Before the

Federal Communications Commission

Washington, DC 20554

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

Joint Comments of Internet Engineers, Pioneers, and Technologists on the Technical Flaws in the FCC's Notice of Proposed Rule-making and the Need for the Light-Touch, Bright-Line Rules from the Open Internet Order

The undersigned submit the following statement in opposition to the Federal Communications Commission's Notice of Proposed Rulemaking – WC Docket No. 17-108, which seeks to reclassify Broadband Internet Access Service (BIAS) providers as "information services," as opposed to "telecommunications services."[1] Based on certain questions the FCC asks in the Notice of Proposed Rulemaking (NPRM), we are concerned that the FCC (or at least Chairman Pai and the authors of the NPRM) appears 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. Due to this fundamental misunderstanding of how the technology underlying the Internet works, we believe that if the FCC were to move forward with its NPRM as proposed, the results could be disastrous: the FCC would be making a major regulatory decision based on plainly incorrect assumptions about the underlying technology and Internet ecosystem.

---

[1] Restoring Internet Freedom, 82 Fed. Reg. 105 (proposed May 18, 2017) (to be codified at 47 CFR pt. 8 and 20) [hereinafter NPRM].

In order to correct the FCC's fundamental misunderstanding, we supply these comments, which contain certain facts about the structure, history, and evolving nature of the Internet.[2] We then point out how the Internet (and in particular BIAS) has changed since 2002, when the FCC first explicitly classified BIAS as an information service, and explain why that classification is no longer appropriate. Drawing on this background information, we then respond to specific questions from the NPRM. We then emphasize the need for the light-touch, bright-line rules present in the 2015 Open Internet Order. We explain the risks to innovation that could occur should the FCC reclassify BIAS as an information service and thus relinquish its authority to enforce light-touch, bright-line rules. We also provide nearly a dozen different examples of consumer harm that could have been prevented by the light-touch, bright-line rules as well as several examples of consumer benefits that happened as a result of the 2015 Open Internet Order. Finally, we conclude by emphasizing that if the FCC decides to move forward with some of the proposals in this NPRM then the result will have a disastrous effect on innovation in the Internet ecosystem as a whole.

I. A Brief Introduction to the Internet

A. A Network of Networks

Fundamentally, the Internet is a collection of tens of thousands of individual networks of computers and other devices owned, operated, and maintained by different entities.[3] In order to facilitate global communication, each of these independent networks interconnects to one or more of the other networks, thus leading to the term "Internet". While each of these networks speaks the same language and can thus be described using the same technical tools, the actual forms of the networks vary widely in terms of their architecture (i.e. their size and shape)

---

[2] Brief of the Amici Curiae Electronic Frontier Foundation, American Civil Liberties Union, and the American Civil Liberties Union of the Nation's Capital in Support of the Respondents, *United States Telecom Association v. Federal Commc'ns Comm'n,* 825 F.3d 674 (D.C. Cir. 2016) (No. 15-1063). Note that much of the text from these comments is drawn, sometimes word-for-word, from a previous letter provided by many of the same signatories.

[3] *CIDR Report*, www.cidr-report.org/as2.0/ (last visited Sept. 14, 2015).

and the underlying technology they use to connect devices. These differences depend in large part on the purpose each network serves.

For example, the type of network that is perhaps most familiar is a Local Area Network (LAN). LAN networks, such as the wired network in an office building or a Wi-Fi network in a home, connect a relatively small number of devices together. LAN networks connect to the Internet via yet another network, that of an Internet service provider, or ISP.

A typical ISP network connects anywhere from dozens to millions of homes and businesses (or in the case of some wireless ISPs, mobile devices) to the rest of the Internet. This connection occurs in two parts. First, the ISP must connect its customers (i.e. its retail subscribers) within a given geographic area to its own network facilities. This connection can be made over a variety of mediums: coaxial cables (originally used solely for cable TV transmission), copper wires (originally used solely for telephone communication), fiber optic cables, or, in the case of wireless ISPs, radio waves. For most communications mediums, ISPs configure the connection to be asymmetric: ISPs reserve more of the capacity of the connection (i.e. bandwidth) for downloads – data traveling to the customer – than they do for uploads from the customer.[4]

Second, the ISP's network connects to one or more of the other networks that make up the Internet. Typically, this second connection is made to either another ISP or an entity known as a "backbone provider." Unlike a retail ISP, a traditional backbone provider does not sell Internet access to individuals. Instead, backbone providers are "high capacity long-haul transmission facilities" which offer to connect different networks together in what are called "peering arrangements."[5]

In peering arrangements, the two connecting parties formalize the role each will play in their interconnection: what levels of traffic will be allowed to and from

---

[4] An exception is fiber connections, which many ISPs do not configure to be asymmetric, with the exception of some residential gigabit passive optical networks.

[5] *Verizon Communications, Inc.,* 20 FCC Rcd. 18433, 18493 (2005).

each party, where the interconnection will be located physically, and who will pay for upgrades to the interconnection if needed. Peering between large entities is often done in a settlement-free manner, meaning that no money is exchanged as part of the peering arrangement. This sort of settlement-free peering is sometimes dependent on the two networks exchanging similar levels of traffic.[6] However, an equal traffic exchange requirement frequently does not make much sense when backbone providers or edge providers[7] connect to ISP networks, due to the inherent asymmetric nature of ISP traffic. In other words, because most ISP customers download more than they upload, any peering arrangement between a backbone or edge provider and a retail ISP's network will result in more traffic being sent from the backbone or edge provider to the ISP than vice versa.

Finally, it should be noted that the same company often acts in different roles: a large ISP can provide backbone service to other, smaller ISPs, and also provide edge connections to individual customers. Similarly, a large edge provider may own similar infrastructure to a backbone provider. Thus, it is important when discussing the roles of the major players on the Internet to focus on the specific context in which they are being discussed; to do otherwise can lead to confusion and mismatched assumptions.[8]

---

[6] *See, e.g.*, *IPV4 and IPV6 Settlement-Free Peering Policy*, TIME WARNER CABLE, http://help.twcable.com/twc_settlement_free_peering_policy.html (last visited July. 14, 2017).

[7] The Open Internet Order defines an edge provider as "Any individual or entity that provides any content, application, or service over the Internet, and any individual or entity that provides a device used for accessing any content, application, or service over the Internet," and we adopt that terminology here. *See Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd. 5601, 5883-5884.

[8] For example, an ISP may have different customers depending on its role: as a retail ISP, its customers are the retail customers who subscribe to its service for Internet access, but if it also provides transit services as a backbone provider, then in that role its customers would be other ISPs.

B. Packet-Switching and Congestion

While the above gives an accurate picture of how the Internet is laid out, it does not explain how the different networks actually succeed in communicating with one another.

Two major technical principles underlie how the Internet functions. The first is the concept of packet switching. In a packet switched network, the data to be transmitted (be it a webpage, images, sound files, or a video) is broken down into chunks known as packets, each of which is sent off individually to its destination.[9] An Internet packet contains several important pieces of information: the numerical address of the device which sent the packet, known as an Internet Protocol address (or IP address); the IP address of the intended recipient; the type of data the packet contains; and the actual data, often referred to as the "payload."[10] In this way, a packet is similar to a postcard—anyone who is part of the delivery chain can read whom it is intended for, who sent it, and what it says. (Note that this does not hold true if the content of the packet is encrypted—then the packet is more like a postcard where the message is written in code only the sender and receiver can understand, but anyone reading the postcard can still see who the sender and receiver are.)

When it comes time for a computer to transmit a packet, the computer sends it to the next "hop" in the delivery chain, typically a network device known as a "router." A router is a specialized device that bridges the connection between multiple communications links, whose sole job is to send packets one step closer to their destination. It does this via a "routing table," which lists all the communication links the device is attached to, and the range of IP addresses that can be found on each of those links. Thus when a packet arrives, the router compares its destination address to the routing table and then sends it off on the appropriate link.

---

[9] Jonathan E. Nuechterlein & Philip J. Weiser, DIGITAL CROSSROADS: AMERICAN TELECOMMUNICATIONS POLICY IN THE INTERNET AGE 42-43 (1st ed. 2005).

[10] Information Sciences Institute, UNIV. OF SOUTHERN CALIFORNIA, DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION (1981), https://tools.ietf.org/html/rfc791.

This form of routing is critical to how the Internet functions today. All the originating computer needs to know is that the network will take care of the routing, and all each router needs to know is which of its outgoing links is closer to the destination than it is itself. In this way, an ISP customer's device can tell the ISP where to send its data, without having to know how the ISP has constructed its network or even what networks it interconnects with.

Of course, sometimes packets arrive at a router faster than the router can process them or faster than the communications link can transmit them, leading to congestion. Internet congestion is analogous to the traffic congestion that might occur when a busy four-lane interstate splits into two smaller two-lane highways: even though there is theoretically enough capacity, if all of the cars coming from the interstate want to travel along only one of the smaller highways, a backup will ensue. Similarly, if a router receives packets faster than it can transmit them along their desired links, the packets will be stored in a buffer until they can be sent. Unlike traffic congestion, however, if too many packets fill up the buffer, any new packets will simply be "dropped", or discarded. Thus the Internet is a "best-effort" service: devices make their best effort to deliver packets, but do not guarantee that they will succeed.[11]

C. The Principles of Openness and Non-Interference Are Key Features of the Internet's Design

The Internet is more than just a way for computers across the globe to exchange packets of data; it is a platform on which people have developed a variety of important technologies, from web browsing to email to social

[11] In fact, the TCP (Transmission Control Protocol) indirectly uses dropped packets as a signal to determine how fast it should transmit data. Each TCP packet contains a sequence number, which indicates how many bytes of data have been sent so far. If the device on the receiving end is missing data because packets have been dropped (e.g. it has bytes one through ten, and then twelve through twenty), then it sends a signal to the sender indicating that it has only received some of the packets. The sender then reduces its transmission rate (and re-sends the missing packets), because the network is likely congested at some point along the route the packets are taking. In this way, the routers along the path don't have to worry about making sure a packet is never dropped or that it does successfully get to its destination; the endpoints detect congestion automatically and reduce their transmission rate accordingly.

networking to online courses. The Internet's tremendous growth and popularity as a platform have been due at least in part to two design principles, both of which ensure that the Internet is an open, neutral platform.

