THE DIFFICULTY WITH REGULATING NETWORK NEUTRALITY♦

INTRODUCTION

Network neutrality is, and has been, an essential design element of the Internet.[1] The Internet was originally designed to embody an "end-to-end" principle,[2] and neutrality is a consequence of that design.[3]

1 *See* Brett M. Frischmann & Barbara van Schewick, *Network Neutrality and the Economics of an Information Superhighway: A Reply to Professor Yoo*, 47 JURIMETRICS J. 383, 385–86 (2007) ("The current Internet infrastructure evolved with the so-called 'end-to-end' design principle as its central tenet.").

2 *See* Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. REV. 925, 930–31 (2001) (stating that end-to-end design requires the pipes that carry information to be as simple and general as possible, and intelligence in the system should exist only at the ends, or rather, the users).

3 BARBARA VAN SCHEWICK, INTERNET ARCHITECTURE AND INNOVATION 57–60 (2010); *see*

Narrower than end-to-end, neutrality encompasses the idea that "a maximally useful public information network aspires to treat all content, sites, and platforms equally . . . allow[ing] the network to carry every form of information and support every kind of application."[4] The Internet's neutral architecture has facilitated and encouraged users to engage in socially beneficial activities such as content and application innovation, political and non-political discourse, and building and sustaining communities through social content.[5]

Increasingly, there has been pressure to move from a neutral network to a network that is optimized for particular functions (such as video streaming),[6] and technology has responded to that call through the creation of a powerful technology called Deep-Packet Inspection ("DPI"). DPI allows access providers to identify, store, and read addressing and *content* information within packets.[7] Network providers can now efficiently view the contents of packets to determine whether to slow them down, speed them up, or block them. Providers can also store packets for later access.[8] The DPI market has flourished as access

---

Frischmann & van Schewick, *supra* note 1, at 385–86 ("As a consequence of [the end-to-end] design, the network was application-blind; this prevented [access] providers from distinguishing between the applications and content running over the network and from affecting their execution.").

4 Tim Wu, *Network Neutrality Frequently Asked Questions*, TIM WU, http://timwu.org/network_neutrality.html (last visited Mar. 18, 2011).

5 BRETT M. FRISCHMANN, INFRASTRUCTURE: THE SOCIAL VALUE OF SHARED RESOURCES 298 (forthcoming 2012, on file with author) (for a discussion of social benefits created by the Internet, see pages 231–41); *see also* YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM 59–90 (2006), *available at* http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf (examining various content and applications that were made possible by the Internet managed as a commons and facilitator of peer-production).

6 *See* Frischmann & van Schewick, *supra* note 1, at 387 ("There is considerable pressure to change . . . from many sources, including the Internet's evolution to broadband[,] . . . rapid increase in users [of broadband,] demand for latency-sensitive applications such as video-on-demand and IP telephony, demand for security measures and spam regulation measures implemented at the 'core' of the Internet, and, more generally and importantly, demand for increased returns on infrastructure investments.").

7 Free Press's explanation of the situation is as follows:

> Messages on the Internet are broken down into small units called packets. Each packet contains a header and a data field. The header contains . . . the source and destination addresses. The data field contains everything else, including the identity of the source application (such as a Web browser request, a peer-to-peer transfer, or an e-mail), as well as the message itself (part of the contents of a Web page, file or e-mail). Packets are much like letters – the outside of the envelope is like the packet header, and the inside, like the data field, carries the message.
>
> . . . DPI technology opens and reads the data field [of packets] in real time, allowing network operators to identify and control, at a precise level, everyday uses of the Internet. Operators can tag packets for fast-lane or slow-lane treatment – or block the packets altogether – based on what they contain or which application sent them.

M. Chris Riley & Ben Scott, *Deep Packet Inspection: The End of the Internet as We Know It?*, FREE PRESS, 3 (Mar. 2009), http://www.freepress.net/files/Deep_Packet_Inspection_The_End_of_the_Internet_As_We_Know_It.pdf.

