CCTV Center for Media and Democracy | Burlington VT

Testimony to Energy & Telecommunications

Andrew B. Crawford, acrawford@cctv.org, 802-324-1915

21 March 2018

H 680: An act relating to protecting consumers and promoting an open internet in Vermont

Hello,

Thank you for allowing me to offer my testimony with regard to H.680. I would like to address two sections of the bill with my testimony, specifically 8204 and 8205.

> In (Section 8204) H.680, as introduced, starting on page 11 line 14 through page 13 line 3 a number of CERTIFICATE CRITERIA; PRACTICES PROHIBITED; REQUIRED DISCLOSURES are enumerated.
>
> In (Section 8205) H.680, as introduced, starting on page 13 line 4 through page 15 line 2 a number of COMMISSION RULES are enumerated.

Internet access is used like a multi-purpose utility, and I believe it should be classified as such. I believe that there are many reasons to support net neutrality, and I am in favor of regulation to

classify violations of net neutrality provisions as a violation of consumer protection against unfair and deceptive act in trade and commerce.

The goal of this legislation should be to enable broad innovation on top of the Autonomous System (AS) networks that make up the Internet while preserving equity of access to internet resources and performance. The legislation should also not legislate certain types of network management or a specific technical architecture, as that can stifle adaptability and innovation within and between provider networks.

The foundation of the Internet is the TCP/IP protocol suite and the additional application protocols that run on the Network / Internet Layers. My testimony will be related to some of the challenges related to enforcement of the PRACTICES PROHIBITED, not to the merits of implementing net neutrality consumer protection provisions.

The legislation does give flexibility with respect to required disclosures. It also provides for a crucially important initial certification process for the provider, a complaint protocol, and leeway for the Commission to develop additional protocols for handling complaints. These are all valuable components.

I have a number of concerns about the ability to enforce these rules and the potential unintended consequences of the current legislation as proposed. The rules set a high bar for determining that there is purposeful action on the part of providers to “degrade or impair” service based on “content, application, service, or device”. In cases of enforcement it will be a necessary to have measurements that allow the Commission to:

A. Evaluate the character and performance of the route between two “Edge providers” or “Persons” attempting to establish or having established a connection using the TCP/IP protocol suite.

B. Evaluate the character and performance of higher Layer protocol traffic that is encapsulated and routed between two “Edge providers” and/or “Persons” attempting to connect or having established a connection using the protocol in question.

C. Have an understanding of the historical statistical performance of comparable routes between two “Edge providers” and/or “Persons” connected or attempting to connect using the TCP/IP protocol suite.

D. Have an understanding of the historical statistical performance of the higher Layer protocols in use between two “Edge providers” and/or “Persons” connected or attempting to connect.

Items A through D deal with the necessity to measure changes in the character and performance of the service provided to the “Edge provider” or “Persons”. This requires a significant effort at data collection and processing on behalf of the entity filing a complaint (customer), and more importantly, a set of third party background measurements from which the entity filing a complaint can prove a deviation in their case. There are some successful studies of baseline congestion on the Internet including methodologies for identifying and measuring congestion at AS interconnection points in a route using time-sequence latency probing (TSLP)

measurements from CAIDA's Archipelago instrumentation distributed across the Internet by the team Clark et al. [1] and the more digestible slides of Smaragdakis et al.[2]. In particular I hope that the findings from their recently compiled two year study will soon be published, Clark et al. [3]. An analysis of consumer oriented tools, both commercial and governmental, are detailed and evaluated in the work by Koukoutsidis [4]. In work by Sundaresan et al. there is a focus on methods for Identifying TCP congestion signatures which hold promise at discriminating between "congestion experienced on interconnection links from congestion that naturally occurs when a last mile link is filled to capacity" [5]. While all of these methods for identifying congestion locations and magnitude are valuable, the bar is set very high for average consumers to combine these disparate data sources to prove deliberate degradation or impairment of their connections to the internet and successfully associate that with the provider's deliberate action. Also, without the type of background data forthcoming from Clark et al. [3], and the use of CAIDA's Ark infrastructure, I do not know of any other third party source of data that can be used to effectively characterize background inter-AS congestion. Also it may be necessary for citizens or organizations that want to improve the resolution of data within the state of Vermont to host additional Ark monitors throughout the state's AS networks. It also may be a useful precondition that a provider host one of these monitors.

If a complaint is successful in delineating a source of congestion ("interference or degradation") on the provider's network, the consumer ("Edge provider" or "Persons") must also be able to successfully argue that this congestion:

E. Is not the result of "reasonable network management practices"

F. Is not related to the customer using a “harmful device”

G. Is not the result of a customer sending or receiving “unlawful Internet traffic”

H. Is not the result of a customer sending or receiving “unlawful Internet content”

In case E, proving that a “network management practice” is or is not reasonable faces both a challenge of technical proficiency as well as access to information detailing the internal network management practices of a provider, often considered trade secrets. While there may some flexibility in dealing with this information under a complaint proceeding that is covered by an NDA as proposed, it would be difficult to challenge a network management practice without the ability to compare the actual effects of that management practice to some other network management practice or no management practice at all. Ideally this would be done using a representative traffic load in a simulation or experiment. Essentially it asks the Commission to judge that the network management practice is unreasonable based upon industry standards as opposed to real world performance standards.