The first of these design principles is the idea of the layered network communications stack (often referred to as simply "the network stack"). Essentially, the network stack is a way of abstracting the design of software needed for Internet communication into multiple layers, where each layer is responsible for certain functions, but can implement those functions in any way that meets the specifications. For example, the "physical layer" is responsible for physically transmitting and receiving bits. It can do so over fiber optic cable, copper telephone lines, radio signals, etc., as long as it provides a way for the layer above it to access the "transmit and receive bits" function. Further up the stack is the "network layer," which is responsible for ensuring each device on the network has a unique address, and for sending and receiving packets of data to specific addresses. It is at this layer that the famous Internet Protocol actually resides, which provides a "send data to a certain address" function to the layer above. Similarly, further up is the "transport layer," which is the layer that is usually exposed to applications in order to send data to other devices. This is the layer at which the also well-known Transmission Control Protocol (TCP) resides, which is responsible for ensuring that data gets to its destination reliably and intact.[12]

The key takeaway from the idea of the network stack is that the specification is defined well enough for a developer to understand how her protocol will interact with the rest of the network stack, while at the same time flexible enough to allow for different implementations and widely-varying uses cases (since each layer can tell the layer below it to carry any type of data). This is why the same Internet Protocol can support such varied applications as email and real-time video-conferencing and NTP (Network Time Protocol), a service that automatically syncs the clocks of Internet-connected computers with microsecond accuracy. If

---

[12] Douglas E. Comer, INTERNETWORKING WITH TCP/IP, VOL. 1 (6th ed. 2013). Note that for simplicity of explanation, some of the layers have been omitted, such as the link layer (which sits between the physical layer and the network layer).

someone wants to develop a new Internet application or protocol, all they have to do is insert their new technology at the appropriate layer; the layers below will perform their functions regardless of the type of data the developer tasks them to handle. This openness allows developers to build new and different types of applications without having to worry about the technical details of the layers below. "Consider, for instance, how these design principles collectively facilitated the rise of the World Wide Web application. Because the network is general, its founder Tim Berners-Lee could introduce it without requiring any changes to—or permission from—the underlying physical network."[13] All he had to do was define the protocol, and the underlying layers transported the data as desired.

The second design principle is the "end-to-end principle." In order for a network to be general purpose, the nodes that make up the interior of the network should not assume that end points will have a specific goal when using the network or that they will use specific protocols; instead, application-specific features should only reside in the devices that connect to the network at its edge.[14]

It is easy to see how the end-to-end principle applies in the case of the Internet. The interior of the network, made up of the communications links (i.e. the physical cables) and the routers that connect them, originally did very little processing or modification of the packets they handled.[15] In fact, the Internet Protocol, which is the protocol routers use to communicate, does not even have a way for a device to make sure a packet arrived at its final destination. All the

---

[13] Brief Amicus Curiae of Internet Engineers and Technologists Urging That The FCC's Order Be Affirmed, *Verizon v. Federal Commc'ns Comm'n,* 740 F.3d 623 (D.C. Cir. 2014) (No. 11-1355).

[14] J.H. Saltzer, D.P. Reed & D.D. Clark, *End-to-End Arguments in System Design*, 2 ACM Transactions on Computer Systems 277 (1984).

[15] We note that many network operators and equipment vendors contest the fundamental nature of the "end-to-end" principle. However, their arguments are usually made in order to claim that they (or their equipment) can "add value" to the network by adding "smarts" to the network itself—usually as a way to try to reverse the commoditization of network hardware and services. Further, as we explain in Section IV.A, this insertion of "smarts" into the interior of the network frequently causes problems for developers of innovative new protocols and applications designed to run on a neutral Internet.

Internet Protocol requires is for a router to read incoming packets, figure out the next hop along their path, and make its best effort to send them off. The actual specialization comes entirely from the computers and servers and smartphones that connect at the "edge" of the Internet. This is how the Internet can support protocols that require guaranteed delivery of data (such as file transfer protocols), as well as protocols where guaranteeing delivery is less important than ensuring that the packets are received at low latency (such as protocols for voice or video chat).

D. Cross-Layer Applications Enhance Basic Infrastructure

The network-stack architecture of the Internet is crucial to its past and continued versatile and innovative nature, and it has allowed for the evolution of additional complexity to support the simple-seeming experience of modern user-facing applications. Several application-layer protocols whose development was made possible by virtue of the stacked model have since become crucial to the smooth functioning of tasks that at first glance would appear to be fully encompassed by lower layers.

1. The Cross-Layer Nature of DNS

For example, as explained above, resources on the Internet are addressed by their IP address, but a modern user does not know offhand the IP address of the site they are attempting to access. For example, a user would likely not directly attempt to visit 69.50.232.54, but would instead enter "eff.org" into a browser's URL bar. The Domain Name System (DNS) is the protocol that provides this convenience to the user. Yet while from a network engineering implementation standpoint DNS is an application-layer protocol, its primary purpose is to enhance functionality otherwise provided by the internetwork layer. Additionally, no typical end user would manually and intentionally use DNS on its own. For the standard use case, DNS and IP go hand-in-hand. From the standpoint of looking at where the benefits of DNS are realized, it would be more reasonable to consider them in line with the layer they affect rather than the layer they are implemented in, and recognize DNS' current place in practice as a tacked-on implementation detail of the more fundamental Internet layer.

DNS allows a vital level of abstraction. With DNS, the user can request a named resource, such as a domain name (e.g. www.eff.org), or a particular page

location at that domain (e.g. www.eff.org/about). By using DNS, the user does not need to know the IP address. More significantly, the IP address can change over time, including if the site moves behind a Content Delivery Network (CDN) to deliver the content more efficiently and ensure it remains available in case of a denial of service attack. The benefit to the user is that they request the particular resource they want, using an addressing system that is human-memorable. The underlying system may address that same resource in whichever way is best for its own functioning, to say nothing of how it chooses to route that request, but these details are all hidden away and irrelevant to the user. In the user's mental model, the endpoint is represented by the resource's URL, which is what they specify.

Furthermore, DNS is itself a multi-step protocol requiring different players to function.[16] The user first contacts the recursive resolver, which might be located within an ISP, or today is often a third-party provider. This resolver gets its information by contacting several authoritative DNS servers. At the top level are the "root servers", which are located around the world and run by different independent bodies such as the US Department of Defense, ICANN, and the University of Maryland.[17] These servers respond to the recursive resolver with the location of the Top Level Domain (TLD) servers for the domain in question; for "eff.org", this would be one of the ".org" servers. Then a request is sent to one of these TLD servers, which will know the IP address of the server(s) to ask next. The last DNS server in the chain will know the IP address assigned to the domain itself. This cooperative process is designed such that no single player provides the entire service.

2. Internet Routing's Similarities to Telephone Call Routing

In a system that in many ways parallels the telephone network, Internet routing is dynamically controlled by application-layer services that communicate to establish network paths. Dynamic routing increases the capacity of the network

---

[16] *How the Domain Name System (DNS) Works*, VERISIGN https://www.verisign.com/en_US/website-presence/online/how-dns-works/index.xhtml. (last visited July 14, 2017).

[17] *Root Servers*, INTERNET ASSIGNED NUMBER AUTHORITY (IANA), https://www.iana.org/domains/root/servers (last visited July 14, 2017).

by spreading load along popular links to less utilized pathways, and also takes into account policy decisions. In both the Internet and the public-switched telephone network (PSTN), dynamic routing is a basic functionality that is an integral part of the system's structure.

Though the PSTN was originally constructed with fixed routes, dynamic routing was added in the 1980s to reduce network congestion.[18] Later, regulatory pressure to allow people to keep their phone numbers when switching to a new provider required complexity and routing schemes to be added. With the growth of Voice over IP (VoIP), interchange between the Internet and the PSTN further blurred the line between the two. Now, in a modern PSTN network, a series of complex management decisions mean that the number dialed is largely disconnected from how it is routed, or even if it will enter the classic PSTN network at all, and the underlying network is expected to handle all of this routing complexity as a basic matter of course. In this way, both the Internet and the PSTN are alike: the end user chooses a destination to send their data to, and the network takes care of figuring out how to get it to that destination.

On the Internet, the primary routing management protocol is the Border Gateway Protocol (BGP). Residing at the application layer, but vital to internetworking, BGP allows ISPs to announce the routes that packets can follow to arrive at a destination.[19] This gives ISPs control over where packets will go, avoiding congestion and honoring peering agreements in much the same way as the PSTN. Unlike the PSTN, which has a dedicated channel for communicating route information, BGP information is sent over TCP. Yet the output of BGP is vital to the functioning of the internetwork layer so that routers know how to configure themselves, making it a cross-layer protocol.

In both of these systems, the PSTN and the Internet, the concept of a "point" that information is sent to is an abstraction that, for carriers' own good, does not

---

[18] Deep Medhi, *Routing Management in the PSTN and Internet: A Historical Perspective*, 15 J. NETWORK AND SYSTEMS MGMT. 1 (2007).

[19] Y. Rekhter et al, *A Border Gateway Protocol 4 (BPG-4)*, THE INTERNET SOCIETY (Jan. 2006), https://tools.ietf.org/html/rfc4271 (last visited July 14, 2017).

map to the functioning of a system capable of handling the complex requirement caused by a modern heavy system load.

II. How the Internet Has Changed Since 2002

While technologies like the Internet Protocol and TCP have changed little since the early nineties, part of the Internet's resilience and value comes from the myriad ways in which those underlying protocols can be used. It should come as no surprise, then, that the Internet as a whole is not a static, monolithic creation, but a constantly evolving system. In this section, we describe the major ways the Internet as a whole, and consumer ISPs in particular, have changed since 2002, when the FCC first decided to classify broadband service as an information service. By explaining these changes, we show that the primary function of ISPs today is to transmit-to and from points specified by the user-information of the user's choosing, without change in the form or content of the information as sent and received.

A. New Internet Protocols and Services Continue to be Invented

Although it may seem obvious, it is worth noting that new services and applications that rely on the Internet are constantly being developed. For example, take the continuing rise of the "Internet of Things," a term used to describe the increasingly Internet-connected nature of objects in our environment that were not traditionally thought of as Internet-connected computers.[20] Typical examples include everything from Internet-connected home appliances to wearable devices (including fitness and health-tracking devices) and even Internet-connected automobiles. Many of these devices use the Internet in novel ways and could be seriously affected by blocking or throttling based on protocol or service.

Additionally, innovation surrounding the Internet is not limited to new services that use existing protocols to communicate. Current innovation goes even deeper, down the network stack to new protocols and fundamentally new ways of

---

[20] Bonnie Cha, *A Beginner's Guide to Understanding the Internet of Things,* RE/CODE (Jan. 15, 2015), http://recode.net/2015/01/15/a-beginners-guide-to-understanding-the-internet-of-things/ (last visited July 14, 2017).

using the network. For example, the "InterPlanetary File System (IPFS) is a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files,"[21] first developed in 2014.[22] The goal of IPFS is to create a more permanent, more distributed version of the World Wide Web, one in which the entirety of files available on the Web are distributed to millions of computers across the globe. If successful, IPFS would make censorship of individual webpages or websites technically impossible, while also ensuring that a permanent record of all the files ever posted on the Web is always available for archival and historical purposes. IPFS relies on the underlying decentralized, open infrastructure of the Internet, distributing data using peer-to-peer protocols that are fundamentally different from the sorts of protocols used to transmit webpages, emails, or streaming videos.

The key takeaway from these examples is that Internet innovation is ongoing—but more importantly, this sort of innovation relies on the open, neutral nature of the Internet. To be absolutely clear, much of this innovation has occurred without any assistance from broadband ISPs (and in some cases, despite interference from broadband ISPs). While it is certainly true that ISP investment in increasing bandwidth (and innovations in how to provide that bandwidth) has enabled many of the services people think of as part and parcel of their Internet experience today (e.g. video streaming), the overwhelmingly vast majority of those services were not actually created by ISPs and are not offered by ISPs. They are offered by third parties that the customer simply wants to transmit data to and receive data from—without interference by their ISP.

