discarding packets when a flow exceeds a configured rate) or metering (i.e., passively measuring the rate of each flow). Rate shaping devolves to rate policing when the number of retained packets reaches a configured limit.
4. Queueing of packets based on classification and/or flow identity. As they are received (i.e. before classification), packets are stored in data structures called “buffers”. Buffers are further organized into first-in, first-out (FIFO) queues. A router typically has several queues at the input and/or output of each interface. Each buffer is added to a queue, typically based upon packet classification results.
5. Packet discard. Routers (and their component modules) can buffer a finite number of packets. When packet arrivals exceed packet departures the router must discard some packets; i.e., by returning packet buffers to the free buffer pool. Discard is normal, even desirable, behavior[[7]](#footnote-7). In particular, it is used by the TCP protocol as a congestion signal for end-to-end rate control. For this reason, current best practice is to discard packets pro-actively[[8]](#footnote-8), in advance of severe congestion. Strategies for doing so are complex, and small changes to discard algorithms or their parameters can have a significant effect on congestion.
6. Packet scheduling. When an outgoing link becomes idle, the router must select which queue to service next. Service consists of removing a packet buffer from the selected queue, serializing it, and transmitting the resulting bit stream over the link. Scheduling disciplines are typically sophisticated[[9]](#footnote-9), and are configured by the broadband provider in order to effectuate various objectives. In addition, a scheduler can also serve as a traffic shaper.
7. Packet marking. Internet Protocol (IP) [[10]](#footnote-10) packet headers contain a field called the “Differentiated Services Code Point” (DSCP)[[11]](#footnote-11), and another field called “Explicit Congestion Notification”(ECN)[[12]](#footnote-12). The former is used to alter the match and action of packet classifiers. The latter is used as a secondary network congestion signal, to be used by TCP’s congestion management mechanisms. A router may alter these fields, based on packet classification, queue occupancy and/or traffic conditioning. The altered DSCP field is seen by classifiers in subsequent routers along the path. Thus, when a router alters the DSCP field, it changes forwarding actions (e.g., different queueing or discard policies) along the remainder of the path. When a router alters the ECN field, the rate of the flow is expected to be reduced. [Note that the *Joint Comments* doubt that these capabilities are widely deployed in the public Internet.]

All of these mechanisms are indispensable for network function or reasonable network management.

* Classification and sometimes flow identification are needed in order to determine which actions must be taken on a packet, and to determine the “next hop” link over which the packet is to be forwarded.
* Traffic conditioning is used in conjunction with queueing and scheduling in order to effect bandwidth allocation (as we describe below). It is also used to enforce rate caps, for congestion management[[13]](#footnote-13) and defense against certain kinds of attacks.
* Queuing provides for in-order transmission of packets, for fairness between flows, and for management of bandwidth.
* Discard protects the router’s buffer resources against overload, and is the primary congestion signal used by TCP to adjust its rate.
* Marking simplifies packet classification at subsequent routers, and effects traffic management for particular flows.

All of these mechanisms can also be abused, to the detriment of Open Internet principles.

* Packet classification and sometimes flow identification are necessary precursors to discrimination against (or in favor of) certain packets or flows.
* Traffic conditioning can be abused, possibly in conjunction with queueing and scheduling, to throttle disfavored flows.
* Special advantaged or disadvantaged queues can be configured for discriminatory treatment.
* Packet discard can be used unfairly to favor or disfavor specific flows through TCP’s congestion avoidance mechanism.
* DSCP marking can be used to indicate favored or disfavored flows, and ECN marking can be used to effect TCP congestion avoidance for disfavored flows.

## Bandwidth Reservation and Admission Control

The Best Effort service is based on cooperative sharing of resources. Packet flows start and end without explicit notification to, or permission from, the network. They are assumed to adjust their rates according to TCP’s slow start and congestion avoidance mechanisms, based on presence or absence of congestion signals. This behavior gives each flow an approximately fair share of the capacity of the bottleneck link. Rate adjustment in response to congestion signaling is a form of closed loop control. No capacity is reserved for a Best Effort flow; it takes what it gets.

Services that rely, wholly or partly, upon open loop control have different mechanisms for resource sharing. Capacity (or “bandwidth”) is reserved. Reservation can be dynamic, using a signaling protocol such as RSVP[[14]](#footnote-14) to negotiate bandwidth at the start of a flow, and release it at the end. It can also be static. Reservation typically means preferential, rather than exclusive, access to capacity. If a flow is not using all of its reserved bandwidth, the unused capacity is available for other flows. Open loop controlled flows are defined by a traffic specification (TSpec) which characterizes the flow’s rate. A traffic conditioner enforces compliance with the TSpec, delaying, dropping or marking packets in excess of the agreed rate. The reserved bandwidth is a function of the TSpec. Some services allow a flow to have a reserved component and a Best Effort component.