8 *See id.* Allowing access providers to look into the contents of packets using DPI has important privacy implications discussed in detail in Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417 (2009).

providers continue to invest in the new technology.[9]

DPI allows access providers to directly violate the neutrality principle because it provides a mechanism for unequal treatment of content.[10] For example, in 2008, Comcast admitted using DPI to block BitTorrent[11] traffic traveling its network.[12] The ability to treat content unequally could mean the stifling of free speech,[13] or the blocking of a marketplace competitor over that service provider's network.[14] The tension between network neutrality and DPI is significant – so much so that the Federal Communications Commission ("FCC") has intervened.[15]

The FCC's first attempt to provide substantive regulation of the open Internet[16] was in a Notice of Proposed Rulemaking ("NPRM")

---

9 The world-wide DPI industry has grown from an under–$400 million business in 2007 to an estimated $1 billion in 2010. Kyle Rosenthal, *Deep Packet Inspection: Vendors Tap into New Markets*, DPACKET (Nov. 28, 2007), https://www.dpacket.org/articles/deep-packet-inspection-vendors-tap-new-markets, and is projected to grow to a $1.5 billion business by 2013, Nate Anderson, *Deep Packet Inspection Soon to Be $1.5 Billion Business*, ARS TECHNICA (June 16, 2010, 11:16AM), http://arstechnica.com/tech-policy/news/2010/06/deep-packet-inspection-soon-to-be-15-billion-business.ars (citing Infonetics Research, a telecommunications market researching company).

10 *See* Wu, *supra* note 4. In addition, AT&T used DPI to monitor Internet traffic on the west coast of the U.S. at the request of the National Security Agency. Declan McCullagh, *AT&T Sued over NSA Spy Program*, CNET News (Jan. 31, 2006, 1:11PM), http://news.cnet.com/AT38T-sued-over-NSA-spy-program/2100-1028_3-6033501.html.

11 BitTorrent, a form of peer-to-peer communication, is an application designed to facilitate the efficient transfer of large files. As of 2009, it was estimated to constitute between 35% and 67.5% of all global Internet traffic, and is often used as an anonymous way to infringe intellectual property rights in music, software, movies, and television shows. Rebecca Giblin, *A Bit Liable? A Guide to Navigating the U.S. Secondary Liability Patchwork*, 25 SANTA CLARA COMPUTER & HIGH TECH. L.J. 7, 9–10 (2009).

12 *See Comcast Network Management Practices Order*, 23 FCC Rcd. 13,028, ¶ 42, at 13,051 (2008) [hereinafter *2008 Comcast Decision*], *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-183A1.pdf, *rev'd on other grounds*, Comcast Corp. v. FCC, 600 F.3d 642 (D.C. Cir. 2010).

13 Jon Peha, Professor of Electrical Engineering and Public Policy at Carnegie Mellon University, calls this "Stifling Free Speech for Fun and Profit." Jon M. Peha, *The Benefits and Risks of Mandating Network Neutrality, and the Quest for a Balanced Policy*, 34 TELECOMM. POL'Y RES. CONF. 1, 13 (2006), http://www.ece.cmu.edu/~peha/balanced_net_neutrality_policy.pdf.

14 VAN SCHEWICK, *supra* note 3, at 270 (stating that, though network providers do not always have incentives to block competitors, there are many situations, which van Schewick discusses, where access providers can increase their profits by discriminating against competitors in complementary markets).

15 The FCC has been involved in the network neutrality debate since at least 2005 when its Internet Policy Statement set forth the following original four principles of the open Internet: consumers are entitled to 1) access lawful content of their choice, 2) run applications and use services of their choice, 3) connect any non-harmful and lawful device to the network, and 4) competition among network, application, and content providers. *Appropriate Framework for Broadband Access to the Internet over Wireline Facilities*, 20 FCC Rcd. 14,986 (2005), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf. Subsequent to the Policy Statement, the FCC proposed a more specific and substantive rule in a Notice of Proposed Rulemaking, *In the Matter of Preserving the Open Internet; Broadband Industry Practices*, 24 FCC Rcd. 13,064 (2009) [hereinafter NPRM], *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-09-93A1.pdf. The FCC produced the Report and Order after public comments on the NPRM, Preserving the Open Internet, 76 Fed. Reg. 59,192 (Sept. 23, 2011) (to be codified at 47 C.F.R. pts. 0 and 8) [hereinafter Report], *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-09-23/pdf/2011-24259.pdf.

