

July 17, 2017

Ms. Marlene H. Dortch, Secretary  
Federal Communications Commission  
445 Twelfth Street, SW

Washington, DC 20054

*Via Electronic Filing*

In the Matter of	)	
	)	
Restoring Internet Freedom	)	WC Docket No. 17-108

Dear Ms. Dortch,

I<sup>1</sup> offer these comments to aid the Commission in reaching the proper conclusion in construing the nature of Internet Service, determining the regulatory classification of Internet Service (IS) over broadband networks, in creating the regulations that should apply to Internet Service providers (ISP), and in repealing the regulations that should not apply to such services. These comments examine the Internet Model of multi-stakeholder governance, the nature of Internet Service, and the roles of the FCC and Congress in Internet rule-making and enforcement.

---

<sup>1</sup> I am an independent network engineering consultant and policy analyst, presently working at High Tech Forum as editor and founder and as an independent consultant. These remarks are offered in my personal capacity and do not necessarily represent the opinions of any client or sponsor. I have previously offered comments in the “Protecting and Promoting the Open Internet” docket, GN 14-28, the “Preserving the Open Internet” and “Broadband Industry Practices” dockets, GN 09-191 and WC 07-52 respectively, and offered testimony at the [FCC En Banc Public Hearing on Broadband Network Management Practices in Cambridge on February 25, 2008](#) as an invited technical expert. My CV is available at <http://www.bennett.com/resume.pdf>.

## Table of Contents

<b>Summary .....</b>	<b>3</b>
<b>The Internet Model .....</b>	<b>6</b>
<b>The Nature of Internet Service.....</b>	<b>10</b>
Internet Service is an Information Service .....	11
Internet Protocol Packet Transfer is an Information Service .....	12
Managing Internet Bandwidth is an Information Service .....	13
Attack Mitigation is an Information Service .....	15
Domain Name Service is an Information Service .....	16
Routing is an Information Service.....	17
Relationship of Telecommunications and Information Service Elements of Internet Service Provision .....	21
<b>The Classification of Internet Service .....</b>	<b>23</b>
<b>The Regulation of Internet Service.....</b>	<b>27</b>
<b>The Mis-Regulation of Internet Service .....</b>	<b>29</b>
<b>The Measurement of Internet Service Progress .....</b>	<b>32</b>
<b>The Congressional Role .....</b>	<b>35</b>

## Table of Figures

<b>Figure 1: Wireshark capture of DNS transactions occurring before Netflix content is streamed.....</b>	<b>25</b>
<b>Figure 2: Roles in Internet Ecosystem maintenance. ....</b>	<b>27</b>
<b>Figure 3: Year-by-Year Broadband Speed Improvement with Regulatory Events.....</b>	<b>33</b>

## Summary

The Internet is a global system comprised of some 40,000 privately owned and operated networks around the world.<sup>2</sup> The Internet has given rise to a unique system of multi-stakeholder governance known as “The Internet Model”.<sup>3</sup> It is important for national regulators to be mindful of the Internet Model when considering matters of local concern.

Actions by national and regional powers inconsistent the international structure of the Internet risk fragmenting the global Internet into “splinternets” that threaten the overall integrity of the system. A fragmented Internet does not serve United States interests in global commerce and the projection of American democratic values around the world.

In 2015, former Chairman Wheeler made a fundamental error in misconstruing the nature of Internet Service, misclassifying the service under Title II, and issuing bright-line bans on practices that can be beneficial in certain contexts. This arbitrary, top-down, hyper-regulatory action sent a message to other national regulators that it is acceptable to subordinate free expression, global commerce, and democratic values to short-term political concerns.

Perhaps in recognition of the inadequacy of the 2015 Open Internet Order’s bright line rules, the Order compounded its errors by creating a “no unreasonable interference/disadvantage” standard (AKA, “Internet Conduct Standard”) granting itself the authority to impose unpublished regulations in the future should it deem an ISP practice troublesome from the standpoint of consumer freedom or edge provider opportunity.

The 2015 Order asserted “Internet Protocol packet transfer is telecommunications”, following mistaken commenter claims about the nature of Internet Protocol and Internet Service. In reality, Internet Protocol (IP) is more an information format than a means of transmission.

We can’t make sweeping claims about the treatment of a given information format simply on the basis of the format; we need to examine the treatment itself. The 2015 Order failed to conduct such an evaluation.

Internet Service is a combination of transmission and information processing; according to my limited understanding of the law, this means it must be classified as an Information Service in its totality.

While not particularly germane to the argument, there is in fact much more information

---

<sup>2</sup> These remarks are confined to the Internet on the planet Earth. Some go further and describe the Internet as an interplanetary system because of the Mars Rover; see Dino Grandoni, “Is The Mars Rover Using The Internet 182 Million Miles From Earth?,” *Huffington Post*, October 4, 2012, sec. Tech, [http://www.huffingtonpost.com/2012/10/04/mars-rover-internet\\_n\\_1940579.html](http://www.huffingtonpost.com/2012/10/04/mars-rover-internet_n_1940579.html).

<sup>3</sup> Internet Society, “Internet Governance - Why the Multistakeholder Approach Works,” April 26, 2016, <https://www.internetsociety.org/doc/internet-governance-why-multistakeholder-approach-works>.

processing than transmission in this service. It takes a special kind of shortsightedness to characterize the Domain Name Service (DNS) – a vital part of every Internet Service – as an aid to transmission rather than a distinct, high-value Information Service.

In today's Internet, DNS is a tool that allows the providers of edge services to organize their networks, direct users to appropriate devices, and balance processing loads within their networks. While these purposes relate to network management, loosely defined, the managed networks belong to edge service providers.

Edge providers are not customers of ISPs, so the services DNS provides to them cannot be construed as part of a commercial offer to ISP customers. Because the primary function of DNS to ISP customers is the processing, storage, and retrieval of information about domain names – strings of structured text – it cannot be involved in the transmission of information between the customer and points of her choosing on the Internet.

Internet end points are identified with persistent, globally unique IP address, which are binary numbers, either 32 or 128 bits in size. A domain name is not an IP address, and an IP address is not a domain name. In fact, a single domain name may suggest a number of discrete IP addresses and an IP address may suggest a number of (often unrelated) domain names.

The over-arching assumption in the “net neutrality” regulations currently in place is that Internet service as it existed at some point in the past was as good as it can ever possibly be, barring innovation in capacity (or “speed”) and consumer price. Thus, net neutrality seeks to prevent change in all dimensions of the service other than speed and price. This suppression of service evolution is excused by the 2015 order's “virtuous cycle/circle conjecture” (VC/CC).

While VC/CC has emotional appeal, it remains untested, unconfirmed, poorly articulated, and unsupported by either the technical or the economic literature. If the VC/CC is correct, it must surely produce measurable evidence, but there has thus far been no effort to find and disclose any data on the subject.

A rational rule set for broadband Internet service providers must allow service providers to explore opportunities for improvement outside the two permitted dimensions. There are clearly unmet needs in the Internet marketplace: areas with inadequate capability to support modern applications, new applications failing to appear as rapidly as possible, a rate of network upgrade that is slower than it might be, and substantial fear that the Internet is either unsafe to a sizeable population.

Many Americans still feel that the Internet is not worth its cost in terms of dollars, fear, and time. Edge services consolidate at an alarming rate, which suggests there are problems with Internet economics that are not confined to ISPs. Of particular concern at the dawn of the Internet of Things (IoT) and fifth generation mobile networks (5G) is the fact that the Internet still does not provide applications with the Quality of Service

suitable for real-time transactions including but not limited to high-definition voice and video conferencing, telemedicine, and telerobotics.

ISPs need the freedom to address both present and future challenges without looking over their shoulders at 19<sup>th</sup> and 20<sup>th</sup> century norms and regulations. It is arrogant for those of us who contemplate ISP regulation in 2017 to assume that the knowledge we have gathered from 40 years of Internet experience can guide us straight to the proper paradigm for regulating the Internet of 2060.

The regulations that apply to the Internet at the end of this rulemaking need to be testable and measurable. The progress that the Internet has made since its 1970s prototype stage has always been measurable. We know peak and average speeds, latency, packet loss, and transmission load. We can count the number of users, services, and transactions.

We can see migrations onto and off of the Internet, the creation of new services, consolidations, and service terminations. We can tell if more people are doing more things at more places on the Internet, and we can compare the rate of this vector to rates at various points in the past.

The FCC's overall goal should be accelerating the Internet's overall rate of improvement, broadly defined. It should therefore refrain from imposing arbitrary preferences that are not and can never be verifiable. The lesson we've learned best from the past is that the Internet reached its present state in a largely deregulated marketplace. The virtue of deregulation is that it doesn't require regulators to be omniscient beings with special insights about the future.

Restoring the Internet to broad deregulation overseen by a diverse body of stakeholders is the best way to ensure continued progress.

## The Internet Model

The Internet Model of governance is a multi-stakeholder approach adapted to the Internet's unique circumstances. Former NTIA Administrator Lawrence Strickling described the benefits this model has provided to citizens through its application to the Internet:<sup>4</sup>

*Today the world's citizens are benefitting from the growth and innovation of the Internet. The Internet has flourished because of the approach taken from its infancy to resolve technical and policy questions. Known as the multistakeholder process, it involves the full involvement of all stakeholders, consensus-based decision-making and operating in an open, transparent and accountable manner. The multistakeholder model has promoted freedom of expression, both online and off. It has ensured the Internet is a robust, open platform for innovation, investment, economic growth and the creation of wealth throughout the world, including in developing countries.*

More importantly, Strickling touted the superiority of the Internet model over traditional telecom regulation:

*Decentralized control over the Internet involving innovators, entrepreneurs and experts is far preferable to a top-down government approach that has political dealmakers charting the future of the Internet, especially for citizens of countries in the developing world. We need to work together to chart a course beyond Dubai that considers these matters in suitable multistakeholder venues so that discussions are well informed by the voices of all interested parties. Our shared commitment should be to ensure that our respective citizens benefit from the Internet and our USTTI bonds provide a solid foundation for us to chart a path forward together.*

The Internet is a dynamic system, constantly evolving, improving, facing new challenges, enabling new forms of interaction, and extending infrastructure based on new technologies to new users and new areas. Because the facts are constantly changing, the traditional top-down regulatory model is difficult to apply to the Internet.