B. ISP Caching is Being Replaced by Third-Party Caching Services

In the early days of the Internet, many ISPs set up caching servers that would sit between their customers and the rest of the Internet. These servers would record what data customers were requesting from the World Wide Web, and store

---

[21] *The IPFS Project*, https://ipfs.io/ (last visited July 14, 2017).

[22] *History for IPFS*, GITHUB, https://github.com/ipfs/ipfs/commits/master/README.md (last visited July 14, 2017).

copies in a local cache that the server could send when other customers made the same request. For example, if many customers were reading the same newspaper article about net neutrality, the ISP would store a copy of that article on the caching server. Then, when a new request for the article came in, the ISP would send back the local copy instead of waiting for the request to go all the way to the newspaper's server and back via the Internet. This way the ISP could reduce the amount of time it took for a customer to download the article (since the ISP's caching server would be closer to the customer than the newspaper's server), and ISPs could save on bandwidth (since they would not have to re-download the article from the newspaper's server every time a new request came in).[23]

However, recent changes have decreased the need for ISP caching services. This is due to the widespread use of Content Delivery Networks, or CDNs. CDNs are very similar to the caching servers described above, except they are often operated by companies other than ISPs (such as edge providers, or third-party companies who sell their CDN service to edge providers). CDNs consist of Internet-connected caching servers strategically placed in different geographic regions, on the edge of or inside the network of one or more ISPs. Content originators upload their content to these caching servers, so that they can have fine-grained control of what gets cached and how long it stays cached—control they do not have over ISP-controlled caches.

In addition to becoming unnecessary, ISP caching is also becoming less feasible due to the increasing proportion of Internet traffic that is encrypted. (In 2010 less than 2% of traffic on the Internet was encrypted[24], but by February of 2017 over half of Internet traffic was encrypted.[25]) Encryption prevents ISP

---

[23] James F. Kurose & Keith W. Ross, COMPUTER NETWORKING: A TOP-DOWN APPROACH (4th ed. 2007).

[24] *Sandvine Intelligent Broadband Networks, Global Internet Phenomena Report* (2011), *available at* https://www.sandvine.com/downloads/general/global-internet-phenomena/2011/1h-2011-global-internet-phenomena-report.pdf (last visited July 14, 2017).

[25] Gennie Gebhart, *We're Halfway to Encrypting the Entire Web,* ELECTRONIC FRONTIER FOUNDATION (Feb. 21, 2017), https://www.eff.org/deeplinks/2017/02/were-halfway-encrypting-entire-web (last visited July 14, 2017).

caching from being effective, because when a user requests a webpage or file over an encrypted connection the ISP cannot see the name or location of the file the user is requesting or the contents of the file itself. As a result, the ISP has no way of knowing what files are popular enough to cache, nor any way of knowing when a user requests a popular file. Given the inevitability of ubiquitous encryption, ISP caching is destined to become an obsolete practice.[26]

Thus, this example also illustrates how the role ISPs play in the Internet ecosystem has changed since 2002. In the early days of the Internet, caching and processing was a key component of running an ISP and managing its network; today, that role is filled by third-parties, and once again customers and edge services simply expect ISPs to transmit data to and from their destinations, be they servers run by third-party CDNs inside the ISPs network, or distant servers on the other side of the globe.

C. DNS and Email Are No Longer the Province Solely of ISPs

Another major change since the turn of the millennium has been the dramatic surge in popularity of third-party email providers. For example, consider US email providers. Currently, Microsoft, Google, and Yahoo (the top three in the US, barring mass-marketing email providers) were ranked first, ninth, and eleventh in the world in terms of volume of email sent. For comparison, the top three US ISPs, Comcast, Charter, and AT&T[27] ranked 17th, 26th, and 12th.[28] While not all of

---

[26] Indeed, all major browsers have announced that they will only support the next version of the famous HTTP protocol, HTTP/2, over encrypted connections. Dan Goodin, *New Firefox Version Says "Might as Well" to Encrypting All Web Traffic*, ARS TECHNICA (Apr. 1, 2015), http://arstechnica.com/security/2015/04/new-firefox-version-says-might-as-well-to-encrypting-all-web-traffic/ (last visited July 14, 2017).

[27] *Press Release: About 960,000 Added Broadband in 1Q 2017*" LEICHTMAN RESEARCH GROUP, INC. (May 19, 2017), http://www.leichtmanresearch.com/press/051917release.html (last visited July 14, 2017).

[28] *Email & Spam Data, June 2017,* TALOS INTELLIGENCE, https://talosintelligence.com/reputation_center/email_rep#top-senders-owner (last visited July 14, 2017). Note that some companies are listed under multiple organizational names; when cited above, we have provided the highest ranking for a given company's consumer-focused service.

the email coming from those domains is generated by customers, the dramatic difference in popularity illustrates the decreasing relevance ISP customers put on the information services provided by their ISPs.

Similarly, fewer people are making use of their ISPs' Domain Name Systems (DNS), in large part because over a dozen different ISPs (including AT&T[29], Cablevision[30], Charter[31], Comcast[32], Cox[33], CenturyLink[34], Frontier[35], Mediacom[36], RCN[37], Sprint[38], T-Mobile[39], Time Warner[40], and Verizon[41]) have

---

[29] Forum Post, AT&T COMMUNITY FORUMS, (Mar. 27, 2017 at 12:40 PM), https://forums.att.com/t5/AT-T-Internet-Features/ATT-DNS-Assist-Page/td-p/5108480 (last visited July 14, 2017).

[30] *DNS Assistance Service*, OPTIMUM (archived from Sept. 25, 2008), https://web.archive.org/web/20090813095417/http://www.optimum.net:80/Article/DNS (last visited July 14, 2017).

[31] Evan Anderson, *Fixing Charter's DNS Hijacking,* EVAN J.D. ANDERSON (June 23, 2010), https://ejdanderson.wordpress.com/2010/06/23/fixing-charters-dns-hijacking/ (last visited July 14, 2017).

[32] Cade Metz, *Comcast Trials DNS Hijacker*, THE REGISTER (July 28, 2009 at 8:26 PM), http://www.theregister.co.uk/2009/07/28/comcast_dns_hijacker/ (last visited July 14, 2017).

[33] Nate Ritter, *How to Turn Off (Disable) Cox's 404 Hijacking/Interception*, THE BLOG OF NATE RITTER, WEB CHEF (Oct. 3, 2008), http://blog.perfectspace.com/2008/10/03/how-to-turn-off-disable-cox-404-hijacking/ (last visited July 14, 2017).

[34] Forum Post, DSLREPORTS (Dec. 21, 2011, 1:44 PM), http://www.dslreports.com/forum/r26682725- (last visited July 14, 2017).

[35] Forum Post, DSLREPORTS (July 21, 2015, 12:35 AM), http://www.dslreports.com/forum/r30184337-Frontier-DNS-servers-redirecting-to-ads-page (last visited July 14, 2017).

[36] Karl Bode, *Mediacom Users Still Struggle To Opt Out of DNS Redirection Ads*, DSLReports (April 28, 2014, 8:19 AM), https://www.dslreports.com/shownews/Mediacom-Users-Still-Struggle-To-Opt-Out-Of-DNS-Redirection-Ads-128723-page (last visited July 14, 2017).

[37] Bill Adler, *Who Stole My Web Browser?*, INFINITEEDGE (Oct. 13, 2009), http://infiniteedge.blogspot.com/2009/10/who-stole-my-web-browser.html (last visited July 14, 2017).

[38] Reddit Post, REDDIT, http://www.reddit.com/r/Sprint/comments/2fl6pk/are_sprint_3g_and_4g_towers_hijacking_nxdomain/ (last visited July 14, 2017).

engaged in the practice of DNS hijacking over the past decade. As a result of DNS hijacking, consumers have been exposed to degraded performance, malfunctioning applications, and security vulnerabilities.[42]

At the same time, free, open DNS servers, often offering better performance or more features than ISP DNS servers, have proliferated online.[43] For example, Google offers the Google Public DNS, free for any Internet user, which handles over 400 billion DNS requests per day.[44] Many ISP customers have chosen to use such third-party DNS services in order to avoid the security and performance issues ISPs have introduced into their own DNS services.

D. Customers Depend on ISPs for Internet Access, Not Information Services

In the early days of Internet access, customers frequently chose which ISP to subscribe to based on the content and information services that ISP supplied in addition to general Internet access. ISPs like AOL, Compuserve, or Prodigy differentiated themselves based on the different information services each

---

[39] Reddit Post, REDDIT, https://www.reddit.com/r/tmobile/comments/3dyk1h/how_do_i_turn_of_nxdomain_hijacking/ (last visited July 14, 2017).

[40] Nate Ritter, *How to Turn Off (Disable) Road Runner's 404 Hijacking/Interception,* THE BLOG OF NATE RITTER, WEB CHEF (Feb. 29, 2008), http://blog.perfectspace.com/2008/02/29/how-to-turn-off-disable-road-runners-404-hijackinginterception/ (last visited July 14, 2017).

[41] *Opting Out of DNS Assistance*, VERIZON.COM, http://www.verizon.com/support/residential/internet/fiosinternet/troubleshooting/network/questionsone/99031.htm (last visited July 14, 2017).

[42] Ryan Single, *ISPs' Error Page Ads Let Hackers Hijack Entire Web, Researcher Discloses*, WIRED (April 19, 2008), https://www.wired.com/2008/04/isps-error-page.

[43] Yunhong Gu, *Google Public DNS and Location-Sensitive DNS Responses,* GOOGLE WEBMASTER CENTRAL BLOG (Dec. 15, 2014), http://googlewebmastercentral.blogspot.com/2014/12/google-public-dns-and-location.html (last visited July 14, 2017).

[44] *Introduction to Google Public DNS,* GOOGLE, https://developers.google.com/speed/public-dns/docs/intro (last visited July 14, 2017).

provided—services like chat rooms, bulletin board systems, email, and specialized content only available to an ISP's own subscribers.[45]

Now, however, ISPs compete primarily on the reliability and bandwidth of their Internet connections.[46] Customers subscribe to an ISP's service not for information services the ISP might provide, but because the subscription enables customers to transmit and receive data to and from the wider Internet. The information services ISPs provide are no longer connected in any meaningful way to the data routing and transmission service they offer. Saying that ISPs provide an information service to their customers because they offer caching and webmail in addition to Internet connectivity is like saying that airlines are in the business of providing an entertainment service because they offer in-flight movies in addition to transportation. While these additional services might be selling points, they are not integral to the fundamental offering ISPs and airlines make: to transport things (either data or people) at the customer's request.

III. Technical Responses to the FCC's NRPM

In light of the foregoing, we can better anticipate the technical consequences of the NPRM and the risks of the information service classification it proposes. We provide specific technical clarifications in response to selected allegations and misconceptions introduced in the NPRM, and in doing so strongly recommend that the regulatory structure proposed by the NPRM be rejected.