16 The terms "open Internet" and "network neutrality" are synonymous, and will be used

released in October 2009. The NPRM resulted in a cacophony of public comments, proving that regulating network neutrality is extremely difficult.[17] Many arguments were made supporting access provider control over content, including the evolving nature of technology and the issues that creates,[18] increasing users and uses of the Internet,[19] and constant security threats that could be more easily disposed of with technology such as DPI.[20] However, many arguments were made in support of neutrality, discouraging DPI use, including the loss of socially beneficial spillovers provided by an open Internet,[21] and the loss of a free and open platform that facilitates the growth of the worldwide economy.[22] In an attempt to balance these interests, the FCC recently published its final Report and Order for Preserving the Open Internet ("Report") in the Federal Register, which establishes a general principle that neutrality should be safeguarded.[23] Despite this safeguard, the FCC provided for a reasonable network management exception to neutrality, which allows access providers to treat content unequally if the provider is reasonably managing its network.[24]

The reasonable network management exception is a broad

interchangeably throughout this Note. However, the FCC refers to the issue as "open Internet." *See, e.g.*, Report, 76 Fed. Reg. 59,192.

17 A search of the FCC E-Filings database for comments in this proceeding shows over 10,000 filings, with a variety of viewpoints. Search for Filings, FCC ELECTRONIC COMMENT FILING SYSTEM, http://fjallfoss.fcc.gov/ecfs/comment_search/input?z=dhy64 (input "09-191" under "Proceeding Number" and "10/22/09" in the "From:" field under "Received") (last visited Mar. 30, 2011).

18 NPRM, *supra* note 15, ¶ 134, at 13,112.

19 There has been a 480.4% increase in worldwide Internet users since 2000, *Internet Usage Statistics*, INTERNET WORLD STATS, http://www.internetworldstats.com/stats.htm (last visited Aug. 6, 2011), and a 151.7% increase in United States Internet users since 2000, *Internet Usage and Population in North America*, INTERNET WORLD STATS, http://www.internetworldstats.com/stats14.htm#north (last visited Aug. 6, 2011). Additionally, applications and content have increasingly become bandwidth-heavy, such as Internet video and peer-to-peer technology. *See* Christopher S. Yoo, *Network Neutrality, Consumers, and Innovation*, 2008 U. CHI. LEGAL F. 179, 187-96 (2008).

20 *See IT Pros Expect Network Threats to Increase as Budgets Decline*, HELP NET SECURITY (June 24, 2010), http://www.net-security.org/secworld.php?id=9471; *see also* AT&T Comments to Notice of Proposed Rulemaking, WC Docket 07-52, FED. COMM. COMMISSION, 183 (Jan. 14, 2010), http://fjallfoss.fcc.gov/ecfs/document/view?id=7020377217 [hereinafter AT&T Comments] (describing cybersecurity threats as "[p]erhaps the most pressing network management challenge of all").

21 *See generally* FRISCHMANN, *supra* note 5, at 306 ("The Internet is a spillover-rich environment because of the basic user capabilities it provides and the incredibly wide variety of user activities that generate and share public and social goods.").

22 *See generally* Robert D. Atkinson, et al., *The Internet Economy 25 Years After .Com: Transforming Commerce and Life*, INFORMATION TECHNOLOGY & INNOVATION FOUNDATION, 43 (Mar. 2010), http://www.itif.org/files/2010-25-years.pdf ("In 2010, global e-commerce activity totaled an estimated $10 trillion. . . . Within the United States . . . a study commissioned by the Interactive Advertising Bureau found that 1.2 million Americans are employed directly to conduct Internet advertising and commerce, build and maintain the Internet infrastructure, and facilitate its use. Each Internet job supports approximately 1.54 additional jobs elsewhere in the economy, for a total of 3.05 million jobs, or roughly 2 percent of employed Americans. The dollar value of their wages totals approximately $300 billion, or around 2 percent of U.S. GDP.").