The sum of reservations at each resource must not exceed the capacity of that resource. The admission control function performs bandwidth reservation[[15]](#footnote-15), only if sufficient capacity is available; otherwise the network must deny the flow. The flow might proceed as Best Effort, or it might be blocked.

These flows coexist with Best Effort flows. Typically, a network engineer will allocate a pool of capacity to be shared by all Best Effort flows. The capacity in this pool is not available for reservations. Best effort flows share that pool, along with any capacity that has been reserved but not in use. The capacity of the Best Effort pool must be sufficient to meet acceptable performance targets for Best Effort traffic.

As we describe below, there are numerous valid reasons for open loop controls in addition to closed loop controls. Thus, bandwidth reservation and admission control are needed in order to offer services other than Best Effort. They also are subject to anti-competitive and anti-consumer abuse by broadband providers. If flat-rate charging applies for Best Effort service, and additional pricing applies for other services, broadband providers are incented to minimize the Best Effort pool. This has the effect of starving Best Effort flows. This is the technical substance of the feared “fast lanes”. Admission control is subject to commercially unreasonable discrimination, such as giving precedence to admission of favored flows (e.g., from an affiliated entity) or denying access to non-favored flows.

## Domain Name Service

The Internet’s Domain Name Service (DNS) resolves human-usable domain names (e.g., “fcc.gov”) into IP addresses (e.g., 192.52.94.5). It allows applications to use human-friendly, topology independent names, while the network infrastructure operates on machine-friendly, topology dependent addresses. It also allows content to be location independent.

DNS is a distributed database system, comprised of “name servers”. It is the only part of the Internet’s architecture that is hierarchical, rather than peer-to-peer in structure. The database need not be consistent: a name frequently resolves to different addresses, depending on which name server is queried.

DNS is an important service provided by ISPs; in light of *Brand X*, this includes broadband providers. Typically, when a consumer device connects to its local network, it uses the Dynamic Host Configuration Protocol (DHCP) to obtain the IP address of a local primary and secondary Name Server. The source of this information is the broadband provider’s DHCP server (or its proxy), which provides the addresses of the broadband provider’ DNS server (or a proxy). As a result, unless the user configures their device to use a different DNS server, name resolution is controlled by the broadband service provider.

The flexibility of DNS is extremely valuable to the Internet’s operation. In particular, content distribution networks (CDNs) use DNS to resolve the name of a content resource to the most optimal server that has that content. However, this flexibility can also be abused by ISPs to redirect user queries to their own services and content. Further, the largest broadband provider ISPs[[16]](#footnote-16) have recently entered the CDN market, and thus compete with independent CDN providers. This might be an incentive to improperly modify databases in their DNS servers.

## Routing

The Internet’s routing system distributes topology information, which is used by each router to create a “forwarding database”. The forwarding database maps destination IP addresses to a “next hop” or outgoing link to be used by packets which carry that address.

The routing system can be abused in order to send packets to favored destinations along specially engineered paths not available to disfavored packets. It can also be abused to send packets to disfavored destinations over unnecessarily long or frequently congested paths.

## Recent developments [not part of our 2014 comments]

The industry is undergoing massive transformation, much of it with the theme that purpose-built, chassis-based hardware with embedded software should be displaced by generic hardware and virtualized and largely open-sourced software running in generic servers. The ostensible benefits include:

### Capital cost reduction, by using generic “white box” hardware with generic Ethernet interconnects rather than proprietary, high-margin chassis.

### Greater scalability; as endpoints are added and new services emerge, the growth and upgrade path is simplified.

### Reduced clerical overhead through automation of previously manual tasks.

### Streamlining and modernization

### Reduced time to create and roll out new services. Providers can develop new service software, or adapt and customize open source software, reducing dependency upon vendors. Agile development and DevOps shorten development cycles, trading a little risk for timeliness.

This last point is an opportunity for abuse. With embedded systems, an ISP seeking new technical means to violate Open Internet principles would need to conspire with vendors. This would leave a trail of evidence and broad risk of disclosure. Even trivial additions would require a long process for the vendor to prioritize, resource, develop, test and release. With software defined networks (SDN) and network function virtualization (NFV), the ISP has complete control over software development, and ability to deploy new features selectively and covertly. SDN and NFV are, on balance, a great improvement upon past architectures and practices. However they also give ISPs – even rouge employees –the opportunity to modify packet processing behavior in ways detrimental to consumers and competition. For example, one could imagine a covert virtual network function (VNF) that performed traffic analysis for purposes of profiling individual consumers based on their usage patterns. Another might hijack DNS requests from a third-party server to the ISP’s own DNS server. While these threats are hypothetical, they are not whimsical, and the Commission must have the authority to preemptively prohibit them and respond promptly to complaints.