---

[45] Michael Wolff, NETSTUDY, 1-4 (1997).

[46] *See, e.g.*, *Sprint 4g Commercial,* YOUTUBE, https://www.youtube.com/watch?v=NPdkvg9Kw-M (last visited Sept. 14, 2015) (touting the bandwidth of Sprint's 4G wireless network); *Comcast-Fast Rabbit*, YOUTUBE, https://www.youtube.com/watch?v=h16qMJ_LCyg (last visited Sept. 14, 2015) (comparing Comcast's high-speed Internet access with "a rabbit/panther with turbines backed by an unusually strong tailwind on ice . . . driven by an over-caffeinated fighter pilot with a lead foot all traveling down a ski jump in Switzerland under better than ideal conditions.").

A. The NPRM Fundamentally Misunderstands Who Offers Which Services Online

First, the NPRM fundamentally misunderstands which entities offer which services to customers online, and as a result, claims that it is ISPs, and not edge providers, who provide the wealth of useful services customers can find on the Internet today. For example, the NPRM states:

> We believe that Internet service providers offer the "capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications." Whether posting on social media or drafting a blog, a broadband Internet user is able to generate and make available information online. Whether reading a newspaper's website or browsing the results from a search engine, a broadband Internet user is able to acquire and retrieve information online. Whether it's an address book or a grocery list, a broadband Internet user is able to store and utilize information online. Whether uploading filtered photographs or translating text into a foreign language, a broadband Internet user is able to transform and process information online. In short, broadband Internet access service appears to offer its users the "capability" to perform each and every one of the functions listed in the definition—and accordingly appears to be an information service by definition. We seek comment on this analysis.[47]

In this paragraph, the Commission conflates the roles of Internet Service Providers and the myriad companies that offer substantive services on the Internet as a whole. No BIAS provider offers the capabilities listed, like posting on social media, reading a newspaper's website, storing a grocery list, translating text into a foreign language, by itself. Rather, the vast majority of these capabilities (and in the case of many BIAS providers, all of these services) are offered by other third

[47] NPRM ¶ 27.

parties on the Internet. ISPs merely provide the transport between the end user and the capability that they are attempting to access.

The NPRM's analysis is fundamentally flawed. It confuses offering the capability to *connect* to a third-party service with offering the capability of the third-party service itself, and implies that because ISPs allow users to connect to third-party services of the users' choosing, somehow it is the ISP itself that is offering that service. If the same flawed logic were applied to the telephone network, one would conclude that because Verizon's customers can use their phones to order a pizza, it is Verizon (instead of the local pizza parlor) that is offering the capability for having pizza delivered. The same logic makes a media company of the US Postal Service merely because one may have magazines delivered by mail. The NPRM's characterization of ISPs as offering the capabilities associated with the totality of available services on the Internet similarly defies common sense.

We next answer several questions from the same paragraph.

"Can broadband Internet users indeed access these capabilities?"[48]

Obviously, BIAS customers can indeed access these capabilities, but only with the involvement of other parties that actually provide the service to which the broadband service is providing a connection. If these third parties did not exist, then BIAS customers would not be able to access these capabilities—despite the fact that the BIAS provider would still be offering the exact same services to their customers. As a result, it is obvious that ISPs do not provide these capabilities in-and-of-themselves, but simply provide access to them via their telecommunications offerings.

"Are there other capabilities that a broadband Internet user may receive with service?"[49]

---

[48] *Id.*

[49] *Id.*

Given the end-to-end principle, any service that appears on the Internet will be available to ISP customers. However, the end-to-end principle depends on non-interference by ISPs. If the FCC reclassifies BIAS providers as information services and is unable to enforce light-touch rules against ISP interference with customer traffic, many new capabilities the FCC has not envisioned will never come to be.

"If broadband Internet access service does not afford one of the listed capabilities to users, what effect would that have on our statutory analysis?"[50]

As we stated above, broadband Internet access does not directly provide any of the listed capabilities. For example, if a series of extremely coincidental bugs simultaneously forced all the cloud storage providers in the world to go offline, then BIAS customers would no longer have the capability to upload information to them—even though the fundamental service provided by their ISPs had not changed. Thus, it is incorrect to say that BIAS providers offer these capabilities; they simply offer the transmission of data on behalf of customers to and from edge providers that provide these services themselves.

Since broadband service does not directly provide any of the listed capabilities to users, this portion of the NPRM's statutory analysis is baseless and fundamentally incorrect. Any analysis that BIAS should be classified as an information service because of the services offered by third parties on the Internet is inherently flawed.

"More fundamentally, we seek comment on how the Commission should assess whether a broadband provider is "offering" a capability. Should we asses [sic] this from the perspective of the user, from the provider, or through some other lens?"[51]

As we have explained, from no perspective does a broadband provider "offer" any of the listed capabilities. When an Internet user wants to search for cat

---

[50] *Id.*

[51] *Id.*

pictures, the search engine DuckDuckGo might offer that capability to her, but given that all the ISP does is transmit data to and from a server the ISP does not own, under no reasonable interpretation does the ISP "offer" that capability.

> In the Title II Order, the Commission in turn found that "consumers are very likely to use their high-speed Internet connections to take advantage of competing services offered by third parties" and asserted the service "is useful to consumers today primarily as a conduit for reaching modular content, applications, and services that are provided by unaffiliated third parties." We seek comment on how consumers are using broadband Internet access service today. It appears that, as in 2002 and 2013, broadband Internet users "obtain many functions from companies" other than their Internet service provider.[52]

The Title II Order's analysis is correct: in 2017, BIAS customers primarily use their Internet service as a conduit for reaching content provided by unaffiliated third parties. Although the NPRM implies otherwise, this is a marked departure from how broadband customers used their broadband Internet access service in 2002. As we explained in Section II.D, in the early days of Internet access, customers frequently chose which ISP to subscribe to based on the content and information services that ISPs supplied in addition to general Internet access. ISPs like AOL, Compuserve, or Prodigy differentiated themselves based on the different information services each provided—services like chat rooms, bulletin board systems, email, and specialized content only available to an ISP's own subscribers. In other words, ISPs competed on what information services they actually provided themselves. Not so today.

Further, although Internet users obtained many functions from third parties in 2002, the wealth of capabilities that users can find on the Internet today simply did not exist at that time. Very few services that today are common household names existed in 2002: Wikipedia had only 20,000 articles (compared to its current

---

[52] *Id.* ¶ 28.

5.4 million),[53] Google did not have its IPO until 2004[54], Facebook would not exist (even as a prototype) for another year,[55] YouTube was three years away from its creation,[56] Twitter was four years away from being founded,[57] and Netflix was five years away from streaming its first movie online.[58]

In short, Internet users today have more choices of third-party services to use, and are far less likely to use their ISP for anything besides providing a connection to those services.

"It also appears that many broadband Internet users rely on services, such as Domain Name Service (DNS) and email, from their ISP. Is that correct?"[59]

While it is true that many broadband Internet users do still rely on DNS and email services from their ISP, as mentioned in Section II.C, that number is dwindling. Further, even though many Internet users take advantage of third-party DNS services, we do not believe DNS should be seen as a separate technical service for purposes of arguing for reclassification, as we described in more detail in Section I.D.1.

---

[53] *Compare Main Page*, WIKIPEDIA (archived from Jan. 24, 2002), https://web.archive.org/web/20020124190441/http://www.wikipedia.com:80/ *with Main Page*, WIKIPEDIA, https://en.wikipedia.org/wiki/Main_Page (last visited July 14, 2017).

[54] Google Inc. Registration Statement (Form S-1) (Apr. 29, 2004). https://www.sec.gov/Archives/edgar/data/1288776/000119312504073639/ds1.htm.

[55] Katharine A. Kaplan, *Facemash Creator Survives Ad Board*, THE HARVARD CRIMSON (Nov. 19, 2003), http://www.thecrimson.com/article/2003/11/19/facemash-creator-survives-ad-board-the/.

[56] Miguel Helft & Matt Richtel, *Venture Firm Shares a YouTube Jackpot*, NEW YORK TIMES (Oct. 10, 2006), http://www.nytimes.com/2006/10/10/technology/10payday.html.

[57] Nicholas Carson, *The Real History of Twitter*, BUSINESS INSIDER (Apr. 13, 2011), http://www.businessinsider.com/how-twitter-was-founded-2011-4.

[58] Nate Anderson, *Netflix Offers Streaming Movies to Subscribers*, ARS TECHNICA (Jan. 16, 2007), https://arstechnica.com/uncategorized/2007/01/8627/.

[59] NPRM ¶ 28.

> More generally, we seek comment on the relevance of this analysis. The definition of "information service" speaks to the 'capability' to perform certain functions. Is a consumer capable of accessing these online services without Internet access service? Could a consumer access these online services using traditional telecommunications services like telephone service or point-to-point special access? Or are we correct that offering Internet access is precisely what makes the service capable of "generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information" to consumers?[60]

This interpretation of the role ISPs play in a customer's online experience is so fundamentally alien to the standard conception of how the Internet works that a well-known April Fools' joke addresses precisely this question. On April 1, 1990, David Waitzman first proposed the famous "IP over Avian Carriers" protocol[61] (fully realized in 1999[62]). The protocol proposes exactly what its title suggests: that birds provide the same functionality that ISPs are expected to (albeit in a slightly faster and less error-prone manner), namely transmitting IP packets to and from destinations of the user's choosing. The humor in the joke is the fact that the Internet is so well-layered and oblivious to lower-level protocols that birds carrying messages could technically bring Internet functionality to end users. And lest it be argued that in reality only a broadband provider can provide access to online service, the Avian Carriers protocol was implemented in 2001.[63]

Humor aside, the technical answer to the NPRM's question is: yes, a consumer could access these services without broadband Internet access service.

---

[60] *Id.*

[61] David Waitzman, *A Standard for the Transmission of IP Datagrams on Avian Carriers*, RFC 1149 (Apr. 1, 1990), https://tools.ietf.org/html/rfc1149.

[62] David Waitzman, *IP over Avian Carriers with Quality of Service*, RFC 2549 (Apr. 1, 1999), https://tools.ietf.org/html/rfc2549.

[63] David Waitzman, *A Standard for the Transmission of IP Datagrams on Avian Carriers*, RFC 1149 (Apr. 1, 1990), https://tools.ietf.org/html/rfc1149.

To claim otherwise fundamentally misunderstands how the Internet works on a technical level.

As we explained before, offering access to the Internet is no more what makes BIAS capable of "generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information" than offering the ability to make telephone calls is what makes telephone service capable of having a pizza delivered to one's door in thirty minutes or less.

B. The NPRM Displays a Disturbing Lack of Knowledge of How Data is Routed on the Internet (and in the Telephone Network)

In addition to inaccurately portraying what services ISPs offer, the NPRM also gets basic facts wrong about how the technology underlying the Internet works. For example, in paragraph 10, the FCC seeks to imply that the 1998 Stevens Report is accurate in its conclusion that "Internet access providers do not offer a pure transmission path; they combine computer processing, information provision, and other computer-mediated offerings with data transport."[64] This is simply false, as we explain below.