Proving that traffic or content is legal (case G, case H) should be straightforward, but to add these clauses in consumer protection legislation is duplicative of the other laws prohibiting such traffic or content. Indeed, the addition of the lawful / unlawful clauses to traffic or content induces the provider to specifically inspect packets and the protocols in use, encouraging the provider to preemptively enforce these other laws in a technocratic manner directly inconsistent with net neutrality provisions. The provider’s operational security is necessarily a concern, and illegal activity on networks exists, but I do not think we want to legislate or encourage the

technocratic regulation of the latter to providers, that is precisely one of the outcomes that net neutrality seeks to avoid.

Case F has to do with what constitutes a harmful device. Who is responsible for the definition of a harmful device? I do not have a clear understanding of how a customer, provider, or Commission, would discern that a device is “harmful”. If the device is built implementing a hardware and software stack to interoperate successfully with the TCP/IP suite and other higher Layer protocol standards, I don’t know how it could be deemed “harmful” or “unlawful”. Genuine hardware or software bugs could break it’s interoperability with these aforementioned protocol standards. However, I don’t believe that type of interoperability problem constitutes the device being harmful or unlawful. A device created for the purpose of breaking intended operation of the network, like the recent revelation around Sandvine based network security appliances [6] used for malicious activity on provider networks, would clearly fly in the face of net neutrality. Would the Commission consider devices like that harmful? I think there is a conflation with how an actor (provider or consumer) can use such a device for malicious activity as opposed to the device itself being somehow inherently harmful. I fully expect that providers will take measures to ensure the operational security of their networks, but they should not be given the license to enforce and adjudicate against devices that don’t break standards of interoperability. If operators do not want to be dictated a technical hardware and software stack for their operations through legislation, why would a customer be any different? I do not think that there is a place for categorizing specific devices as harmful, illegal, or unlawful as part of net neutrality legislation though it certainly deserves more discussion and thought on the part of policymakers.

I have attempted to briefly illuminate some of the very real enforcement challenges and questions that any consumer protection focused net neutrality legislation will face. The critiques here are not exhaustive. I can offer a few other ideas for consideration. These basic questions about provider actions may be helpful at framing various classes of anti-consumer activity.

1. Is a provider blocking any TCP/IP suite protocols?
2. Is a provider degrading the performance of any TCP/IP suite protocols?
3. Is a provider blocking any application protocols that run on top of the Network / Internet Layer?
4. Is a provider degrading the performance of any application protocols that run on top of the Network / Internet Layer?

Affirmative answers to the questions above by a provider restrict the fundamental ability of the "Edge provider or "Persons" (i.e. consumers) to use the network in the way it was intended to be used. Affirmative answers will also impede the ability of the "Edge provider or "Persons" to collect the data necessary for filing a complaint in the first place.

"The Model Framework on Network Neutrality was initiated by the Council of Europe and developed by the ***Dynamic Coalition on Network Neutrality*** *(a multistakeholder component of the United Nations Internet Governance Forum) under the coordination of Dr. Luca Belli."* This compiled model for Net Neutrality regulation has been endorsed by many of the international organizations https://www.thisisnetneutrality.org/ [7] that are leading the charge for Net Neutrality regulations across the globe. I hereby incorporate below the model net neutrality

framework as retrieved from [7] on 2018-04-03 below. It seeks to successfully address many of my concerns above with the initial draft of H.680.

I. What Net Neutrality is

Network Neutrality is the principle according to which Internet traffic shall be treated equally, without discrimination, restriction or interference regardless of its sender, recipient, type or content, so that Internet users' freedom of choice is not restricted by favouring or disfavouring the transmission of Internet traffic associated with particular content, services, applications, or devices.

II. Exceptions to Net Neutrality

In accordance with the Network Neutrality principle, Internet service providers shall refrain from discriminating, restricting, or otherwise interfering with the transmission of Internet traffic, unless such interference is strictly necessary and proportionate to:

a) give effect to a legislative provision or court order;

b) preserve the integrity and security of the network, services and the Internet users' terminal equipment;

c) prevent the transmission of unsolicited communications for direct marketing purposes to Internet users who have given their prior consent to such restrictive measures;

d) comply with an explicit request from the subscriber, provided that this request is given freely and is not incentivised by the Internet service provider or its commercial partner;

e) mitigate the effects of temporary and exceptional network congestion, primarily by means of application-agnostic measures or, when these measures do not prove efficient, by means of application-specific measures.

III. Applies to all internet services, regardless of technology

The Network Neutrality principle shall apply to all Internet access services and Internet transit services offered by ISPs, regardless of the underlying technology used to transmit signals.