# broadband investment is growing

The NPRM is premised on the dogma that burdensome regulation somehow inhibits broadband investment. This is contrary to our long experience and understanding of the broadband provider and equipment market. Indeed, our most recent report, for the respected industry analysis firm *Heavy Reading*[[17]](#footnote-17) , presents evidence of robust growth in infrastructure investment. “Acute needs for x-haul for 4G mobile densification and 5G, IoT, business services upgrades, and Gigabit broadband is driving a resurgence in access fiber construction.”[[18]](#footnote-18) In addition, MSOs are rapidly deploying DOCSIS 3.1 and are upgrading their HFC infrastructure with node splits, bandwidth upgrades and fiber-deep architectures. These share the same business drivers as those that motivate the telecom players.

Our understanding of marketplace realities fully supports the analysis and conclusions of Part VI of Free Press’ Comments.[[19]](#footnote-19) With respect to the broadband markets that we cover, we fully concur. We commend the research and analysis of Derek Turner et al, finding it to be thorough and well-reasoned. Indeed, had we been commissioned to write such a report, we would have used the same sources and methodologies. They completely debunk, in our view, the arguments and cherry-picked facts of USTA, Singer, et. al.

More recent evidence supports Free Press. For example, the three Tier-1 telecom carriers each announced major expansions of their fiber-to-the-home footprint. In the words of Veronica Bloodworth, SVP of Construction at AT&T "Our team is focused on building Fiber to the premises… we are hockey sticking our fiber deployment[[20]](#footnote-20)". Beyond their merger commitment to the Commission to pass 14M homes, they are on track to pass 17M homes by the end of 2018[[21]](#footnote-21). Verizon has adopted the slogan “Fiber is Sexy Again”, a refrain repeated by their CEO, CFO and Chief Network Officer[[22]](#footnote-22). More substantively, they announced a 3-year, $3B procurement contract with Corning to purchase fiber cables and accessories of the kind they use to build FTTH distribution networks. They tout high-profile multi-service fiber build in the City of Boston as a template for future deployments. They also continue to expand their serve footprint within FTTH-served wire centers. They have filed discontinuance notices for wireline telephone service, transitioning to fiber, at an increasing pace. In the meantime, Tier-2 and rural operators have been increasing their rates of fiber deployment. Thirty percent of rural carriers have adopted FTTH over their entire footprint[[23]](#footnote-23). Investors once again are interested in these kinds of deployments; for example, broadband revenue bonds are once again marketable, and hedge funds have made massive equity investments. Singer estimates that announced deployments will almost double the number of US homes passed, from 32.5M to 55M. According to SNL Kagan, domestic US telecom spending on FTTH optical network terminators and optical line terminator ports rose nearly 50% in 2016.[[24]](#footnote-24)

On the cable side, all of the major MSOs have announced plant upgrades, typically to eliminate unreliable, bandwidth-limiting equipment from the network and better support DOCSIS 3.1. For example, Comcast plans to install 1M new fiber nodes in their network, in addition to the present 250,000. Similarly, Cox is installing 200k fiber nodes in addition to the existing 25k. Altice plans to upgrade most of their footprint to FTTH by the end of 2022.

The trends show a vibrant industry with big plans, not one contracting from over-regulation. Subjectively, the level of enthusiasm at the recent Fiber Broadband Council’s FiberConnect 2017 conference, relative to the rather dour mood at conferences we attended in 2014 and 2015, inspired our confidence. If providers are supposed to be “going Gault” from infrastructure building, the memo never made it out of their K Street offices.

# ISPs are more like Telecommunications providers than Information providers

We strongly concur with the Joint Comments of Internet Engineers, Pioneers, and Technologists[[25]](#footnote-25) (“Joint Comments”) First, we know many of the signatories personally, and others by reputation. Among them are some of the leading experts and innovators in Internet technologies. Their views are not to be taken lightly. They correctly warn that the authors of the NPRM “appear(s) to lack a fundamental understanding of what the Internet's technology promises to provide, how the Internet actually works, which entities in the Internet ecosystem provide which services, and what the similarities and differences are between the Internet and other telecommunications systems the FCC regulates as telecommunications services.” This is a familiar complaint, and our Open Internet NPRM comments[[26]](#footnote-26) reflected some of this frustration. Their cogent explanations bear thoughtful reading and comprehension.