The top-down model presumes that the regulator makes a finding of fact and applies the pertinent regulation. While this process is straightforward in a milieu of slow change or no change, such as the telephone network space, it has always been difficult to apply to the Internet.

---

<sup>4</sup> Lawrence E. Strickling, "Moving Together Beyond Dubai," *NTIA*, April 2, 2013, <https://www.ntia.doc.gov/blog/2013/moving-together-beyond-dubai>.

The FCC's infamous 2008 Comcast Order illustrates these difficulties.<sup>5</sup> This matter involved a complaint about a network management practice briefly used by Comcast for the purpose of protecting those of its customers using the Vonage VoIP telephone service from call degradation.

The practice lent itself to colorful description. While it consisted of reducing the number of virtual circuits used by P2P file transfer programs BitTorrent and Vuze, the manner of the reduction involved injecting "TCP Reset" packets into the customer data stream. Hence, critics declared Comcast was "impersonating" users.<sup>6</sup>

Other critics claimed Comcast was deliberately degrading P2P in order to protect its MVPD business.<sup>7</sup> But the reality was that Comcast deployed a stopgap system to protect users of VoIP after the order it had placed for upgraded DOCSIS 3 CMTS systems was put on hold by the vendor because of a delay in the development of the DOCSIS 3 standard.<sup>8</sup>

By the time the FCC issued its order, Comcast had discontinued the TCP Reset practice in favor of an application-neutral approach to congestion management known as "Fair Share". The Fair Share system was shared with the Internet Engineering Task Force and published in RFC 6057.<sup>9</sup>

The Fair Share system didn't solve the entire problem that P2P created for VoIP; the problem was actually triggered by "buffer bloat", a widespread issue with router design that was not well understood for many years.<sup>10</sup>

BitTorrent modified its own code to reduce the impact it had on other applications, again sharing the approach with IETF in the LEDBAT RFC.<sup>11</sup> IETF went on to develop an understanding of the problems inherent in controlling queue delay caused by buffer bloat.<sup>12</sup> Modern DOCSIS CMTS systems incorporate Active Queue Management systems

---

<sup>5</sup> Federal Communications Commission, "Memorandum Report and Order in the Matter of Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications et Al.," August 1, 2008, [https://apps.fcc.gov/edocs\\_public/attachmatch/FCC-08-183A1.pdf](https://apps.fcc.gov/edocs_public/attachmatch/FCC-08-183A1.pdf).

<sup>6</sup> Susan P Crawford, "Comcast Is Pretending to Be You," *Susan Crawford*, October 19, 2007, <http://scrawford.net/comcast-is-pretending-to-be-you/>.

<sup>7</sup> Matthew Lasar, "Cable and Telcos Side with Comcast in FCC BitTorrent Dispute," *Ars Technica*, February 19, 2008, <https://arstechnica.com/uncategorized/2008/02/cable-and-telcos-side-with-comcast-in-fcc-bittorrent-dispute/>; Marvin Ammori et al., "Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation For Secretly Degrading Peer-to-Peer Applications" (Federal Communications Commission, November 1, 2007), [https://www.publicknowledge.org/.../fp\\_pk\\_comcast\\_complaint.pdf](https://www.publicknowledge.org/.../fp_pk_comcast_complaint.pdf).

<sup>8</sup> Personal communication with DOCSIS 3 standards developers.

<sup>9</sup> Jim Mills et al., "Comcast's Protocol-Agnostic Congestion Management System," n.d., <https://tools.ietf.org/html/rfc6057>.

<sup>10</sup> Wikipedia, "Bufferbloat," *Wikipedia*, accessed July 15, 2011, <http://en.wikipedia.org/wiki/Bufferbloat>.

<sup>11</sup> Mirja Kuehlewind et al., "Low Extra Delay Background Transport (LEDBAT)," n.d., <https://tools.ietf.org/html/rfc6817>.

<sup>12</sup> Kathleen Nichols and Van Vacobson, "Controlling Queue Delay," *ACM Queue*, May 6, 2012, <http://queue.acm.org/detail.cfm?id=2209336>.

that resolve the buffer bloat problem in an acceptable manner, but the issue demands additional work.<sup>13</sup>

The FCC's action, an order demanding that Comcast discontinue a practice it had already discontinued, was not helpful. The Order was vacated by the courts, but the takeaway for many was to provide the agency with a stronger legal footing for what was essentially a useless, symbolic action.<sup>14</sup> Today, advocacy groups still raise money by complaining about the Comcast-BitTorrent matter.<sup>15</sup>

This is not to say that BitTorrent users didn't have a legitimate beef with Comcast. Some uses of P2P file transfer programs are legitimate, and users should be entitled to run these programs for lawful purposes.

This matter is important because it contrasts FCC enforcement of an Internet user issue with multi-stakeholder action. The FCC's fact-finding fell short because, in fact, no one understood the buffer bloat problem in 2007-8. The FCC's enforcement action did not go to the heart of the problem because the agency didn't know what the problem actually was.

To the extent that buffer bloat, inter-application side-effects, and Internet congestion are understood today, that understanding and the relevant mitigations have come from the multi-stakeholder arena rather than the realm of regulation.

Regulatory actions tend to divide the world into good guys and bad buys, white hats and black hats. But the Internet can only be the functional, reliable, and ever-improving system it is when parties of all stripes cooperate with each other.

Hence, regulatory bodies and governments as a whole can best serve the interests of their citizens by declining to take a superior position in disputes about how best to advance the Internet.

The Title II order took the U. S. and the Internet in the wrong direction. This is apparent from the delayed rate of improvement in Internet performance and continued complaints about the direction in which the Internet is headed.<sup>16</sup>

The FCC's first instinct when it encounters a legitimate issue with Internet management should be to involve the multi-stakeholder community through such means as reaching

---

<sup>13</sup> Greg White, "How DOCSIS 3.1 Reduces Latency with Active Queue Management," *CableLabs*, June 6, 2014, <http://www.cablelabs.com/how-docsis-3-1-reduces-latency-with-active-queue-management/>.

<sup>14</sup> Edward Wyatt, "Court Favors Comcast in F.C.C. 'Net Neutrality' Ruling," *The New York Times*, April 6, 2010, sec. Technology, <https://www.nytimes.com/2010/04/07/technology/07net.html>.

<sup>15</sup> Free Press, "Net Neutrality Violations: A Brief History," *Free Press*, n.d., <https://www.freepress.net/blog/2017/04/25/net-neutrality-violations-brief-history>.

<sup>16</sup> Richard Bennett, "Open Internet Orders Degrade Internet Improvement," *High Tech Forum*, June 19, 2017, <http://hightechforum.org/open-internet-orders-degrade-internet-improvement/>; Nilay Patel, "The Internet Is Fucked (Again) - The Verge," *The Verge*, July 12, 2017, <https://www.theverge.com/2017/7/12/15715030/what-is-net-neutrality-fcc-ajit-pai-bill-rules-repealed>.



out to the Broadband Internet Technical Advisory Group (BITAG), the Internet Engineering Task Force (IETF), the Internet Society, and professional organizations such as ACM and IEEE.

## The Nature of Internet Service

The Title II order follows in the footsteps of the Comcast order by misunderstanding the problem. Internet Service Provider networks are every bit as much a part of the Internet as are the networks operated by Edge Service providers such as Google, Facebook, Amazon, Microsoft, and Netflix.

In fact, every service of every stripe operating in the Internet ecosystem combines transmission and information processing. The apparent goal of the Title II order was simply to divide the Internet between bad guy ISPs and good guy edge providers. But both are businesses with the same balance of incentives for behaviors that are socially valuable and socially destructive.

The purpose of this section is to highlight FCC technical errors in construing ISPs as Title II providers.

For purposes of this analysis, I will stipulate that an element of telecommunications service is embedded at the data link layer<sup>17</sup> of the service the ISP offers to the public. This is the case for both facilities-based ISPs such as Comcast, AT&T, Verizon, et al., and is also the case for unbundled, Over-the-Top (OTT) ISPs such as Sonic.net, a firm that offers ISP service over AT&T's DSL lines in California.

Even when Sonic.net provides Internet Services over AT&T facilities, it uses its own facilities, either leased or owned, to connect DSLAMs in AT&T Central Offices to the Internet Exchanges that reach the Internet as a whole.

It is also the case that there is an element of telecommunications in the provision of MVPD video services because MVPDs transmit information of the user's choosing from one or more network broadcast centers to one or more television sets, DVRs, personal computers, or other devices of the customer's choosing. The user makes the choice about the information he or she will receive when subscribing to a rate plan, makes it again when programming their DVR, and makes it yet again when choosing a recorded program to view.

An MVPD is an MVPD and not a telecommunications service because of the content it delivers and the menu of programs it follows, not by virtue of the fact that the content is transmitted from one place to another. Similarly, an ISP is an Information Service because of the actions it must perform in order to make computers at the customer premise a functional part of the global system we know as the Internet.