> . . . Internet service providers do not appear to offer 'telecommunications,' i.e., '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,' to their users. For one, broadband Internet users do not typically specify the 'points' between and among which information is sent online. Instead, routing decisions are based on the architecture of the network, not on consumers' instructions, and consumers are often unaware of where online content is stored.[65]

Saying that Internet users do not specify the points to which information is sent online is like saying that telephone users do not specify the phone they want

---

[64] NPRM ¶ 10.

[65] NPRM ¶ 29.

their call sent to when they dial a phone number. As explained in Section I.D.2, both the Internet and the telephone network make use of dynamic routing based on the architecture of the network. Further, in both networks the customer is often unaware of where the endpoint is actually located—particularly in mobile networks, where a phone customer may have absolutely no way of knowing, a priori, even what country a mobile phone might be located in.

Thus, this interpretation of what it means to transmit information between or among points specified by the user, i.e. that the user must explicitly tell the network what routing decisions to take, has no basis in reality. Taken to its logical conclusion, it would require the FCC to similarly decide that telephone services are also not telecommunications services—an obviously absurd conclusion.

"Domain names must be translated into IP addresses (and there is no one-to-one correspondence between the two)." [66]

This is correct, and ISPs do indeed usually provide this service (i.e. DNS). However, as explained in Section II.C., ISP-provided DNS is by no means necessary, and ISPs are often not the best at providing the service. Users can and do change their DNS provider to lower round-trip latency and thereby have faster overall Internet service.[67]

"Even IP addresses may not specify where information is transmitted to or from because caching servers store and serve popular information to reduce network loads."[68]

Again, this is correct, but it does not have any bearing on the argument about classification one way or another. Further, as explained in Section II.B, caching

---

[66] *Id.*

[67] Young Xu, *2017 Update: Comparing the Performance of Popular Public DNS Providers*, THOUSAND EYES (May 15, 2017), https://blog.thousandeyes.com/comparing-performance-popular-public-dns-providers-2017/.

[68] NPRM ¶ 29.

services provided by an ISP without the assistance or involvement of a third-party are becoming increasingly rare, thanks to widespread encryption of web traffic.

"We believe that consumers want and pay for these functionalities that go beyond mere transmission—and that they have come to expect them as part and parcel of broadband Internet access service. We seek comment on our analysis."[69]

The NPRM is correct that consumers want and pay for these functionalities, i.e. routing. But the NPRM is incorrect when it says that routing is not part of mere transmission. To say that making routing decisions is not a necessary requirement for "mere transmission" implies the FCC is still living in a world where people dial a phone number by verbally asking an operator to connect them to a specific line. No modern telecommunications network, be it the PSTN or the Internet, requires (or could conceivably require) an end-point (including a BIAS customer) to know the details of how the network is laid out. Simply put, customers expect their ISP to route their traffic as "part and parcel of broadband Internet access service" *because it is a necessary functionality for the transmission of data in any modern network.*

"How are broadband Internet users' requests for information handled by Internet service providers today?"

Section I answers this question in detail; we refer the FCC to that section instead of reproducing it here.

"What functionalities beyond mere transmission do Internet service providers incorporate into their broadband Internet access service?"[70]

As explained in Sections II.B and II.C, ISPs provide caching and email services, but for quite some time these services have been declining in relevance.

> We particularly seek comment on the Title II Order's assertion that the phrase 'points specified by the user' is ambiguous—how should we

---

[69] NPRM ¶ 29.

[70] *Id.*

> interpret that phrase so that it carries with it independent meaning and is not mere surplusage? Is it enough, as the Title II Order asserted, for a broadband Internet user to specify the information he is trying to access but not the "points" between or among which the information will be transmitted? Does it matter that the Internet service provider specifies the points between and among which information will be transmitted?[71]

Even with caching, DNS, CDNs, anycast networks, or any other type of information optimization for the benefit of the network load or convenience, the user still has to specify the point where they expect to find the information. Though the point may be virtualized, it is a fundamental component of Internet architecture that requests require a destination point that they are attempting to set up a channel with. As explained in Section I.B, the user specifies the endpoints that they would like to communicate with, and the network is only responsible for transferring packets back and forth between the two.

Thus, an ISP no more specifies the points between which information will be transmitted when a user's browser issues an HTTP request to a specific IP address than a telephone company specifies the points between which information will be transmitted when a user's mobile phone speed-dials a specific phone number. In both cases, the user indicates the desired end-point for their communications and the network routes the communications appropriately to reach that end-point.

> Internet service providers routinely change the form or content of the information sent over their networks—for example, by using firewalls to block harmful content or using protocol processing to interweave IPv4 networks with IPv6 networks . . . . We seek comment on our analysis . . . . What constitutes a 'change in the form' of information? If not the protocol-processing for internetworking—considered an enhanced service under the Computer Inquiries—how should we

---

[71] *Id.*

interpret this phase so it carries with it independent meaning and is not mere surplusage?[72]

This analysis is fundamentally flawed and again shows a basic misunderstanding of how the Internet works. Changing the packet structure of an IP packet from IPv4 to IPv6 no more changes the form of the information contained within the packet (i.e. the payload) than taking a letter out of a FedEx envelope and putting it in a UPS envelope changes the form of the letter.

That's because when a customer sends an IP packet to their ISP, *they are not asking their ISP to transmit the IP packet itself, unchanged, to its destination.*[73] Rather, they are asking their ISP to transmit the *payload* of the packet—the data contained within the packet—to its destination unchanged. As we explained in Section I.C, the IP protocol resides at the "network" layer of the layered network communications model. When a device wishes to transmit data on a network, it takes that data, encapsulates it in a sequence of IP packets, and *then* transmits it (i.e. by passing it to the next layer down in the stack, where it will eventually be physically transmitted on the communications medium).

In other words, when a BIAS customer transmits an IP packet to their ISP, the customer is essentially telling the ISP, "Here is some data. I am sending it to you as the payload in an IP packet, since IP is the language our computers have agreed to use so that I can tell you where I want my data to go. I don't care if you repackage my data (the payload) using other protocols along the way, so long as you don't change the form of the payload itself. I need the payload to reach its destination unchanged, but I don't care how it gets there."

Examined in this way, it is obvious that customers *do not expect their ISPs to change the form or content of the data they entrust their ISPs to deliver*. Further,

---

[72] NPRM ¶ 30.

[73] Indeed, even without interweaving IPv4 and IPv6, the IP specification itself could not function if packets were required to be transmitted completely unchanged at each step—the IP protocol specifies that each time an IP packet is transmitted, the Time To Live (TTL) field must be decremented. *See* Information Sciences Institute, *DARPA Internet Program Protocol Specification*, (Sept. 1981), https://tools.ietf.org/html/rfc791.

most ISPs do not usually change the form or content of this data, because doing so would violate the end-to-end principle. Indeed it is considered malicious behavior to change payload data in-flight on the network, and the ability to do so is slowly being eradicated as Internet encryption grows more prevalent (see Section II.B, particularly Footnotes 25 and 26).

> How could we plausibly conclude that it is not a "change in the . . . content" to use of [sic] firewalls and other reasonable network management tools to shield broadband Internet users from unwanted intrusions and thereby alter what information reaches the user for the user's benefit? We seek comment on other ways in which Internet service providers change the form or content of information to facilitate a broadband Internet user's experience on line.[74]

Again, the NPRM displays a stunning lack of technical knowledge. Rather than changing content, a firewall blocks certain types of content based on the source, destination, or port (which might indicate what class of information the packet contains). Blocking potentially harmful connections does not change the form of any information—it simply prevents those connections from reaching the end user, and so long as it is done without objection by the user, certainly constitutes reasonable network management. This is very similar to how telephone networks address unwanted robocalls: the network provider determines what calls are likely to be unwanted based on information like the validity of the source phone number or the caller ID information and then blocks the call—without changing the form or content of the call.[75] Once again, followed to its logical conclusion, the NPRM's theory would require the FCC to reclassify the PSTN as an information service as well—an obviously ridiculous result.

---

[74] NPRM ¶ 30.

[75] Federal Communications Commission, *Notice of Proposed Rulemaking and Notice of Inquiry in the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls*, (Mar. 2, 2017), http://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0302/DOC-343731A1.pdf.

IV. The FCC Should Uphold the Light-Touch, Bright-Line Rules from the Open Internet Order

As developers, engineers, and designers, we realize that without openness and neutrality the Internet as we know it will cease to exist, because it is that openness and neutrality that gives the Internet its flexibility, leads to its growth, and has made it a vital resource for all aspects of modern life. Based on legal analysis done by others[76] we are concerned that if the FCC proceeds with this NPRM and reclassifies BIAS providers as information services, it will be unable to enforce the light-touch, bright-line rules the FCC promulgated as part of the 2015 Open Internet Order. We believe those light-touch rules are essential to the continued innovation and flexibility of the Internet. Thus the NPRM, if approved, would decimate the openness and neutrality that have contributed to the Internet's explosive growth over the past several decades. Further, service providers could *and would* revert to engaging in the practices of blocking, throttling, and interference. These practices would upend the Internet, making development of new protocols and services dramatically more difficult, breaking existing protocols and services, and even introducing security vulnerabilities that would not have been present without service provider interference. In short, if the current rules are not preserved, the rapid pace of innovation the Internet has experienced over the last forty years could come to a disastrous halt. We urge the Commission to reject the NPRM.

A. Risks of Approving the Rule as Proposed

We begin by elaborating on precisely what ISPs would be able to do in the absence of a clear and limited Open Internet rule. First and foremost, ISPs would be free to block, throttle, or speed up data based on its content, source, destination, or what service or application generated it. ISPs could degrade (or altogether block) certain protocols, content, or websites. A frequently given example is that of an ISP degrading traffic containing streaming movies from some or all edge providers, in order to encourage its customers to instead use its own media-

[76] *See, e.g., In re Restoring Internet Freedom*, WC Docket No. 17-108, Comments of the Electronic Frontier Foundation (July 17, 2017).

streaming service. But this sort of blocking and throttling would only be the tip of the iceberg. ISPs could go further, degrading traffic for any service they do not recognize or have not previously approved of.

That, in turn, could violate the principle of openness upon which the Internet was built. Developers would have to ensure that their new application or protocol would work under different specifications on each of the thousands of networks that make up the Internet. Some networks might decide to handle data differently depending on whether it represents webpages or video. Others might decide to prioritize certain data.[77] Such a haphazard mishmash of different specifications and engineering conditions would have made the growth of the Internet as we know it utterly impossible. Instead, it would have resulted in a balkanized Internet—one in which each ISP was its own private fiefdom, where edge providers had to negotiate with the gatekeeper in order to get access to the end users.