The Joint Comments correctly point out fallacies in the NPRM’s hypothesis that ISPs are more like Information Providers than Telecommunications Providers, under the obsolete yet binding definitions of Computer III and the Telecommunications Act of 1996. The arguments in the NPRM fail to correctly apply the layering principle and the end-to-end principle, which are at the intellectual foundation of the Internet. Paragraph 27 of the NPRM illustrates the majority’s confusion. It suggests that “broadband Internet access service appears to offer its users the “capability” to perform each and every one of of the functions listed in the definition [of an Information Provider in Title II]—and accordingly appears to be an information service by definition. In light of layering and the end-to-end principle, this is not true. Telecommunications services, which are hop-by-hop, occur at a lower layer than Information Services, which are end-to-end. They provide and support a service that transports packets between a user and an Information Provider (by the Title II definition). The fact that those “capabilities” pass thorough them does not mean that they are offered by them. To those skilled in the art, such an argument is a non-sequitur and a cognitive dissonance. It is absurd when argued in the intellectual framework of our established model of the Internet.

Compounding this, the NPRM continues the *Cable Modem* fallacy that since broadband internet access providers also act as ISPs, their Telecommunications functions are negated. Email is given as an example, despite the rather obvious fact that most consumers are not using their ISPs’ email service, and ISPs’ email services can just as easily be accessed through a competing Telecommunications Provider as the broadband ISP serving the customer.

The NPRM proceeds to descend into a line of sophistry to the effect that since the entity providing BIAS is called a broadband ISP, and ISPs provide some information services, a broadband ISP is therefore an Information Services provider. This, too, is the *Cable Modem* fallacy, based on the way that broadband services were bundled in the early 2000s. A broadband ISP is not an Information provider that incidentally does some telecom-like things. It is an entity that provides telecom services and may also provide some information services. These services need to be treated separately from a regulatory perspective, regardless of their being offered by the same entity. Very little of the value that consumers obtain from their broadband ISP is in Internet Services. The value is in a Telecommunications service that transports packets across the local access and metro infrastructure to a peering point. All else is incidental. A reasonably savvy consumer could buy a pure IP telecommunications service from a telecommunications provider entity, and buy all information services – email, DNS and so on – from independent information service provider entity.

We cannot overemphasize this point. By way of personal example: we are so fortunate as to be served by Verizon’s FiOS FTTH service at our home/office. As far as we are concerned, all of the value we receive from the Internet portion of our monthly bill comes from the network termination equipment in our basement; our shared use of access fibers from our home to Verizon’s local central office; aggregation and transport from the CO to Verizon’s Greater Boston-area data center; edge routing functions; and transport to peering points (including CDNs). Verizon forwards IP packets bi-directionally between our home/office LAN and the next-hop peering point on the path to the information providers of our choice. These functions all fit within the Title II definition of a Telecom Service. That is what believe we are paying for, both as a consumer/small business and as a subject matter expert. We haven’t bothered to change DNS providers but know that we could (and perhaps should, in the interest of privacy). We don’t know and don’t care whether Verizon caches some of the content we receive. Only one of our numerous email accounts is in the verizon.net domain, and that is now hosted by Verizon’s subsidiary Oath (formerly AOL). Verizon’s network management, security and routing policies are transparent to us as consumers. Our MPVD service and IP telephony service are separate line items on our bill, and we purchase the bundle as a matter of convenience and pricing. This is not the *Cable Modem*-era model, where Information and Telecommunications services were essentially joined at the hip. Verizon is our Telecommunications Services provider and we incidentally and separately also obtain a small portion of our Information Services from Verizon.

The Joint Comments explain how the Internet has evolved since the Cable Modem order. We fully agree with their analysis, and have nothing further to add.

The Joint Comments proceed to eviscerate the NPRM’s rhetorical questions, addressing its willful misunderstandings of the relationships between entities and the services they provide, and the nature of packet switching in the Internet. We admire their patience in explaining these basic principles to a deliberately obtuse audience. We would elaborate further on their responses if time allowed.