The task of an Internet Service Provider is essentially the same regardless of whether it connects to users over dial-up facilities or over broadband: on the Internet-facing side of

---

<sup>17</sup> The data link layer is layer 2 in the Open Systems Interconnection model of network structure. Its scope is the transmission of information from one point in a network to another. It does not carry sufficient information to allow for routing across network boundaries.

the service, it performs the same services in either case. If a dial-up or unbundled ISP is not merely offering a Telecommunications Service, neither is a broadband ISP.

ISPs were classified as “enhanced services” before 1996, and as Title I information services after the Telecommunications Act became law. This was the correct classification because of the nature of Internet Service.

### Internet Service is an Information Service

It’s common to say that ISPs provide “access to the Internet”. The Communications Act does so at §230(e)(2):

*INTERACTIVE COMPUTER SERVICE.--The term "interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.<sup>18</sup>*

“Access to the Internet” has to be understood as shorthand for “joining a customer premise computer to the Internet” because the actual service of the ISP makes the customer’s computer a part of the Internet, just as capable of providing content and services to others as to providing the customer access to content and services hosted by other, co-equal computers on the rest of the Internet. Examples of making content and services available from customer premise equipment include sending email, engaging in chat, operating a web or ftp server, and engaging in peer-to-peer file sharing with BitTorrent. These are routine activities familiar to nearly everyone who uses a connected computer, smartphone, or entertainment device today.

The Internet is effectively a federation of interconnected computers, not simply a bulletin board system like America Online’s (AOL) and CompuServe’s legacy services. There can be no “access to the Internet” when the Internet is fundamentally different from a bulletin board; the mode of interaction Internet users employ is one of membership and participation, not one of access.

In the proceedings of the 2002 TPRC conference, FCC employee and conference chair Robert Cannon provides a concise description of Internet Service:

*The Internet is the Internet all the way to the end. At the end is generally a computer. It is in that computer that the higher layer intelligence (applications, services, and content) exist and is created. The computer uses applications to create content and injects this content as packets into the network, the network itself doesn’t interact with the content. The content is created and processed at the end. Thus **it is inaccurate to say that, for example, an ISP gives an end user access to the Internet, as if the Internet were some far off and remote thing.***

---

<sup>18</sup> “Communications Act of 1934, as Amended by the Telecommunications Act of 1996,” Pub. L. No. 104–104, 110 Stat. 56, § 151 et seq., 47 U. S. C. S 151 et seq. (1996), <http://transition.fcc.gov/Reports/1934new.pdf>.

*Rather, the ISP provisions Internet connectivity. Every device and end user that has Internet connectivity is “on Net” and is a part of the Internet.*<sup>19</sup> [Emphasis added.]

As a matter of fact, at §230(e)(2) the Communications Act states that Internet Service is an Information Service.

### **Internet Protocol Packet Transfer is an Information Service**

Contrary to popular myth, Internet Protocol is part of the Internet’s routing function rather than a transmission function. Internet Protocol is a Network Layer element in terms of the OSI Reference Model, and as such its only concern is with crossing the boundaries between networks. This is not a transmission function, since the means of crossing network boundaries is the simple movement of a packet descriptor from one area of memory within a router (a reception queue attached to the ingress port) to another area of memory (a transmission queue attached to the egress queue).<sup>20</sup>

The transmission and reception functions that characterize transmission are actually accomplished by Ethernet circuitry (or the functional equivalent) because Internet Protocol implementations lack the capability to perform transmission or reception; IP code can only request these services, it cannot perform them.

In other words, Internet Protocol packets are passive content transmitted by network circuitry. To declare Internet Protocol a form of transmission is as false as declaring train tickets to be forms of transportation. The train does the transportation, not the ticket and certainly not the passenger.

The Internet Protocol packet format identifies a desired destination network, but it cannot take any independent action to cause the packet to reach that destination. This is to say that by itself, Internet Protocol is utterly incapable of transmitting information; it is a passive information format that depends on active elements such as Ethernet and the Boundary Gateway Protocol (BGP) for actual transmission.

Internet Protocol exists in two forms today, versions four and six, which use different address formats and different options for requested transmission services. While most traffic transiting the Internet from end to end is enclosed in either the IPv4 or the IPv6 envelope, Internet Protocol is not the only format recognized by ISPs.

ISPs also use Dynamic Host Configuration Protocol (DHCP) to provision IP addresses and to set customer premise configuration options such as Domain Name Server (DNS)

---

<sup>19</sup> Robert Cannon, “Will the Real Internet Please Stand Up? An Attorney’s Quest to Define the Internet,” in *Rethinking Rights and Regulations: Institutional Responses to New Communication Technologies* (Research Conference on Information, Communication, and Internet Policy (30th: 2002), Arlington, VA: MIT Press, 2003), 55–80.

<sup>20</sup> A packet descriptor is an internal information element created and processed by a router to facilitate transmission and/or reception. The end user does not create the packet descriptor, and the descriptor is not preserved after a packet has been processed. Packet descriptors are the means by which layer 2 and 3 functions communicate with each other.

addresses and Classless Inter-Domain Routing (CIDR) parameters. Given that DHCP makes it possible for IP to function, it's difficult to accept arguments that IP is the elemental service provided by ISPs. In fact, IP packet transfer is one in a bundle of many information services provided by ISPs.

The declaration that Internet Service is nothing more or less than packet transmission is "cherry picking" that suppresses evidence of the many related functions that ISPs provide.<sup>21</sup> IP packets move from source to destination over a multiplicity of Data Link Layer paths provided by many ISPs, including the originating ISP, the destination ISP, and some number (zero or more) of intermediary ISPs (AKA "transit providers").

But even if we accept the argument that IP packet transfer is the elementary ISP service, it still does not follow that Internet Service is telecommunication; this is because IP packet transfer depends on routing, Ethernet services, third party networks, and agreements between and among deregulated network operators for the processing of information packets according to freely negotiated Service Level Agreements.

In addition to these dependencies, users and "edge services" affect the quality of end-to-end Internet Service, as we've seen in the slowdowns recently inflicted on the general population of Internet users by Netflix and Cogent.<sup>22</sup> Singling out one link in this chain for special regulatory treatment while leaving the others deregulated would be arbitrary.

### Managing Internet Bandwidth is an Information Service

As a member of the Internet, customer premise equipment is obligated to behave in a manner consistent with Internet norms, and is required to protect itself from dangerous activities performed by other members. One example of conforming to Internet norms is the TCP Congestion Control system governed by "Jacobson's Algorithm".<sup>23</sup> The Internet lacks a built-in mechanism for protecting itself from overload.

This is not by design; Internet protocol designers included a mechanism known as "Source Quench" in the original specification of the Internet Control Message Protocol that was meant to provide overload protection, but it didn't work (see: RFC 777).<sup>24</sup> The Source Quench mechanism wasn't tested until Ethernet bypassed ARPANet in the mid-1980s and the Internet suffered Congestion Collapse.<sup>25</sup>

---

<sup>21</sup> A similar claim was made in the Comcast/BitTorrent case by advocates who insisted that blocking a single TCP connection was the same as blocking an entire BitTorrent transaction. These advocates glossed over the fact that BitTorrent transactions use dozens of TCP connections, no one of which is essential the entire transaction. Blocking some but not all TCP connections in a transaction simply slows the transaction down but does not cause it fail.

<sup>22</sup> Dan Rayburn, "Cogent Now Admits They Slowed Down Netflix's Traffic, Creating A Fast Lane & Slow Lane," *StreamingMediaBlog.Com*, November 5, 2014, <http://blog.streamingmedia.com/2014/11/cogent-now-admits-slowed-netflixs-traffic-creating-fast-lane-slow-lane.html>.

<sup>23</sup> Van Jacobson, "Congestion Avoidance and Control," *Computer Communication Review*, ACM Special Interest Group on Data Communication, 25, no. 1 (1995): 157.

<sup>24</sup> J Postel, "RFC 777 - Internet Control Message Protocol" (Network Working Group, April 1981), 777, <https://tools.ietf.org/html/rfc777>.

<sup>25</sup> W. Stevens, "TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms" (Network Working Group, January 1997), <http://tools.ietf.org/pdf/rfc2001.pdf>.

Jacobson's Algorithm requires Internet members – known as “hosts” – to reduce their rate of transmission when signaled by an Internet router that congestion is growing to dangerous levels. The router discarding a packet typically provides this signal, but altering a bit in the Internet Protocol header can also provide it; this latter method is known as “Explicit Congestion Notification” (ECN).<sup>26</sup> While hosts that do not conform to Jacobson's Algorithm are not kicked off the Internet, its successful operation depends on broad conformance because normal Internet operation involves hosts cycling between underload and near overload.

Hosts are owned and maintained by end users, and routers are owned and maintained by ISPs and by end users; residential-focused, business-focused, and transit-focused ISPs all participate in this system, but they don't necessarily signal congestion at by the same means or at the same time. The use of packet discard as congestion signal is obviously ambiguous, because packet discard also takes place for other reasons: when wireless packets collide, they tend to be dropped by the receiving host because their addressing information can't be trusted.

Routers also implement a number of different sub-algorithms of the Jacobson master scheme, such as Random Early Detection, Weighted Random Early Detection, Adaptive Random Early Detection, and Robust Random Early Detection.<sup>27</sup> The choice and execution of these algorithms is an example of close interaction between customer premise equipment and ISPs, not only those that directly serve the end user but also those connected directly to the customer's ISP or to other ISPs connected to the end user's ISP.