But blocking and throttling are not the only dangers. ISPs could decide to violate the end-to-end principle, inserting nodes in their network that tried to "enhance" their customers' experience by augmenting or transforming some content. This might seem like a reasonable design, since conceivably an ISP might have access to information that edge providers would not. For example, an ISP might be able to provide more relevant search results or other information since it has a complete record of its customers' unencrypted browsing histories. But this sort of interference could not only introduce bugs into services and webpages that weren't expecting it, it could make it impossible for some applications (including applications yet to be dreamed of) to work correctly. Worse yet, it could also

---

[77] It is worth noting that the Internet Protocol does specify a field in the header of IP packets known as the "differential service" field, meant to indicate some sort of priority. However, in the over thirty years since the widespread adoption of IP, no consensus has been reached about how edge devices should populate that field for use on the public Internet (as opposed to within private networks, such as a company's LAN). As a result, traffic prioritization on the *public* Internet is almost nonexistent. The closest the Internet engineering community has come to a standard on prioritization is RFC 2474, which is a proposed standard last updated in 1998, and which has not seen widespread adoption. K. Nichols et al., *Definition of the Differentiated Services Filed (DS Field) in the IPv4 and IPv6* Headers, THE INTERNET SOCIETY (Dec. 1998), https://tools.ietf.org/html/rfc2474.

introduce security vulnerabilities which a malicious actor could use to harm the ISP's customers.

If ISPs could engage in this sort of blocking, throttling, and interference (which would no doubt occur in the absence of the light-touch, bright-line rules in the Open Internet Order), it would transform the Internet from a permission-less environment (in which anyone can develop a new app or protocol and deploy it confident that the Internet treats all traffic equally) into one in which developers would first need to seek approval from or pay fees to ISPs before deploying their latest groundbreaking technology. Developers and engineers would no longer be able to depend on the core assumption that the Internet will treat all data equally. The sort of rapid innovation the Internet has fueled for the past two decades would come to a sudden and disastrous halt.

B. Concrete Examples of Consumer Harm in the Absence of Bright-Line Rules

These sorts of threats to the Internet's openness and neutrality are real. None of the scenarios described in the previous section are hypothetical. In this section, we elaborate on nearly a dozen different examples of consumer harm by ISPs that chose to block, throttle, or otherwise interfere with their paying customers' traffic. We hope that this section will help answer the following question from the NPRM:

> We also seek comment on specific ways in which consumers were harmed under the light-touch regulatory framework that existed before the Commission's Title II Order. Much of the Title II Order focused extensively on hypothetical actions Internet service providers "might" take, and how those actions "might" harm consumers, but the Title II Order only articulated four examples of actions Internet service providers arguably took to justify its adoption of the Internet conduct standard under Title II . . . . Is there evidence of actual harm to consumers sufficient to support maintaining the Title II telecommunications service classification for broadband Internet

access service? Is there any evidence that the likelihood of these events occurring decreased with the shift to Title II?[78]

We begin with the four examples described in the Open Internet Order.

1. Examples of Consumer Harm from the Open Internet Order

First, in 2005, the FCC found that Madison River, a BIAS provider based in North Carolina, had been blocking Voice over Internet Protocol (VoIP) ports, thereby preventing its customers from making use of third-party VoIP services. This example of consumer harm is particularly egregious, given that "[f]or those customers who had disconnected their traditional phone lines and were relying solely on Vonage, the blocking meant they had no ability to make calls, even to emergency 911 services."[79] Had the Open Internet Order's light-touch rule against blocking been in place back in 2005, Madison River's customers might not have been put in life-threatening situations.

Second, Comcast has interfered with legitimate traffic based solely on its type. In 2007, the Electronic Frontier Foundation (EFF) confirmed reports that "Some time around May 2007, Comcast installed new software or equipment on its networks that began selectively interfering with some of Comcast customers' TCP/IP connections. The most widely discussed interference was with certain BitTorrent peer-to-peer (P2P) file-sharing communications, but other protocols" were also affected.[80] This interference went far beyond network management, and affected its customers' ability to download public domain works, not to mention properly use non-P2P software like Lotus Notes.

---

[78] NPRM ¶ 50.

[79] Jonathan Krim, *Phone Company Settles in Blocking of Internet Calls*, THE WASHINGTON POST (Mar. 4, 2005), http://www.washingtonpost.com/wp-dyn/content/article/2005/03/25/AR2005032501328.html (last visited July 14, 2017.

[80] Peter Eckersley et al., *Packet Forgery By ISPs: A Report on the Comcast Affair,* ELECTRONIC FRONTIER FOUNDATION (Nov. 28, 2007), https://www.eff.org/wp/packet-forgery-isps-report-comcast-affair (last visited July 14, 2017).

Third, in 2012, AT&T chose to block data sent to and from users of Apple's Facetime software.[81] In particular, AT&T announced in August of 2012 that only certain, more expensive data plans would be able to use Facetime, acknowledging explicitly that "the company was using it as a lever to get users to switch over to the new plans which charge for data usage in tiers."[82] In other words, customers were forced to pay more to AT&T to send or receive certain types of data, based on a business decision by AT&T.

Fourth, in 2012, Comcast announced that it would favor its own video-on-demand streaming services over third-party competitor services, by charging customers for the data they used to stream competitor services.[83] In this instance, customers were harmed by Comcast's decision to take advantage of its gatekeeper power to favor its traffic over its competitors, thereby clearly distorting the marketplace for video-on-demand services.

2. Further Examples of Consumer Harm That Could Have Been Prevented by The Light-Touch, Bright-Line Rules in the Open Internet Order

Contrary to what the NPRM suggests, the number and variety of concrete incidents in which customers have been harmed by ISP behavior goes far beyond "the few, scattered anecdotes cited by the Title II Order."[84] There have indeed "been additional, concrete incidents that threaten the four Internet Freedoms sufficient to warrant adopting across-the-board rules,"[85] and we describe several of them here.

---

[81] David Kravets, *AT&T: Holding Facetime Hostage Is No Net-Neutrality Breach*, WIRED (Aug. 22, 2012, 2:24 PM), https://www.wired.com/2012/08/facetime-net-neutrality-flap/ (last visited July 14, 2017).

[82] *Id.*

[83] Kyle Orland, *Comcast: Xbox 360 On Demand Streams Won't Count Against Data Caps*, ARS TECHNICA (Mar. 26, 2012, 11:54 AM), https://arstechnica.com/gaming/2012/03/comcast-xbox-360-on-demand-streams-wont-count-against-data-caps/ (last visited July 14, 2017).

[84] NPRM ¶ 77

[85] *Id.*

i. AT&T's Problematic Zero-Rating

Similar to how Comcast decided to favor its own video-on-demand services, other carriers have chosen to distort the market and give their own video services an unfair advantage as well. First, AT&T has decided not to charge customers for data used by its DIRECTV content, while charging third-parties more to similarly zero-rate data. The FCC's own investigation found that "AT&T offers Sponsored Data to third party content providers at terms and conditions that are effectively less favorable than those it offers to its affiliate, DIRECTV. Such arrangements likely obstruct competition for video programming services delivered over mobile Internet platforms and harm consumers by inhibiting unaffiliated edge providers' ability to provide such service to AT&T's wireless subscribers."[86]

ii. Verizon's Problematic Zero-Rating

Similarly, Verizon also did a disservice to its customers by zero-rating its own content via its go90 program, while charging third-parties more to zero-rate data through its FreeBee Data 360 program. As the FCC's report explained, Verizon had "no safeguards that would prevent Verizon from offering substantially more costly or restrictive terms to enable unaffiliated edge providers to offer services comparable to Verizon's go90 on a zero-rated basis."[87]

In both of these cases, the consumer harm is identical to the Comcast case—an ISP distorts the market for content by using its gatekeeping power to favor some content over others, thereby depressing investment in content by third-parties and reducing the choices available to their customers.

---

[86] Wireless Telecommunications Bureau, Policy Review of Mobile Broadband Operators' Sponsored Data Offerings for Zero-Rated Content and Services 13, https://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0111/DOC-342982A1.pdf.

[87] *Id.*

iii. Search Redirection by More Than Half a Dozen ISPs

In August of 2011, researchers at the International Computer Science Institute published research showing that a number of ISPs, including Cavalier, Cogent, Frontier, Fuse, DirecPC, RCN, and Wide Open West, were rerouting their customers' search queries to a third-party company, Paxfire, which in some cases then sent users to websites they did not request, instead of on to the search engine the user expected. As an EFF blog post at the time explained,

> [T]he purpose appears to be monetization of users' searches. ICSI Networking's investigation has revealed that Paxfire's HTTP proxies selectively siphon search requests out of the proxied traffic flows and redirect them through one or more affiliate marketing programs, presumably resulting in commission payments to Paxfire and the ISPs involved. The affiliate programs involved include Commission Junction, the Google Affiliate Network, LinkShare, and Ask.com. When looking up brand names such as "apple", "dell", "groupon", and "wsj", the affiliate programs direct the queries to the corresponding brands' websites or to search assistance pages instead of providing the intended search engine results page.[88]

The consumer harm is obvious: consumers' data was being shared with third-parties they had never heard of, and their web searches were being rerouted without their permission.

iv. AIO and Cricket Wireless Stripping Encryption

In September 2013, an engineer for the VPN company Golden Frog noticed that he was unable to send email securely because his wireless provider (AIO Wireless, which then merged with Cricket Wireless) was stripping the encryption off his connections to mail servers.[89] Once again, the consumer harm here is

---

[88] Christian Kreibich et al., *Widespread Hijacking of Search Traffic in the United States*, ELECTRONIC FRONTIER FOUNDATION (Aug. 4, 2011), https://www.eff.org/deeplinks/2011/07/widespread-search-hijacking-in-the-us.

[89] *The FCC Must Prevent ISPs from Blocking Encryption*, GOLDEN FROG (Nov. 4, 2014), https://www.goldenfrog.com/blog/fcc-must-prevent-isps-blocking-encryption.

particularly egregious: an ISP decided that its customers didn't deserve security and privacy when sending emails, and so prevented their customers from making encrypted connections when attempting to send email.

v. Comcast Potentially Introducing Vulnerabilities into its Customers' Web Browsing

In August of 2014, Comcast admitted that it was modifying its customers' web-browsing traffic without their consent by inserting ads into the webpages its customers view.[90] EFF senior staff technologist Seth Schoen discussed the matter with a journalist at the time. "Even if Comcast doesn't have any malicious intent, and even if hackers don't access the JavaScript, the interaction of the JavaScript with websites could 'create' security vulnerabilities in websites,"[91] Schoen said. "Their code, or the interaction of code with other things, could potentially create new security vulnerabilities in sites that didn't have them." Security expert Dan Kaminsky explained further in an e-mail that JavaScript injection has the potential to break "all sorts of stuff, in that you no longer know as a website developer precisely what code is running in browsers out there. You didn't send it, but your customers received it."[92]

In other words, the consumer harm was that by modifying its customers' web traffic, Comcast could inadvertently introduce security vulnerabilities that would put its customers at risk.

---

[90] David Kravets, *Comcast Wi-Fi Serving Self-Promotional Ads Via JavaScript Injection,* ARS TECHNICA (Sept. 8, 2014, 5:00 AM), http://arstechnica.com/tech-policy/2014/09/why-comcasts-javascript-ad-injections-threaten-security-net-neutrality/.