The Joint Comments explain why the Commission should uphold the bright line rules with light touch regulation (note, however that their definition of “light touch” is that of Chairman Wheeler, not Chairman Pai). We are somewhat less cynical about the motivations of broadband ISPs, and consider severe impact from ISP misbehavior to be a moderate risk rather than a near certainty. The bright line rules define boundaries that ISPs rarely try to violate, but they nonetheless have crossed them on occasion. We take to heart the maxim that one should never attribute to malice what can be explained by incompetence, and believe that it holds for most of the parade of horribles cited by the Joint Comments and others. The value of bright line rules is that they back up the ISPs’ internal governance in fending off anti-competitive, anti-consumer schemes. For example, if a marketing executive proposes a way to use the ISP’s BIAS service to advantage their video service over its competitors, the bright line rules give the ISP’s legal staff the footing to block it. In addition, policies, procedures, and mandatory training around the bright line rules reduce the likelihood that misguided low-level employees will violate them.

Contrary to the Commission majority, we believe that prophylactic regulation is a sensible way to prevent abuses of market power. In the real world, in “Internet time”, any anti-consumer/anti-competitive abuses that see light of day require a relatively rapid regulatory response. Light touch application of Title II gives the Commission the authority to adjudicate complaints, and stanch the damage within months, rather than years. Prophylactic regulation keeps honest players honest and fends off bad actors.

The Joint Comments review examples of past harms that might have been prevented by the bright line rules. We have followed most of these, and concur that better regulation would have cut them off. They also reiterate a more general harm, caused by application developers’ need to evade anti-consumer/anti-competitive speed bumps set by ISPs. We are aware of such cases, and agree that the work-arounds are a needless burden on developers and consumers.

The Joint Comments further note that since the Open Internet order, ISPs have stopped prohibiting customers from connecting non-harmful devices and using BIAS in ways that they see fit. We experienced that when our wireless provider prevented us from tethering. Since they lifted that restriction in response to the Open Internet rules, we have been able to use our data plan with our laptop and tablet, both for business and recreation, when WiFi coverage was unavailable. Our history with Part 68 of the Commission’s rules, and with other CPE and equipment competition regulations, demonstrates that sensible regulation opens doors to third-party innovation and yields lower prices and better value for consumers.

# Conclusion

We regret that these comments are neither as complete, nor as refined, as we would wish them to be. As we noted above, they were not written on behalf of any client, but rather as a citizen/expert.

The Chairman should abandon this proceeding. It fails on its merits. It has attracted millions of negative public comments, and it only serves to damage the Commission’s reputation. Barring that, we hope that at least one of the Republican commissioners come to recognize this, and vote against the resulting Order. Otherwise, we have confidence that the DC Circuit will agree that this as an arbitrary and capricious action, well outside the bounds of *Chevron* doctrine, and overturn it.

Respectfully Submitted,

Daniel B. Grossman, dba NetAccess Futures.

1. cite [↑](#footnote-ref-1)
2. cite [↑](#footnote-ref-2)
3. Comments of NetAccess Futures, GN 14-28, April 3, 2014 and July 16, 2014 [↑](#footnote-ref-3)
4. Orwell, George, 1984 [↑](#footnote-ref-4)
5. c.f., Netflix comments [↑](#footnote-ref-5)
6. RFC 1812, RFC 2794 [↑](#footnote-ref-6)
7. ref Jim Gettys [↑](#footnote-ref-7)
8. RFC 7141 [↑](#footnote-ref-8)
9. The seminal work in this area is: Parekh, A.K.; Gallager, R.G. “A generalized processor sharing approach to flow control in integrated services networks-the single node case” IEEE/ACM Transactions on Networking, Volume: 1, Issue: 3 (June, 1993). [↑](#footnote-ref-9)
10. Differences between IP Version 4 and IP Version 6 are not relevant to this discussion [↑](#footnote-ref-10)
11. RFC 2474, RFC 2475 [↑](#footnote-ref-11)
12. RFC 3168 [↑](#footnote-ref-12)
13. Gettys, infa. [↑](#footnote-ref-13)
14. cite RFC [↑](#footnote-ref-14)
15. Bandwidth broker paper; RFC 4125-4128, RFC 4804 [↑](#footnote-ref-15)
16. Comcast cite, Verizon cite [↑](#footnote-ref-16)
17. cite HR report, to be published [↑](#footnote-ref-17)
18. cite Light Reading blog post [↑](#footnote-ref-18)
19. cite Free Press Comments, July 17 [↑](#footnote-ref-19)
20. Cite…Light Reading 6/19 AT&T sponsored blog [↑](#footnote-ref-20)
21. cite [↑](#footnote-ref-21)
22. Cites for all of these [↑](#footnote-ref-22)
23. cite [↑](#footnote-ref-23)
24. cite [↑](#footnote-ref-24)
25. cite [↑](#footnote-ref-25)
26. cite [↑](#footnote-ref-26)