Implementing Jacobson's Algorithm requires extensive information processing in the customer's hosts and routers as well as in the ISP's routers, in part to distinguish packet loss due to congestion from that caused by other factors, and in part to select and implement the most effective congestion control mechanism. We are not at the final stage of Internet congestion avoidance and management, of course. Not only is the technical literature replete with research in this area, such policy works as *A “Third Way” on Net Neutrality* address this matter as well.<sup>28</sup>

Bandwidth management is essential to Internet Service because packet-switching systems allocate bandwidth on demand and apportion it among concurrent users dynamically. This differs from the way telecommunication networks operate; when telephone users take part in calls, the telephone network allocates a fixed quantum of bandwidth to callers, limited to a few kilohertz, and this allocation lasts for the duration of the call whether it is used or not. But when Internet users access a web server, the ISP allocates bandwidth dynamically.

---

<sup>26</sup> K. Ramakrishnan, S. Floyd, and D. Black, “RFC 3168 - The Addition of Explicit Congestion Notification (ECN) to IP” (Internet RFC, September 2001), <http://tools.ietf.org/rfc/rfc3168.txt>.

<sup>27</sup> Wikipedia, “Random Early Detection,” accessed December 23, 2014, [http://en.wikipedia.org/wiki/Random\\_early\\_detection](http://en.wikipedia.org/wiki/Random_early_detection).

<sup>28</sup> Robert D. Atkinson and Philip J. Weiser, “ITIF: A ‘Third Way’ on Network Neutrality,” report (Washington, DC: Information Technology and Innovation Foundation, May 30, 2006), <http://www.itif.org/index.php?id=63>.

If only one user is active on a given path or segment at a time, that user is able to use the entire capacity of that path, but if many users are active, each contends with the others for capacity and the ultimate assignment is a function of patterns of user demand, location of end points, upstream congestion, server capacity, and a host of other factors. At each point in the path between the ISP's customer and the Internet-based service that user accesses, decisions are made regarding the treatment of each packet.

This isn't simply "the management of a telecommunications service" as some may argue. The management of a telecommunications service is a set of actions that ensure the service conforms to a predetermined level of quality, but dynamic bandwidth management in a packet switched network is a real-time negotiation of service parameters.

When network load is light, users enjoy a better quality experience than they enjoy when load is heavy. On a telecommunication network the user's experience is the same whether the network is lightly or heavily loaded. An overloaded packet switched network continues to function, but does so slowly, while an overloaded telecommunications network simply refuses to connect new calls.

Consequently, Internet service is a dynamic service made available on a statistical basis and provided by a system that relies on information processing, while telecommunication is static service that can be provided on an analog network where human operators plug wires into panels to make connections, as it was for many years. It would not be possible to provide packet switching in the same manner as it relies on millisecond-by-millisecond dynamic decisions made dozens of times in the transmission of each information packet.

### **Attack Mitigation is an Information Service**

Billions of people use the Internet through their own computers worldwide, and (unsurprisingly) some are up to no good. The Commission is aware that criminals use the Internet for the theft of intellectual property, identity theft, and extortion. This is no trivial matter as the connectionless nature of Internet Protocol makes it an ideal vehicle for Denial of Service attacks, and the insecure nature of basic Domain Name Service allows criminals to use DNS and Simple Network Management Protocol (SNMP) as amplifiers for attacks. Distributed DoS attacks are made possible by viruses that enable botnet operators to invade and take over end-user systems in order to enlist them into their botnets, where they can be used to send spam and to take part in DDoS attacks.

There is no parallel to a DDoS attack using amplification to bring a web site to its knees in the realm of plain old telephone service.

Mitigating these attacks requires ISPs to engage a multi-pronged strategy, using information technology to distribute anti-virus software to end user computers, to monitor networks for suspicious traffic and attacks, to block (or redirect) attack traffic when it is found, and to notify other ISPs of infected computers on the other ISP network so that end users can take appropriate action.



Attack mitigation is not simply a management function performed to make networks operate; it's an added-value service that is necessary to reduce the incidence of unlawful activity across the Internet.

The most obvious and well-known element of attack mitigation is the anti-virus software that ISPs make available to their customers, typically free of charge. Anti-virus software is an intensive use of information processing to search for viruses in downloads and incoming email, to monitor the integrity of system files, and to distribute attack knowledge to software producers so that they can fix bugs that allow viruses entry where they are not wanted. Internet Service without security would be a meaningless and dangerous offering.

### Domain Name Service is an Information Service

Internet Service always includes Domain Name Service provided over “the largest distributed database in the world”.<sup>29</sup> DNS is an increasingly sophisticated distributed function that translates domain names into IP addresses, its best-known function, but it does much more. DNS implements the DNSSEC protocol, an authentication service that validates the correctness of the domain name to IP address mapping and protects users from man in the middle (MITM) attacks. DNS is also a traffic direction service that connects Content Delivery Network users to the nearest and/or fastest location. DNS also provides a reverse mapping from IP addresses to domain names, and distinguishes authoritative domains from other domain names that may share an IP address.

DNS manages aliased domain names – another case of multiple domain names sharing a common IP address – and provides both IPv4 and IPv6 addresses. DNS distinguishes multiple services within a domain, such as the email “Mail Exchanger” and the web service. The database managed by a DNS server is updated in real time, with updates shared across the entire Internet as needed. DNS servers protect themselves from attacks, since a simple, unprotected DNS server is an attack vector that can amplify DDoS attacks in much the same way an unprotected SNMP agent can.<sup>30</sup>

It must be acknowledged that the largest distributed database in the world is an information service, or nothing is. It must also be acknowledged that DNS is an indispensable part of the Internet Service provided by ISPs.

With the advent of DNSSEC, the DNS service provided by ISPs today is much more information-processing intensive than was the DNS service provided by ISPs when the FCC classified cable modem Internet service as an Information Service. Consequently, the logic that guided the Commission's previous classification decision is even stronger today than it was in 1992. DNSSEC processes much more information than simple DNS did, and for a very good reason: information security. As VeriSign describes it, DNSSEC

---

<sup>29</sup> Fred Donovan, “DNS Infrastructure Is ‘Highly Vulnerable’ to Attacks, Warns Infonetics,” news blog, *Fierce IT Security*, (November 14, 2014), <http://www.fierceitsecurity.com/story/dns-infrastructure-highly-vulnerable-attacks-warns-infonetics/2014-11-13>.

<sup>30</sup> Broadband Internet Technical Advisory Group, “SNMP Reflected Amplification DDoS Attack Mitigation” (Broadband Internet Technical Advisory Group, August 2012), <http://www.bitag.org/documents/SNMP-Reflected-Amplification-DDoS-Attack-Mitigation.pdf>.



is essential for the protection of DNS information from attacks, and DNS itself is essential to the operation of the Internet:

*The Domain Name System (DNS), the Internet's addressing system, is the most critical component of the Internet infrastructure. **Without it, the Internet could not function.***

*However, it was not designed with security in mind. As a result, it is vulnerable to man-in-the-middle (MITM) attacks and cache poisoning. These threats use forged data to redirect Internet traffic to fraudulent sites and unintended addresses.*

*Once an unsuspecting user or device reaches the fraudulent site, cyber criminals can potentially extract credit card data, steal user passwords, eavesdrop on voice over IP (VoIP) communications, plant malicious software or display images and text that defame the legitimate brand or provide misleading information. Given that a single DNS name server can act as the name-to-address resolution point for thousands of users, the potential impact of a MITM attack or cache poisoning can be considerable.<sup>31</sup> [Emphasis added.]*

DNSSEC is information processing, and without it all commercial transactions over the Internet are suspect.

### Routing is an Information Service

Routing is an indispensable element of any packet-switched network such as the Internet. In its most elementary form, the routing function determines whether packets of information received by a router are to be dropped, forwarded, or processed.

A packet is dropped if it comes from an unauthorized source, or if the forwarding path is congested or unavailable. A packet is forwarded if its network identifier matches a known valid route and resources are available for forwarding. Packets are processed if they contain management information such as routing map updates or network management commands.

In commercial settings, all packets potentially have implications for accounting, security, and public safety, so routers also provide these functions. Network Quality of Service is provided and ensured by routers, and these functions are present in routers in a number of different forms.

While the telephone network determines a path from the calling to the called party when calls are setup, it simply records a circuit identifier at call establishment time, which is used by all subsequent elements of the call. Packet switching routers, on the other hand, recalculate the route from source to destination every time a packet is forwarded, a much more intensive information-processing task. Packet routers also react to network failures by choosing alternate routes while a packet is in flight, sometimes reacting to network

---

<sup>31</sup> Verisign, "DNSSEC Test and DNSSEC Testing," corporate blog, *Verisign*, accessed December 29, 2014, [http://www.verisigninc.com/en\\_US/innovation/dnssec/dnssec-test/index.xhtml](http://www.verisigninc.com/en_US/innovation/dnssec/dnssec-test/index.xhtml).

failures in small fractions of a second. Consequently, packet routers perform several orders of magnitude more computation than telephones switches do.

It is useful to compare the functions performed by common web servers with those performed by Internet routers. There is no dispute that web services are Information Services, so it follows that ISP services performed over routers must be information services as well if the two are essentially similar or if routers are more information service intensive. The following chart examines the functions of web servers and routers according to the definition of Information Service in the Communications Act, the offering of a capability for “generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications”.<sup>32</sup> Each term in this definition is presented as an “Information System Property”.