[91] *Id.*

[92] *Id.*

vi. Verizon Adding Super-Cookies to its Customers' Web Traffic

Verizon has also admitted to modifying its customers' traffic without their consent by inserting unique tracking ID numbers into the data its customers send.[93] In this case, the modification of customer traffic allowed third-parties to track Verizon's customers as they browsed the web, even if those customers made efforts to ensure their privacy (e.g. by clearing cookies or using Incognito or Private Browsing Mode).[94] Here, the consumer harm was that customers' attempts to control what information they shared about their browsing history were being completely overruled and ignored by their ISP, via a method the customer had no control over.

vii. T-Mobile Throttling Video Traffic Even When the Network was Uncongested

In January of 2016, EFF research showed that, as part of the company's "Binge On" program, T-Mobile was throttling its customers' video data without regard to congestion, indicating that the practice had nothing to do with reasonable network management. In particular, EFF found,

> [W]hen Binge On is enabled, T-Mobile throttles all HTML5 video streams to around 1.5Mps, even when the phone is capable of downloading at higher speeds, and regardless of whether or not the video provider enrolled in Binge On. This is the case whether the video is being streamed or being downloaded—which means that T-Mobile is artificially reducing the download speeds of customers with Binge On enabled, even if they're downloading the video to watch later. It also means that videos are being

---

[93] Jacob Hoffman-Andrews, *Verizon Injecting Perma-Cookies to Track Mobile Customers, Bypassing Privacy Controls,* ELECTRONIC FRONTIER FOUNDATION (Nov. 3, 2014), https://www.eff.org/deeplinks/2014/11/verizon-x-uidh.

[94] Jacob Hoffman-Andrews, *How Verizon and Turn Defeat Browser Privacy Protections*, ELECTRONIC FRONTIER FOUNDATION (Jan. 14, 2015), https://www.eff.org/deeplinks/2015/01/verizon-and-turn-break-browser-privacy-protections.

throttled even if they're being watched or downloaded to another device via a tethered connection.[95]

Here, the consumer harm was that T-Mobile was artificially throttling its customers' video downloads, even when there was no benefit to customers (i.e. the download was not zero-rated). Additionally, T-Mobile lied to its customers about how the Binge On program worked, claiming that T-Mobile itself was somehow "optimizing" streaming video, when T-Mobile had in fact not deployed any technology that altered the video stream in any way except for slowing it down.

C. More General Harms to Internet Innovation That Have Occurred Due to ISP Blocking, Throttling, and Interference

Beyond the specific examples cited above, port blocking and interference by ISPs in general have forced developers of new protocols and services to "camouflage" their new protocols as existing ones, in order to avoid discriminatory treatment. In fact, this sort of interference has become so bad that network engineers have developed a name for it: the "ossification" of the network stack.[96] As a result of this interference, development of innovative new protocols and services is already being hindered.[97]

D. Concrete Examples of Consumer Benefit Since the Open Internet Order Took Effect

In addition to asking for examples of consumer harm that could have been prevented by the light-touch, bright-line rules in the Open Internet Order, the NPRM also asks what, if any, changes have been

---

[95] Jeremy Gillula, *EFF Confirms: T-Mobile's Binge on Optimization is Just Throttling, Applies Indiscriminately to All Video*, ELECTRONIC FRONTIER FOUNDATION (Jan. 4, 2016), https://www.eff.org/deeplinks/2016/01/eff-confirms-t-mobiles-bingeon-optimization-just-throttling-applies.

[96] *See, e.g.*, IAB Workshop on Stack Evolution in a Middlebox Internet (SEMI) Report (B. Trammell & M. Kuehlewind eds., July 22, 2015), https://tools.ietf.org/html/draft-iab-semi-report-01.

[97] Michio Honda et al., *Is it Still Possible to Extend TCP*?, ACM INTERNET MEASUREMENT CONFERENCE 181 (2011), http://nrg.cs.ucl.ac.uk/mjh/tmp/mboxes.pdf.

> made as a result of Title II reclassification that have had a positive impact on consumers? Was Title II reclassification necessary for any of those changes to occur? Is there any evidence, for example, that consumers' online experiences and Internet access have improved due to policies adopted in the Title II Order?[98]

There are two obvious examples of concrete changes in ISP behavior as a result of the Open Internet Order that have benefited consumers, separate from the prevention of harms described above.

First, prior to the Open Internet Order, many ISPs forbade their customers from attaching non-harmful devices to the network, thereby restricting how customers could use their Internet connections. The most prominent example of this is that prior to the Open Internet Order, many mobile broadband providers forbade their customers from tethering personal computers to their mobile devices in order to use their mobile broadband connection. However, since the Open Internet Order, that prohibition has disappeared from the terms of service of many mobile broadband providers (including Sprint[99] and T-Mobile[100]).

Similarly, prior to the Open Internet Order, many ISPs forbade their customers from using certain applications based on their type, without regard to whether or not the network was congested or the customer had purchased sufficient bandwidth or a high enough data cap to support their use. For example, as of July

---

[98] NPRM ¶ 51

[99] *Compare Sprint Terms & Conditions*, SPRINT (archived from Jan. 23, 2015) https://web.archive.org/web/20150123055809/https://shop2.sprint.com/en/legal/os_general_terms_conditions_popup.shtml (last visited July 14, 2017), *with Sprint Terms Conditions*, SPRINT (Archived from Sept. 5, 2015), https://web.archive.org/web/20150905132630/https://shop2.sprint.com/en/legal/os_general_terms_conditions_popup.shtml (last visited July 14, 2017)

[100] *Compare T-Mobile Terms & Conditions*, T-MOBILE (Nov. 10, 2014), https://www.t-mobile.com/templates/popup.aspx?PAsset=Ftr_Ftr_TermsAndConditionsNov2014 (last visited July 14, 2017) *with T-Mobile Terms & Conditions*, T-MOBILE (Sept. 1, 2016), https://www.t-mobile.com/Templates/Popup.aspx?PAsset=Ftr_Ftr_TermsAndConditions&print=true#EPPUSYD (last visited July 14, 2017).

2014, T-Mobile forbade its customers from using P2P services or using their service for "continuous Web camera posts or broadcasts."[101] However, as of July 2017, that prohibition no longer exists.[102] Similarly, prior to the Open Internet Order, Sprint forbade its customers from using their Internet access for certain activities (such as web hosting or "maintain[ing] continuous active network connections to the Internet such as through a web camera").[103] However, shortly after the publication of the Open Internet Order, those prohibitions were removed.[104]

In both cases, the benefit to customers is clear. Prior to the Open Internet Order, the range of things a customer could do with her broadband Internet connection was dictated by business decisions made by her ISP—not by the actual technical capability of the network or whether the network was suffering from congestion. Thanks to the Open Internet Order, this is no longer the case—ISPs are now prohibited from discriminating against certain types of uses, and customers can use their broadband connections for a wider variety of applications, thus encouraging further innovation in the Internet ecosystem.

V. Conclusion

While we appreciate the FCC's desire to accurately classify BIAS providers, the theories posed and the questions asked by the NPRM indicate a tremendous lack of technical understanding on the part of its authors. We remain concerned that any decision to reclassify based on this lack of technical understanding could

---

[101] *T-Mobile Terms & Conditions*, T-MOBILE (Nov. 10, 2014), https://www.t-mobile.com/templates/popup.aspx?PAsset=Ftr_Ftr_TermsAndConditionsNov2014.

[102] *T-Mobile Terms & Conditions*, T-MOBILE (Sept. 1, 2016), https://www.t-mobile.com/Templates/Popup.aspx?PAsset=Ftr_Ftr_TermsAndConditions&print=true#EPPUSYD.

[103] *Sprint Terms & Conditions*, SPRINT (archived from Jan. 23, 2015) https://web.archive.org/web/20150123055809/https://shop2.sprint.com/en/legal/os_general_terms_conditions_popup.shtml (last visited July 14, 2017).

[104] *Sprint Terms Conditions*, SPRINT (Archived from Sept. 5, 2015), https://web.archive.org/web/20150905132630/https://shop2.sprint.com/en/legal/os_general_terms_conditions_popup.shtml (last visited July 14, 2017).

have dangerous consequences, including stifling future innovation and depressing future investment in the wealth of Internet services that drive such a large part of the U.S. economy.

Furthermore, based on the above examples, coupled with our collective knowledge and experience in designing, building, and operating various parts of the Internet ecosystem, it is clear to us that if the FCC were to reclassify BIAS providers as information services, and thereby put the bright-line, light-touch rules from the Open Internet Order in jeopardy, the result could be a disastrous decrease in the overall value of the Internet. Fortunately, the current rules that the FCC operates under will effectively prevent this worst-case scenario from occurring, so long as the NPRM is not approved.

That is why we, the undersigned computer scientists, network engineers, and Internet professionals, based on our technical analysis and an understanding of both how the Internet was designed, and how it currently functions, respectfully encourage the FCC not to adopt the Notice of Proposed Rulemaking – WC Docket No. 17-108.[105]

Respectfully submitted,

Aaron L. Jones, Phoenix Linux Users Group - Lead Security Instructor / Mesa Community College Adjunct Professor / Software Developer Chandler Arizona Police Department

Aaron Rabinowitz, IT Consultant, EFF Member.

Aaron Zuehlke, Sr IT Security Risk Analyst

Akbar Kara

Alex Payne, independent software engineer and investor

[105] Unless otherwise noted, all of the signatories to this letter have signed in their personal capacity, and not as representatives of their employers or any affiliated organizations.

Alexander Johns, Software Developer, PacificSource Health Plans

Alfred Ganz, network infrastructure consultant (retired)

Alisa Peters, Principal Engineer, 60dB

Allen Cook, Founder & CEO, TOURtech

Andrew Gallo, Principal IT Architect

Andrew J. Ferguson, Professional Engineer

Andrew Joseph Klosterman, PhD, Advanced Technology Group, Office of the CTO, NetApp, Inc.

Andrew McConachie, Internet Infrastructure Engineer

Andrew Nusbaum, Principal Network Engineer, IAC Applications

Andrew Wolfe, Ph.D., Santa Clara University

Andy Sayler, Security Engineer, Twitter

Ash Doyle, Datacenter Team Lead, Kapstone Paper and Packaging

Aviel D. Rubin, Professor of Computer Science; Technical Director, Information Security Institute, Johns Hopkins University

Barbara A. Cherry, Professor, The Media School, Indiana University

Ben Kamen, Ben Kamen Consulting - IT Consulting / Embedded Systems Design and Prototyping

Ben Mobley, Technology Security Officer, Colonial Group International

Ben Tobin, Software Development Manager, Amazon

Ben Turner, Senior Staff Engineer, Silk Labs, Inc.

Benjamin "Gonzo" Granzeau, Lead Systems Engineer, Bluepay Processing

Bob Frankston, Technologist

Brandon Ross, CEO and Chief Network Architect, personally and on behalf of Network Utility Force

Brewster Kahle, Founder, Internet Archive; Member, ISOC Internet Hall of Fame

Brian Behlendorf, Executive Director of Hyperledger, at the Linux Foundation; Chairman of the Board, Electronic Frontier Foundation

Brian G. Coffey, Technology Consultant, Security Researcher, Ethical Hacker

Brian Kernighan, Professor of Computer Science, Princeton University

Bruce Schmoetzer, CEO & Chief Network Architect, Wilke Systems Intl, Inc.