IV. How to treat specialised services

The Network Neutrality principle need not apply to specialised services. Internet service providers should be allowed to offer specialised services in addition to Internet access service, provided that such offerings are not to the detriment of Internet access services, or their performance, affordability, or quality. Offerings to deliver specialised services should be provided on a non-discriminatory basis and their adoption by Internet users should be.

V. Right to a unique internet address

Subscribers of Internet access service have the right to receive and use a public and globally unique Internet address.

VI. Privacy protections

Any techniques to inspect or analyse Internet traffic shall be in accordance with privacy and data protection legislation. By default, such techniques should only examine header information. The use of any technique which inspects or analyses the content of communications should be reviewed by the relevant national data protection authority to assess compliance with the applicable privacy and data protection obligations.

VII. Transparency

Internet service providers shall provide intelligible and transparent information with regard to their traffic management practices and usage policies, notably with regard to the coexistence of Internet access service and specialised services. When network capacity is shared between Internet access services and specialised services, the criteria whereby network capacity is shared, shall be clearly stated.

VIII. Enforcement

The competent national regulatory authority shall:

a) be mandated to regularly monitor and report on Internet traffic management practices and usage policies, in order to ensure Network Neutrality, evaluate the potential impact of the aforementioned practices and policies on fundamental rights, ensure the provision of a sufficient quality of service and the allocation of a satisfactory level of network capacity to the Internet. Reporting should be done in an open and transparent fashion and reports shall be made freely available to the public;

b) put in place appropriate, clear, open and efficient procedures aimed at addressing Network Neutrality complaints. To this end, all Internet users shall be entitled to make use of such complaint procedures in front of the relevant authority;

c) respond to the complaints within a reasonable time and be able to use necessary measures in order to sanction the breach of the Network Neutrality principle.

This authority must have the necessary resources to undertake the aforementioned duties in a timely and effective manner.

IX. Definitions

a) The “Internet” is the publicly accessible electronic communications network of networks that use the Internet Protocol for communication with endpoints reachable, directly or through network address translation, via a globally unique Internet address.

b) The expression “Internet service provider” refers to any legal person that offers Internet access service to the public or Internet transit service to another ISP.

c) The expression “Internet access service” refers to a publicly available electronic communications service that provides connectivity to the Internet, and thereby provides the ability to the subscriber or Internet user to receive and impart data from and to the Internet, irrespective of the underlying technology used to transmit signals.

d) The expression “Internet transit service” refers to the electronic communications service that provides connectivity between Internet service providers.

e) The expression “Internet traffic” refers to any flow of data packets transmitted through the Internet, regardless of the application or device that generated it.

f) The expression “specialised services” refers to electronic communications services that are provided and operated within closed electronic communications networks using the Internet Protocol, but not being part of the Internet. The expression “closed electronic communications networks” refers to networks that rely on strict admission control.

g) The expression "application-agnostic" refers to Internet traffic management practices, measures and techniques that do not depend on the characteristics of specific applications, content, services, devices and uses.

h) The expression "subscriber" refers to the natural or legal person who has entered into an agreement with an Internet service provider to receive Internet access service.

j) The expression "Internet user" refers to the natural or legal person who is using Internet access service, and in that capacity has the freedom to impart and receive information, and to use or offer applications and services through devices of their choice. The Internet user may be the subscriber, or any person to whom the subscriber has granted the right to use the Internet access service s/he receives. Any legal person offering content and/or applications on the Internet is also an Internet user.

Thank you again for the opportunity to submit this testimony.

1. Clark, David D. and Bauer, Steven and Lehr, William and Claffy, KC and Dhamdhere, Amogh D. and Huffaker, Bradley and Luckie, Matthew, Measurement and Analysis of Internet Interconnection and Congestion (September 9, 2014). 2014 TPRC Conference Paper. Available at SSRN: https://ssrn.com/abstract=2417573
2. http://cfp.mit.edu/events/27-OCT-2015/Smaragdakis-CFP2015-congestion.pdf
3. Clark, David D. and Dhamdhere, Amogh D. and Claffy, KC and Luckie, Matthew and Gamero-Garrido, Alexander, Detecting Internet Congestion at Interconnection Points: An

Empirical Analysis (March 16, 2018). Available at SSRN: https://ssrn.com/abstract=3141671

4. Koukoutsidis, Ioannis. "Public QoS and Net Neutrality Measurements: Current Status and Challenges Toward Exploitable Results." *Journal of Information Policy* 5 (2015): 245-86. http://www.jstor.org/stable/10.5325/jinfopoli.5.2015.0245
5. Sundaresan, Srikanth, Mark Allman, Amogh Dhamdhere, and Kc Claffy. “TCP Congestion Signatures,” 64–77. ACM Press, 2017. https://doi.org/10.1145/3131365.3131381.
6. https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/
7. https://www.thisisnetneutrality.org/