Information System property	Web server	Internet router
Generating information	<ul style="list-style-type: none"> <li>• Creates dynamic web pages with personalized content and real-time content such as Twitter streams, ads, and news streams.</li> </ul>	<ul style="list-style-type: none"> <li>• Creates updates to routing table;</li> <li>• Resolves DNS queries;</li> <li>• Forwards information packets;</li> <li>• Signals operational options such as Quality of Service parameters;</li> <li>• Generates error messages in ICMP terms;</li> <li>• Signals congestion to end point by dropping packets;</li> <li>• Gathers network health; and</li> <li>• Responds to network management queries.</li> </ul>
Acquiring information	<ul style="list-style-type: none"> <li>• Obtains information about the user, browser, platform, end point location and advertisements</li> </ul>	<ul style="list-style-type: none"> <li>• Receives packets, routing updates, Quality of Service parameters, end-point location, and load balancing information.</li> </ul>
Storing information	<ul style="list-style-type: none"> <li>• Stores software and software updates, web page elements, user IDs and passwords, comments, and log file elements.</li> </ul>	<ul style="list-style-type: none"> <li>• Stores packets in queues;</li> <li>• Stores software and software updates, next-hop routing information, user IDs and passwords, configuration parameters and log files.</li> </ul>

<sup>32</sup> *Communications Act of 1934, as amended by the Telecommunications Act of 1996.*

Transforming information	<ul style="list-style-type: none"> <li>• Redirects web queries to alternate URIs and URLs and modifies web query content.</li> </ul>	<ul style="list-style-type: none"> <li>• Transforms MAC addresses from original from/to pair to new pair for next hop;</li> <li>• Decrements TTL;</li> <li>• Modifies Class of Service indicators.</li> </ul>
Processing information	<ul style="list-style-type: none"> <li>• Chooses from multiple representations of web pages, images, audio/video streams, and page formats according to user's browser version;</li> <li>• Compresses and decompresses streams;</li> <li>• Examines user cache to determine when to retransmit images; and</li> <li>• Interacts with local caches.</li> </ul>	<p>For each packet transferred:</p> <ul style="list-style-type: none"> <li>• Looks up next hop by prefix or by port;</li> <li>• Determines success or failure of transfers and adjusts best route according to network conditions;</li> <li>• Chooses priority queue by SLA contract and packet preferences;</li> <li>• Discards packets according to various congestion algorithms for long queues;</li> <li>• Re-orders queues as needed;</li> <li>• Determines packet priority by deep packet inspection if necessary;</li> <li>• Determines whether inbound and outbound packets are parts of attacks;</li> <li>• Processes Access Control Lists for forwarding, discards, and other purposes.</li> </ul> <p>On a longer-term basis:</p> <ul style="list-style-type: none"> <li>• Updates routing tables in response to a variety of conditions in the forwarding path, changes in contracts, and attack/malware mitigations.</li> </ul>
Retrieving information	<ul style="list-style-type: none"> <li>• Fetches web pages and page elements from local or network storage, gathers cache information from end user system and end user's</li> </ul>	<ul style="list-style-type: none"> <li>• Fetches routes from neighbors and network-wide functions;</li> <li>• Gathers information from network interfaces;</li> </ul>

	local cache; • Obtains ads for web pages; • Gathers dynamic streams from various network and local sources.	• Receives software updates; • Stays abreast of network conditions on alternate routes; • Obtains DNS updates from more authoritative sources; and • Obtains network management information from other routers.
Utilizing information	• Uses user identity, location, and preferences to authenticate access to protected content, perform financial transactions, sell advertisements, localize services, and obtain desired content as directed by links.	• Utilizes destination address to determine best route; • Utilizes destination network address to determine best route; • Utilizes port-relative network prefixes to determine best route; • Aggregates packet streams in LISP; • Utilizes SLA terms to determine port-based packet queue ordering; • Utilizes stream profiles to identify attacks;
Making information available	• Makes wide variety of information available in a number of forms, as this is the primary function of web server.	• As parts of distributed databases of domain name and routing information, makes a wide variety of location, identity, service level and routing information available across the Internet.

In terms of overall processing power, the contemporary router is several times more powerful than the typical web server. This processing power comes at a price, as the typical router is also several times more expensive than the typical web server. Router users would not be willing to pay this price if end users did not require the router's information service elements.

Routing service is more information processing intensive today than it was in 1992: there are many more routes, there are two types of IP address formats in use, and ISPs support new protocols such as LISP that attempt to deal with the explosion in the size of the

routing table.<sup>33</sup> Routing is also becoming more secure now, thanks to pending upgrades in BGP, the Internet's basic routing information exchange protocol in the interest of security.<sup>34</sup> BGP also has means for exchanging Quality of Service parameters that did not exist until some ten years ago.<sup>35</sup>

Routing is more information-rich than it has ever been.

### Relationship of Telecommunications and Information Service Elements of Internet Service Provision

The OSI Reference Model and similar constructs describe a modular distribution of functions in a network.<sup>36</sup> Layers in these models describe similar functions performed at different scopes. All network layers transmit and receive information, whether they be telecommunications devices, Internet routers, or web servers and browsers, but they do so over paths that differ mainly by distance.

Within the Internet, the telecommunication function consists of a set of circuits connecting one unique end point to another, such as an Ethernet cable connecting a personal computer to an Ethernet switch or an (optical) Ethernet cable from a router to an Ethernet switch. Ethernet is an un-routed service, similar to Wi-Fi, DOCSIS, DSL, or Passive Optical Networking (xPON). For simplicity, I use "Ethernet" as a proxy for any and all of these systems.

Ethernet packets carry a payload consisting of IPv4 or IPv6 data elements and their respective payload (which consists of TCP, HTTP, and similar application-oriented protocols.) The Ethernet frame carries very limited information and is not routable as the addresses Ethernet processes are local to the switch.

IPv4 and IPv6 information packets are co-mingled over Ethernet circuits and contain addresses that are unique across the entire Internet. While an Ethernet switch can interconnect dozens of computers, a router connects any computer to any other computer anywhere in the world. The means of interconnecting the dozen or so devices in a home, office, or neighborhood to each other is telecommunication, and the means of interconnecting any computer to any other computer is an information service.

The telecommunications scope is perhaps as many as a few hundred machines in a closely controlled network, while the information service scope is billions of machines attached over hundreds of millions of telecommunications connections in a loosely

---

<sup>33</sup> D Farinacci et al., "RFC 6830 - The Locator/ID Separation Protocol (LISP)" (RFC Editor, January 2013), <http://tools.ietf.org/html/rfc6830>.

<sup>34</sup> S Bellovin, "Security Requirements for BGP Path Validation" (RFC Editor, August 2014), <http://www.rfc-editor.org/rfc/rfc7353.txt>.

<sup>35</sup> Cisco, "Using BGP Community Values to Control Routing Policy in Upstream Provider Network," corporate site, (August 10, 2005), <http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/28784-bgp-community.html>.

<sup>36</sup> Hubert Zimmerman, "OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection," *IEEE Transactions on Communications* Com-28, no. 4 (April 1980): 425-32.

coordinated, unpredictable mesh in of both good and bad actors, heavy and light users, sophisticated customers and naïve amateurs with wildly different needs and desires.

The manager of a telecommunications network can over-provision the network under his or her control to ensure it never stalls or congests and never provides service to bad actors, but the manager of an Internet service can never have that much control. Routing is a fundamentally different activity from switching, and maintaining the Domain Name Service is fundamentally different from creating a table of computer name to IP address mappings with a text editor (as can be done in Windows, OS X, or Linux).

## The Classification of Internet Service

The proper classification of Internet Service under the Communications Act requires the regulator to determine whether the functions performed by the ISP are more or less similar to those performed by the millions of American consumers with Ethernet switches in their homes and offices than to those performed by web site owners in terms of the extent of their information processing intensity. The law indicates that Information Service is performed over a telecommunications facility, and that it does more information processing than the telecommunications facility does (even in the interest of its internal management).

The descriptions I have provided of congestion management, attack mitigation, domain name service and IP routing show that Internet Service is more than telecommunication. Consumers are more than capable of providing their own “telecommunication” services today with inexpensive hardware that can be bought in retail stores, just as pizza deliverers can provide delivery services with common bicycles and automobiles.

Internet service is, however, a specialized information technology-enabled service that can only be provided by highly skilled operators with a deep pool of talent and a serious investment in equipment, training, and infrastructure. It makes no more sense to classify Internet Service as simple telecommunication than it would to classify integrated circuit design and production as telecommunication simply because some chips are used in telephone networks. These are two vastly different realms, and to confuse them in a way that does injustice to the nature of Internet Service was a clear technical error.

I urge the Commission to change the regulatory classification of Internet Service from Title II to Title I. The FCC is meant to be an independent, expert agency that interprets the law and applies it to technical realities, and those realities are abundantly clear: Internet Service is an Information Service as defined by the Communications Act.

The Communications Act defines “information service” as “the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing, but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service.”

This definition applies to Internet Service because it emphasizes information processing in the essential nature of the service and not merely as a means of managing the service. If we take information processing out of Internet Service, nothing is left but the wired or wireless medium over which information flows and the Data Link Layer (layer two of the Open Systems Interconnection Reference Model) service that actually transmits and receives information frames hop-by-hop in the overall path from client to server or peer

to peer through the internals of the Internet.<sup>37</sup>

The Act defines “telecommunications” as “the transmission, between or among points specified by the user, of information of the user’s choosing, without change in the form or content of the information as sent and received” and “telecommunications service” as “the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used.”

This definition clearly calls out telephony, the only information exchange that promises to send and receive information between end points without alteration of the information’s form or content. This definition is also applicable to the Data Link Layer of the network protocol stack; but it is not applicable at the Network Layer (layer three, where Internet Protocol resides) because layer two addresses are changed hop-by-hop as Network Layer packets transit the Internet, and for other reasons given below.

While telephony is an interaction between persons using telephone handsets that are essential elements of the telephone network, information service is an interaction between computers that involves continual interaction between computers and the transmission network as well as between computers and each other. In an Information Service, the human user – if there is one, which is not the case for Internet of Things applications – interacts with the computer, and the computer mediates this interaction with the network and the paired computer or computers. This is an entirely different and more complex information system than telephony is.

The Communications Act stresses “transmission, between or among points specified by the user”. Internet end points are specified by IPv4 and IPv6 addresses, but Internet users do not know the IP addresses with which they communicate.