Bruce Schneier, Fellow and Lecturer, Harvard Kennedy School of Government; Fellow, Berkman-Klein Center for Internet and Society

C. Lee Davis, DevOps Manager, Fabric.com

Calin Culianu, Software Engineer & Founder, C3 Software

Casey Boardman, Senior Testing Infrastructure Engineer, The MathWorks

Chip Rosenthal, Staff Engineer with a major manufacturer in broadband sector

Chris Bacon, Systems Analyst

Chris Raters, Lead Technologist, BAH

Chris Stover, Senior Programmer, Department of Finance

Christine McQuie, Senior SQL Analyst/DBA, Maryville University

Christopher Boyd, IP Networking Consultant

Christopher Jansen, Director of Development, Bluepay, Inc.

Cliff Sojourner, IP Networking Engineer

Cory Francis Myers, Network Architect, Trinity Mobile Networks

Dan McTeer, Manager, Information Security Services, Adobe Systems, Inc.

Dan S. Wallach, Professor, Department of Computer Science, Rice University; Rice Scholar, Baker Institute for Public Policy

Dan Schlitt, PhD, Retired Internet Manager, City College of New York

Dan Steinberg, SYNTHESIS:Law & Technology

Dan Weinand, Head of Development, ValiMail

Daniel J Grim, II, Chief Technology Officer, University of Delaware

Dave Brockman, Senior Network Engineer, Networks Inc.

David A Smith, CEO/Founder CEO.Vision

David J. Farber, Alfred Fitler Moore Emeritus Professor of Telecommunication, University of Pennsylvania

David Peters, Director of Engineering, Zillow Group

David S. H. Rosenthal, Ph.D., Stanford University (retired)

David Xia, Software engineer

Devon H. O'Dell, Senior Software Engineer, Fastly

Doug Lewis, Director of Engineering, Zillow Group

Dr Andrew Tridgell, Visiting Fellow, Department of Computer Science, Australian National University

Dr. Gregory Glockner, Vice President of Engineering, Gurobi Optimization

Dr. Horst Tebbe, Former Member of Technical staff at Bell Labs

Eamonn O'Brien-Strain, Software Engineer, Google

Ed Lazowska, Bill & Melinda Gates Chair in Computer Science & Engineering, University of Washington

Eleanor Saitta, Security Architect

Eli Davis, Information Security Engineer

Evan Sanders, Lead Site Coordinator / Network Engineer

Fred Posner, Network Engineer, The Palner Group Inc.

Frederick P. Brooks, Jr.; Kenan Professorof Computer Science, Emeritus, University of North Carolina at Chapel Hill, Fellow IEEE, Fellow ACM, recipient, National Medal of Technology.

Frederik Braun, Senior Security Engineer at Mozilla

Gabe Cole, CEO, RTE Group, Inc.

Gabe Goldberg, Member, Board of Advisors, Association of Personal Computer User Groups (APCUG)

Gary Cohn, Network Engineer

George Yanos, retired programmer

Gordon Jacobson, Former Network Operations Center Manager, iRamp.com

Gray R. Capo, President, R3ality Inc.

Hal Murray, retired network engineer and ARPANET veteran

Harold Sinclair, Systems Infrastructure and Security Engineer, New York, NY

Hugo Maxwell Connery, Network Administrator, Technical University of Denmark; participant in the DNS Operations, DNS Private Exchange, and Pervasive Passive Surveillance IETF Working Groups

James D. Guyton, Network Software Developer

James Graebner, Network Engineer, Charter Communications

James L. Doty, Ph.D. - retired

James Renken, Managing Member, Sandwich.Net, LLC

Jamie Lawrence, Systems Engineer

Jared Moore, Masters Student, UW School of Computer Science

Jason R. Archip, KD5LCT

Jean Yang, Assistant Professor, Computer Science Department, Carnegie Mellon University

Jeff Harlan, Senior Performance Engineer, Oath: (formerly Yahoo!)

Jeff Skaistis, VP of Systems Architecture, Logistyx Technologies.

Jeremy Mill, Software Engineer

Jesse Rodriguez, Cybersecurity Analyst

Jill Rouleau, Cloud Reliability Engineer, Canonical

Jim DeLeskie, founder, Mimir Networks

Jim Killinger, President, BulletData, a J.D. Killinger Company

Joe Hamelin, Network Engineer, FCC call sign W7COM

John Aho, Software Developer

John Bartas, Senior Software Engineer, Fortinet, Inc.

John Carbone, Managing Partner, Bonify

John Larkin, Senior Staff Engineer, Qualcomm Inc.

John Romero, Programmer and Game Designer, Romero Games Ltd.

John Souvestre, Founder, Southern Star ISP

Jonathan David Arndt, Programmer

Jonathan Poritz, Associate Professor of Mathematics, Colorado State University - Pueblo

Jonathan Rynd, Vice President of Software Development, Savvysoft

Joseph Clofine, Sr. Manager Product Development, Comcast Cable

Josh Maida, Partner and Director of New Product Development, personally and on behalf of Six Foot, LLC.

Joshua Bloch, Professor of Computer Science, Carnegie Mellon University; author, "Effective Java"; former chief Java Architect, Google; Former Distinguished Engineer, Sun Microsystems

Joshua Colvin, Software Engineer

Joshua Cox, Systems Administrator

Joshua Turton, Senior Developer, Phase2

Judith Turner, editor emerita, The Journal of Electronic Publishing

Julian Macassey, Telecommunications engineer

Justin Findlay, Software Engineer

Karl O. Pinc, President, The Meme Factory, Inc.

Kenneth Lerman, Director of Engineering, Mark Kenny Products Company, LLC

Kraig Beahn, CTO/CEO, Enguity Technology Corp

Lance Cleghorn, Cyber Security Researcher

Lester Earnest, Senior Research Computer Scientist Emeritus, Stanford University

Lonnen, Staff Engineer, Mozilla

Lorna Mitchell, Developer Advocate, IBM

Marcello Velasquez, Solutions Analyst, Nonpublic

Mark Richter, Senior Staff Engineer, Solarflare Communications

Mark Seiden, Security Advisor to Internet Archive, member of ICANN Security and Stability Advisory Committee

Matt Bishop, Professor, Department of Computer Science, University of California at Davis

Matt Dunlap, Autonomous Car Engineer, Optimus Ride

Matthew Douglass, Co-Founder, Practice Fusion

Matthew Kraai, Developer, Debian

Micah Lee, Security Engineer, First Look Media

Michael Grant, Networking Professional

Michael March, iOS Engineer, 60dB

Michael McCormick, Founder & President, Taproot Security

Michael Meyer, Senior Systems Specialist

Micheal Sherrill, Owner, Homegeeks IT Services

Mike Lyon, CEO, Ridge Wireless, Inc.

Mitch Kapor, Partner, Kapor Capital

Neil Hunt, Ex Chief Product Officer, Netflix

Nicholas Lesiecki, Independent Software Consultant, former Google Engineer, former White House Software Engineer

Nicholas Oas, Network Security Engineer

Nicholas Schrag, Senior Engineer for client-side development of free-to-play mobile games

Nick Critser, Senior Developer, Pershing LLC

Nickolas Christopher, Technology Specialist

Patrick Koppula, www.innovatingUSA.org

Paul Corriveau, Principal, Code Zero One

Peter Fonash, Senior Systems Engineer

Peter G. Neumann, Senior Principal Scientist, SRI International Computer Science Lab

Phil Budne, Contract Programmer, Former IETF

Representative

Plato Gonzales, Blockchain Engineer and Electrical Engineer

Professor Douglas Comer, Distinguished Professor of Computer Science, Purdue University

Professor Nick McKeown, Professor of Electrical Engineering and Computer Science, Stanford University; Member, National Academy of Engineering; Member, American Academy of Arts and Sciences

Professor Scott Shenker, Professor in Electrical Engineering and Computer Sciences Department, University of California-Berkeley; Member, National Academy of Engineering

Randy Burton, Principal Consultant, CrowdStrike

Randy Bush, Research Fellow, Internet Initiative Japan

Raven Alder, Chief Technology Officer, Electronic Rights Rainier

Ray Charbonneau, ReallyFixIt.com

Rich Kulawiec, Senior Internet Security Architect, Fire on the Mountain

Richard Chen, Undergraduate in Computer Science, Stanford University

Robert Oliver, Sr. Solution Architect, Dassault Systèmes

Robert Schulman, PMTS, AMD

Ron Teitelbaum, CEO - Head of Engineering, 3D Immersive Collaboration Consulting

Ronald Larsen, Dean and Professor, School of Information Sciences, University of Pittsburgh

Roxanne Gentile, Technology Director

Rusty D. Pickens, Former Senior Advisor for Digital Platforms, U.S. Department of State

Sahle A. Alturaigi, Full-stack web developer, Almarai

Sarah Allen, Program Director, Bridge Foundry; 2013 Presidential Innovation Fellow

Scotty Allen, Chief Technology Officer, Strange Parts; Member, Noisebridge Hackerspace; former Software Engineer, Google

Sean Bastille, Chief Architect, Oath

Shannon McElyea, Strategic Alliances, IMCI Technologies

Shaun Houlihan, Software Engineer, Pindrop Security

Shaun Michelson, Systems Administrator, Apple Hospitality REIT, Inc.

Stefano Zanero, Chair, Cybersecurity STC, IEEE Computer Society

Stephen D. Crocker, CEO, Shinkuro, Inc.

Steve Bauer, Systems Software Specialist, SDSMT

Steve Holton, 20+year telecommunications engineer

Steve Piercy, Web Application Developer

Theodore Randolph, Software Engineer, Cisco Systems

Thomas Chappelow, Director, Nimbox

Tim Pozar, Principal at TwoP LLC

Timothy McGinnis, Internet logical infrastructure consutant

Timothy Spannaus, PhD, Senior Lecturer, Learning Design and Technology, Wayne State University, Detroit, USA

Tom Lyon, Chief Scientist, DriveScale Inc.

Tom Ritter, Staff Engineer, Mozilla

Travis Taylor, Network Administrator w/Sumner Regional Medical Center & Tech Hobbyist/Amateur Radio Operator N0NEK

Trevor M. Reed, M.S., Cyber Security Incident Responder, General Electric

Tyler Lawrence, VP of Infrastructure, Sierra Microproducts Inc.

Vint Cerf, Internet Pioneer

W. Falcon Street, Chief Information Security Officer, State of Florida DEO

William Bourdo, Systems Administrator, Six Foot LLC

William Keeley, Owner B.C.E.

William R. Patterson, MBA, MS (Computer Science), Retired

Wing Cheong Lau, Associate Professor, The Chinese University of Hong Kong

Youssef Mahmoud, CTO, EpiphyteOne

Zachary S. Tschirhart, Scientific Applications Research Scientist, AMD