Internet users communicate with resources rather than end points. These resources are identified by Uniform Resource Identifiers (URI), Uniform Resource Locators (URL), or Uniform Resource Names (URN).<sup>38</sup> Before particular transmissions to specific end points take place, these URIs are mapped onto IP addresses through application logic enabled by interaction with the DNS database.

The logic that maps URIs to IP addresses is quite complex and is not managed by either the ISP or the ISP’s customer. Rather, it is managed by the owner of the information resource identified by the URI. When a Netflix customer plays a movie or television program, a lengthy series of interactions takes place. I have captured one typical sequence using the Wireshark network monitor tool.

This sequence demonstrates that Internet communication is not simply a transmission *between or among points* specified by the user.

---

<sup>37</sup> Ibid.

<sup>38</sup> Larry Masinter, Tim Berners-Lee, and Roy T. Fielding, “Uniform Resource Identifier (URI): Generic Syntax” (Internet RFC, January 2005), <https://tools.ietf.org/html/rfc3986>.



```

DNS      98 Standard query 0x22dc A assets.nflxext.com
DNS      98 Standard query 0x0ca2 AAAA assets.nflxext.com
DNS      189 Standard query response 0x22dc A assets.nflxext.com CNAME sha2.san.akam.nflximg.net CNAME e3067
DNS      229 Standard query response 0x0ca2 AAAA assets.nflxext.com CNAME sha2.san.akam.nflximg.net CNAME e
DNS      97 Standard query 0x3ef1 A art-s.nflximg.net
DNS      97 Standard query 0xa15b AAAA art-s.nflximg.net
DNS      106 Standard query 0x3810 A customerevents.netflix.com
DNS      106 Standard query 0xe220 AAAA customerevents.netflix.com
DNS      177 Standard query response 0x3ef1 A art-s.nflximg.net CNAME sha2.san.akam.nflximg.net CNAME e3067
DNS      245 Standard query response 0xa15b AAAA art-s.nflximg.net CNAME sha2.san.akam.nflximg.net CNAME e3
DNS      313 Standard query response 0x3810 A customerevents.netflix.com CNAME customerevents.geo.netflix.c
DNS      409 Standard query response 0xe220 AAAA customerevents.netflix.com CNAME customerevents.geo.netfli
DNS      122 Standard query 0xf557 A ipv6_1-cx10-c021.1.den001.ix.nflxvideo.net
DNS      122 Standard query 0x24f2 AAAA ipv6_1-cx10-c021.1.den001.ix.nflxvideo.net
DNS      138 Standard query response 0xf557 A ipv6_1-cx10-c021.1.den001.ix.nflxvideo.net A 23.246.10.150
DNS      150 Standard query response 0x24f2 AAAA ipv6_1-cx10-c021.1.den001.ix.nflxvideo.net AAAA 2a00:86c0:
DNS      123 Standard query 0x7156 A ipv6_1-lagg0-c029.1.den001.ix.nflxvideo.net
DNS      123 Standard query 0x5687 AAAA ipv6_1-lagg0-c029.1.den001.ix.nflxvideo.net
DNS      122 Standard query 0x01c4 A ipv6_1-cx10-c024.1.den001.ix.nflxvideo.net
DNS      122 Standard query 0xd96c AAAA ipv6_1-cx10-c024.1.den001.ix.nflxvideo.net
DNS      138 Standard query response 0x01c4 A ipv6_1-cx10-c024.1.den001.ix.nflxvideo.net A 23.246.10.153
DNS      139 Standard query response 0x7156 A ipv6_1-lagg0-c029.1.den001.ix.nflxvideo.net A 23.246.11.133
DNS      151 Standard query response 0x5687 AAAA ipv6_1-lagg0-c029.1.den001.ix.nflxvideo.net AAAA 2a00:86c0:
DNS      150 Standard query response 0xd96c AAAA ipv6_1-cx10-c024.1.den001.ix.nflxvideo.net AAAA 2a00:86c0:
DNS      96 Standard query 0xcf30 A tp-s.nflximg.net
DNS      96 Standard query 0x436c AAAA tp-s.nflximg.net
DNS      244 Standard query response 0x436c AAAA tp-s.nflximg.net CNAME sha2.san.akam.nflximg.net CNAME e3067
DNS      176 Standard query response 0xcf30 A tp-s.nflximg.net CNAME sha2.san.akam.nflximg.net CNAME e3067
DNS      122 Standard query 0x3f49 A ipv6_1-cx10-c020.1.den001.ix.nflxvideo.net
DNS      122 Standard query 0xf80f AAAA ipv6_1-cx10-c020.1.den001.ix.nflxvideo.net
DNS      138 Standard query response 0x3f49 A ipv6_1-cx10-c020.1.den001.ix.nflxvideo.net A 23.246.10.149
DNS      150 Standard query response 0xf80f AAAA ipv6_1-cx10-c020.1.den001.ix.nflxvideo.net AAAA 2a00:86c0:
DNS      122 Standard query 0x84bd A ipv6_1-cx10-c023.1.den001.ix.nflxvideo.net
DNS      122 Standard query 0xcb9d AAAA ipv6_1-cx10-c023.1.den001.ix.nflxvideo.net
DNS      138 Standard query response 0x84bd A ipv6_1-cx10-c023.1.den001.ix.nflxvideo.net A 23.246.10.152
DNS      150 Standard query response 0xcb9d AAAA ipv6_1-cx10-c023.1.den001.ix.nflxvideo.net AAAA 2a00:86c0:
DNS      122 Standard query 0x9bb1 A ipv6_1-cx10-c022.1.den001.ix.nflxvideo.net
DNS      122 Standard query 0xe262 AAAA ipv6_1-cx10-c022.1.den001.ix.nflxvideo.net
DNS      138 Standard query response 0x9bb1 A ipv6_1-cx10-c022.1.den001.ix.nflxvideo.net A 23.246.10.151
DNS      150 Standard query response 0xe262 AAAA ipv6_1-cx10-c022.1.den001.ix.nflxvideo.net AAAA 2a00:86c0:
DNS      122 Standard query 0x29d3 A ipv6_1-cx10-c015.1.den001.ix.nflxvideo.net
DNS      122 Standard query 0xa244 AAAA ipv6_1-cx10-c015.1.den001.ix.nflxvideo.net
DNS      138 Standard query response 0x29d3 A ipv6_1-cx10-c015.1.den001.ix.nflxvideo.net A 23.246.10.144
DNS      150 Standard query response 0xa244 AAAA ipv6_1-cx10-c015.1.den001.ix.nflxvideo.net AAAA 2a00:86c0:
DNS      122 Standard query 0x62b1 A ipv6_1-cx10-c014.1.den001.ix.nflxvideo.net
DNS      122 Standard query 0x8451 AAAA ipv6_1-cx10-c014.1.den001.ix.nflxvideo.net
DNS      138 Standard query response 0x62b1 A ipv6_1-cx10-c014.1.den001.ix.nflxvideo.net A 23.246.10.143
DNS      150 Standard query response 0x8451 AAAA ipv6_1-cx10-c014.1.den001.ix.nflxvideo.net AAAA 2a00:86c0:

```

Figure 1: Wireshark capture of DNS transactions occurring before Netflix content is streamed.

The user requests a program by name from Netflix. Netflix scans its network for the content encoded in a format that it determines best for the user's device, the state of the ISP's network, and the state of the information resources in the Netflix network.

The end user does not specify the end point IP address within the Netflix cloud with which he or she communicates. Netflix makes this choice itself. In this case, the content was transmitted by a server in the "nflxvideo.net" domain, a domain that is probably altogether unknown to the user.

Not only does the user not specify the communication endpoint by IP address, he or she does not even specify it by name. The location of the information resource is entirely hidden from the user. In fact, the information resource exists in multiple formats and locations within the Netflix cloud.

Netflix chooses the endpoints using the DNS provided by the ISP. The matter is not in the hands of the ISP or the ISP's customer. Consequently, this routine information exchange is part of an information service, not a transmission service.

Using the Internet is a matter of interacting with information resources without little or no knowledge or concern for location. Hence, there is more to Internet service than users directing transmissions to points of their choosing.

## The Regulation of Internet Service

Within the Internet Model, governments play important roles in policy development, capacity building, and education, but the primary role played by the FCC in recent years has focused on policy enforcement. In the U. S., the FCC splits Internet policy enforcement duties with other agencies, such as the Federal Trade Commission, the Department of Justice, and state and local governments.

Fig.1 The Internet's governance arrangements are an ecosystem

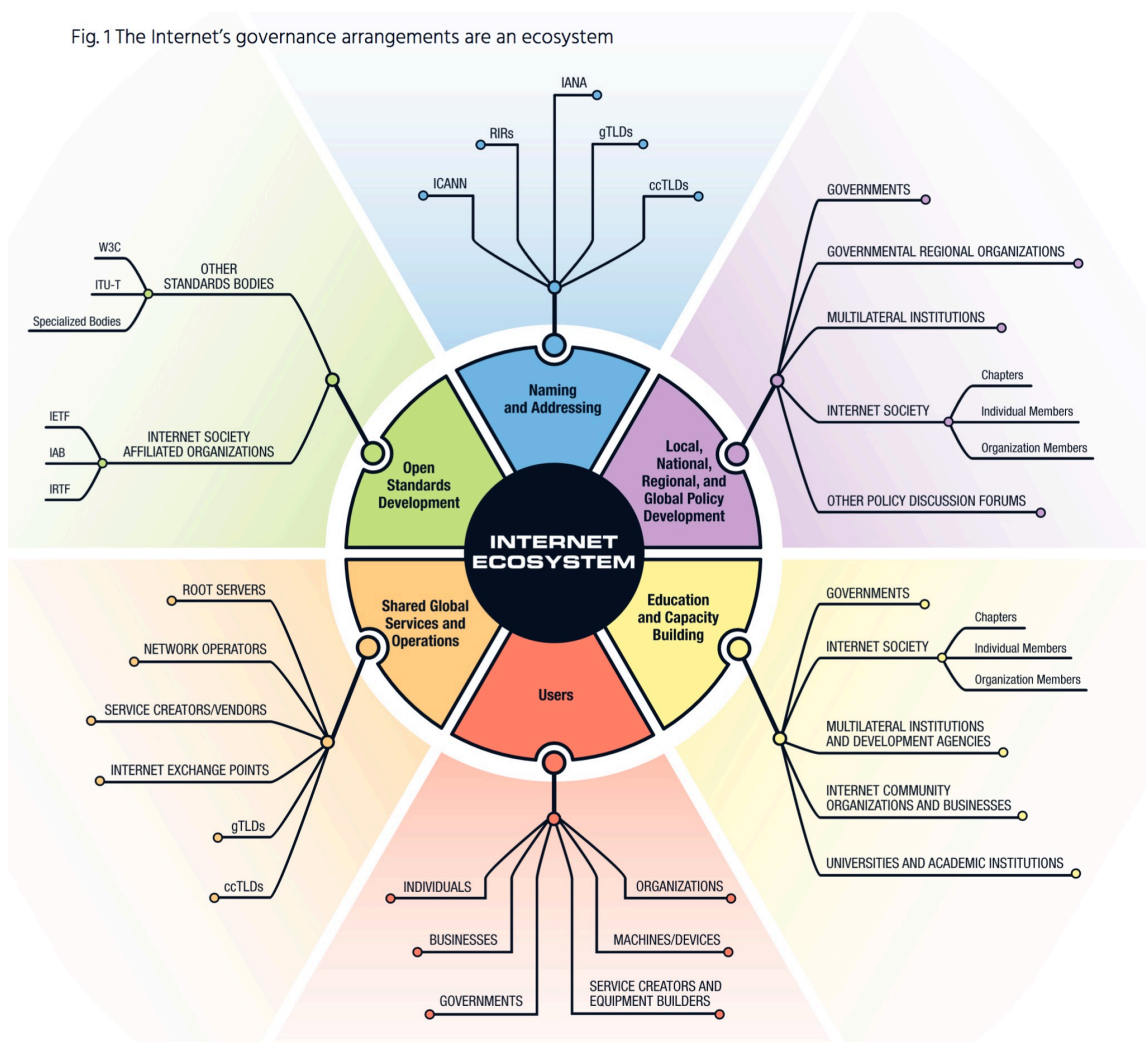


Figure 2: Roles in Internet Ecosystem maintenance.<sup>39</sup>

The health and development of the Internet is best ensured when national regulators emphasize development. This can obviously include sanctions against players whose actions impair growth and development.

It can be difficult for enforcement agencies to determine whether particular practices are harmful to the Internet, just as it can be difficult for the IETF to determine, for example,

<sup>39</sup> Internet Society, "Internet Governance - Why the Multistakeholder Approach Works."

that a given Internet protocol needs to be upgraded or for IANA to determine that a particular global resources needs to be assigned for the exclusive use of one application.

Once Tim Berners-Lee had invented the World-Wide Web in Switzerland, he petitioned IANA to assign TCP port 80 for the exclusive use of his application. IANA granted this permission to the web. We can see now that IANA was wise to give Sir Tim the permission to use port 80 as his application has become very popular, but other exclusive assignments have not panned out quite as well: the assignment of port 126 to the Unisys Unitary Login is less valuable.

The general approach to Internet regulation urged on the Commission by net neutrality advocates is sound in principle even if difficult in practice. On its face, net neutrality is meant to be the foundation for a regulatory regime reflecting certain enduring principles of Internet design and operation.

## The Mis-Regulation of Internet Service

The arguments for net neutrality developed by law professor Lawrence Lessig and his protégés Tim Wu and Barbara van Schewick assert that neutrality is a long-standing principle of Internet architecture.<sup>40</sup> Wu's seminal paper argues that net neutrality is a theory of innovation embedded in the design of the Internet itself:

*For these reasons, Internet Darwinians argue that their innovation theory is embodied in the “end-to-end” design argument, which in essence suggests that networks should be neutral as among applications. As network theorist Jerome Saltzer puts it: “The End-to-End argument says ‘don’t force any service, feature, or restriction on the customer; his application knows best what features it needs, and whether or not to provide those features itself.’” The Internet Protocol suite (IP) was designed to follow the end-to-end principle, and is famously indifferent both to the physical communications medium “below” it, and the applications running “above” it.*<sup>41</sup>

This argument makes two claims, one in the realm of theory and another of a factual nature. The theoretical argument asserts that the Internet is best regulated according to its own unique structure and project, which Wu summarizes as providing “a platform for a competition among application developers.”<sup>42</sup>

The net neutrality argument suggests that regulators should respect the Internet's unique character by refraining from applying traditional regulatory models to it, such as antitrust:

*It is true that mainstream antitrust analysis has come to see price discrimination as generally uncontentious, or at least ambiguous. As between consumers and producers, it hurts some consumers and helps others, while raising the producers' profits. Yet this analysis can, and should, change as in the broadband context, because the practice of price discrimination may have external effects on the process of innovation and competition among applications. That is to say, while price discrimination among applications may not be troubling from a static perspective (as between existing consumers and producers), it may have dynamic consequences, for the competitive development of new applications*<sup>43</sup>.

I agree with Professor Wu that we should regard traditional regulatory models devised for different technical systems and markets with suspicion. We should, to the extent feasible,

---

<sup>40</sup> Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999); Lawrence Lessig, *The Future of Ideas : The Fate of the Commons in a Connected World*, 1st ed. (New York: Random House, 2001).

<sup>41</sup> Tim Wu, “Network Neutrality, Broadband Discrimination,” *SSRN Electronic Journal*, 2003, doi:10.2139/ssrn.388863, page 146.

<sup>42</sup> Ibid.

<sup>43</sup> Ibid, page 154.



consider first and foremost the effects that traditional regulations have on the Internet's growth and development. But the example of antitrust is weak.

We've seen that the Internet tends to favor the creation of winner-take-all monopolies in the application space: Google, Facebook, Netflix, Amazon, et al. It's somewhat intuitive that application monopolies discourage application innovation.

A better example of an inappropriate legacy regulation is Title II Common Carriage, a system devised to limit the abusive effects of a lawful monopoly by creating a semblance of competition by opening ILEC cable plants to open access. Because Wu's paper was a reaction to the removal of Title II regulations on ISPs, it doesn't make an argument on the question of the relevance of Title II to the Internet.

But even if we accept the theory that the Internet should be regulated first and foremost according to its unique character and goals rather than being forced into a legacy model, we don't have to agree that "neutrality" is the foremost example of its architecture. This question is actually empirical in nature.

We can discover the essence of the Internet architecture by examining its history through the RFCs and similar documents and by interviewing its chief inventors. In fact I have done this sort of research in two papers, "Designed for Change: End-to-End Arguments, Internet Innovation, and the Net Neutrality Debate" and "Arrested development: How policy failure impairs Internet progress".<sup>44</sup>

My research shows that the Internet architecture respects the uniqueness not only of the Internet Protocol but also of the multitude of applications it supports. Rather than providing one and only one service level to applications and telling them to "like it or lump it", the Internet includes features and protocols such as Differentiated Services and Integrated Services that allow the Internet to adapt to application needs.

These adaptation protocols are used by 4G and 5G 3GPP networks to support real-time voice, for example. My research, and technical analyses from the multi-stakeholder organization BITAG, suggest that adaptive behaviors are very advanced in the Internet.<sup>45</sup> The BITAG report in particular finds that Quality of Experience is not a zero sum game: the Internet can provide individual applications with the levels of service they need without causing discernable impairment for others.

Consequently, I propose that regulatory models for the Internet respect the body of work produced by the Internet's multi-stakeholder organizations regarding its technical nature,

---

<sup>44</sup> Richard Bennett, "Designed for Change: End-to-End Arguments, Internet Innovation, and the Net Neutrality Debate" (Washington, DC: Information Technology and Innovation Foundation, September 2009), <http://www.itif.org/index.php?id=294>; Richard Bennett, "Arrested Development: How Policy Failure Impairs Internet Progress" (Washington, D.C.: American Enterprise Institute, December 2015), <http://www.aei.org/publication/arrested-development-how-policy-failure-impairs-internet-progress/>.

<sup>45</sup> Broadband Internet Technical Advisory Group, Inc., "Differentiated Treatment of Internet Traffic" (Boulder: BITAG, October 2015), [http://www.bitag.org/documents/BITAG\\_-\\_Differentiated\\_Treatment\\_of\\_Internet\\_Traffic.pdf](http://www.bitag.org/documents/BITAG_-_Differentiated_Treatment_of_Internet_Traffic.pdf).

its offered services, and its financial models. This body of work does not conform to the simplistic end-to-end policy enforcement framework urged on the Commission by Lessig et al.

There are instances in which it is appropriate to block and throttle services, as we learned in the case of BitTorrent. There are also cases in which it is appropriate for an ISP to accept payment from an application provider for a specified level of service, as we learned in the cases of the Amazon Kindle and in Facebook Connect.

Because this is the case, the FCC's 2010 Open Internet Order was more appropriate – and more friendly to innovation – than the heavy-handed, top-down 2015 Order. The FCC needs to find a legal path in the direction of the 2010 regime, but even that regime was flawed.

## The Measurement of Internet Service Progress

Net neutrality policies are unique in that they rarely, if ever, consider the need to check the effects of the policy. The Internet is a large space, but it's highly quantified. So with a little effort we should be able to gain some of the numerical insight that the typical sports fan has about their favorite team. But until quite recently, Moneyball for the Internet wasn't a thing.

That has begun to change as advocates have sought to justify their support or opposition to the 2105 Order by examining its impact on investment. Intuitively, one supposes that a regulatory policy intended to redirect profits from one industry sector to another would depress investment in the disfavored sector, even if depressed profits may spur increased investment in some scenario.

One also supposes that firms in the disfavored sector would find investment options in the favored sector more attractive, but there's that pesky entrenched monopoly problem in the winner-take-all applications/edge service marketplace to contend with. Rather than adding gasoline to the investment debate, I'd like to suggest some measurements that the FCC (or another agency, such as the FTC or NTIA) could make to help us determine whether our Internet policy is on the right track.

Several metrics can help evaluate Internet policy:

- Startup formation: Are new Internet sector businesses forming at a faster or slower rate than the historical norm?
- Startup exits: Are startups going public, merging with larger firms, or shuttering at different rates?
- Consolidation of Internet traffic: This metric, which has been studied by Dr. Roslyn Layton at AEI, suggests that nations with strict net neutrality regulations (such as Netherlands) display greater consolidation among edge services.<sup>46</sup>
- Service differentiation: Impose a taxonomy on edge services that examines their use of traffic differentiation by ISPs. In a successful Internet ecosystem, we should see new services coming to the market, as well as new services of different types.
- Business model differentiation: Following the logic of service differentiation by traffic management type, examine financial models. Are firms breaking away from the ad-supported model of revenue?
- Broadband deployment: Are remote and rural areas enjoying service improvement in terms of speed, latency, and price improvements?
- Broadband adoption: Are new users overcoming their fears of personal safety violations and limited relevance and jumping into Internet use? What applications and services are drawing new users?

---

<sup>46</sup> Richard Bennett, *Roslyn Layton Visits High Tech Forum*, High Tech Forum Podcast, accessed June 14, 2017, <http://hightechforum.org/roslyn-layton-visits-high-tech-forum/>.



- Rate of improvement in broadband speed: Are the measureable properties of wired, wireless, and satellite services improving more or less rapidly than before?

My research on Internet performance is pertinent to the final bullet. On *High Tech Forum*, I follow the progress of Akamai's *State of the Internet* performance measurements. In a recent post, I examined the rate of improvement on a year-by-year basis from 2011 to 2016.<sup>47</sup>

Not surprisingly, broadband speeds are higher in the U. S. today than they were in 2010. This is the expected consequence of Moore's Law in any regulatory regime, and by itself is unremarkable.

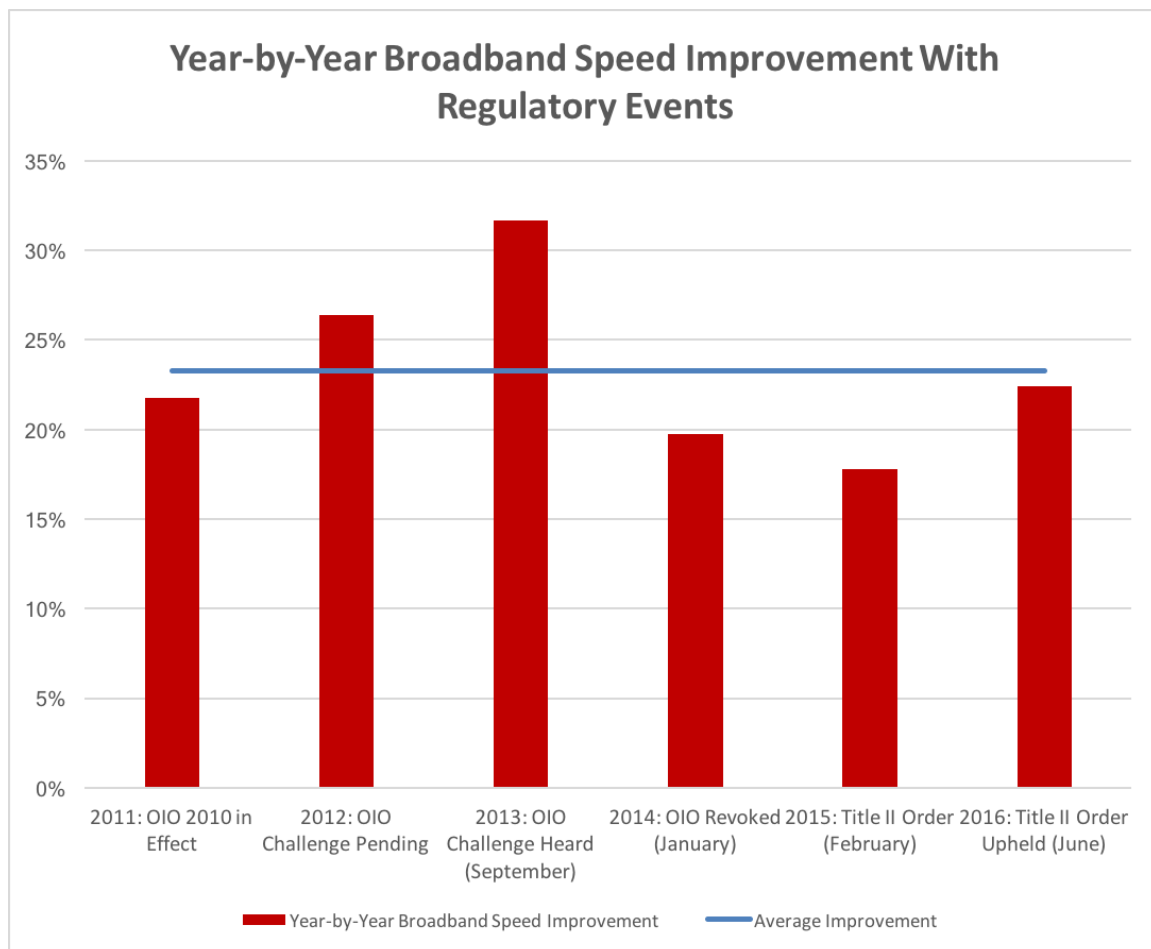


Figure 3: Year-by-Year Broadband Speed Improvement with Regulatory Events

But I found that rates of improvement have been lowest in years following new Internet regulations by the FCC. While the average improvement in broadband speed is 23% per year, the improvement rate dropped to 22% in the year following the 2010 Order.

<sup>47</sup> Bennett, "Open Internet Orders Degrade Internet Improvement."

The year following the 2015 Order was even worse, dropping to 18%. While the improvement rate increased to 22% in 2016, the two year average since the 2015 Order is well below average at 20%.

The data on rates of improvement in speed suggest that court challenges to FCC Open Internet orders have a positive effect while the regulations themselves are depressive. This is a simple back-of-the-envelope calculation, but rates of change analyses should be par for the course at the FCC.

## The Congressional Role

It practically goes without saying that the FCC's attempts at regulating the Internet have been hampered by the inconvenience of abiding by the law. The 2008 Free Press/Public Knowledge Petition was essentially laughed out of court because the agency did not ground it in law.<sup>48</sup> The 2010 Order was largely voided because it applied common carrier regulations to non-common carrier services.<sup>49</sup> And the 2015 Order evaded the law by applying common carrier classification to what are actually non-common carrier services.

When regulatory agencies misclassify services in order to obtain the authority to apply inappropriate regulations, we know we have a problem. When this behavior is allowed by the courts, we know that the problem can only be remedied by Congress. This is where we find ourselves.

The U. S. needs to have a rational, sensible framework for Internet oversight that recognizes the wisdom of the Internet Model, encourages investment and innovation in all Internet sectors, and does not permit firms in any sector to use their size, wealth, and power to inhibit innovation or to rob citizens of their fundamental rights. As this can only come from Congress, I urge the FCC to continue encouraging Congress to provide it with correct authority.

The current vehicle for Congressional Action, the 2015 Thune/Upton draft is flawed.<sup>50</sup> That draft simply codifies three bright-line rules that no ISP has any interest in violating and which don't protect consumers from the bulk of the threats they face when using the Internet.

A better approach would be for Congress to create a multi-stakeholder group to devise a plan for the effective oversight of the entire Internet ecosystem. This plan should identify key stakeholders, supply draft text for a bill, and examine the question of ongoing measurement.

Rather than bright-line rules, we need a responsive and accountable process for applying the Internet Model to the Internet in the interest of stimulating progress. This issue has become too politicized. It needs to be defused such that reasonable people can take sensible actions to provide the rather small degree of protection the issue warrants.

I do not advocate free rein for ISPs, edge providers, or anyone else. But playing "guilty unless proved innocent" has not worked.

---

<sup>48</sup> Wyatt, "Court Favors Comcast in F.C.C. 'Net Neutrality' Ruling."

<sup>49</sup> Gautham Nagesh and Amol Sharma, "Court Tosses Rules of Road for Internet," *Wall Street Journal*, January 15, 2014, sec. Business, <https://www.wsj.com/articles/appeals-court-strikes-down-fcc8217s-net-neutrality-rules-1389714575>.

<sup>50</sup> Sen. John Thune and Rep. Fred Upton, "Thune/Upton Bill" (2015), [https://www.commerce.senate.gov/public/\\_cache/files/7a90bcad-41c9-4f11-b341-9e4c14dac91c/28D2060F1855F668A25A7959F0B4D494.oll15072-3-.pdf](https://www.commerce.senate.gov/public/_cache/files/7a90bcad-41c9-4f11-b341-9e4c14dac91c/28D2060F1855F668A25A7959F0B4D494.oll15072-3-.pdf).