23 Report, 76 Fed. Reg. 59,192, 59,193 (Sept. 23, 2011) (to be codified at 47 C.F.R. pts. 0 and 8), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-09-23/pdf/2011-24259.pdf ("The framework we adopt aims to ensure the Internet remains an open platform . . . .").

24 *Id.* at 59,208.

exception. However, a broad exception, potentially overbroad, may not be the most prudent form for regulating network neutrality. Typically, a regulation can take the form of a rule or a standard. While standards are broader, requiring a case-by-case analysis, rules are stricter, reducing the need for fact-specific analyses. To determine what form is appropriate for a network neutrality regulation, one should engage in a rules-versus-standards analysis specifically in this context. There is no obvious choice, but context can provide useful background when determining whether to regulate with rules or standards.[25]

Network neutrality regulation should be written as a rule, not a standard. Establishing a rule-like regulation will deter non-neutral behavior by access providers, and will preserve the Internet's neutral architecture and the benefits that equal treatment of content provides. In addition, rule-like regulations reduce the burden placed on enforcers, typically users, of the regulation. For these reasons, the reasonable network management exception should also be worded like a rule; those arguing for a broad, standard-like exception have not successfully demonstrated why a broad exception is required.

Part I of this Note will discuss what is at stake in the network neutrality debate. Part II will introduce and explain the FCC's Report for Preserving the Open Internet. Part III will discuss network neutrality and why it requires a rule-like regulation. Part IV will explain that the reasonable network management exception requires rule-like wording, and that those arguing for a broad, standard-like exception have not successfully demonstrated why a standard is more appropriate. Finally, Part V will propose a rule-like reasonable network management exception that conforms to the principles discussed herein.

I. VALUE CREATED BY A NEUTRAL INTERNET

Network neutrality is a much-contested topic, especially surrounding the Report.[26] As a preliminary matter, one must understand that the Internet creates value beyond obvious metrics,[27] such as

---

25 *See* Cass R. Sunstein, *Problems with Rules*, 83 CAL. L. REV. 953, 959 (1995) ("Rules cannot be favored or disfavored in the abstract; everything depends on whether, in context, rules are superior to the alternatives.").

26 The House of Representatives voted to disapprove the FCC's neutrality regulation. Tony Romm, *House Votes to Repeal Net Neutrality Order*, POLITICO (Apr. 8, 2011, 4:22PM), http://www.politico.com/news/stories/0411/52826.html. However, presidential advisors say they will recommend vetoing any anti-neutrality regulation. Tony Romm & Eliza Krigman, *W.H. Vows to Protect Net Neutrality*, POLITICO (Apr. 4, 2011, 6:41PM), http://www.politico.com/news/stories/0411/52525.html. Verizon has appealed the FCC's Report asserting the FCC does not have the authority to enact such rules; Free Press, on the other hand, has appealed the Report because the rules do not go far enough to protect wireless customers. Cecilia Kang, *Verizon Sues FCC over Net Neutrality Rules*, WASH. POST (Sept. 30, 2011, 6:16 PM), http://www.washingtonpost.com/blogs/post-tech/post/verizon-sues-fcc-over-net-neutrality-rules/2011/09/30/gIQAFUP0AL_blog.html. For a discussion of the Report, see *infra* Part II.

27 *See* FRISCHMANN, *supra* note 5, at 298 ("[I]t is incredibly difficult to [place a value on social benefit] . . . [which] leads us to take the social value for granted.").

contribution to e-commerce,[28] despite the inability to quantify such a benefit.[29] However, the neutral architecture of the Internet provides social benefit.[30] Because the end-user is able to participate in almost any activity as a result of the neutrality principle,[31] socially beneficial spillovers are created.[32] It is this social benefit, taking the form of positive externalities, at stake in the regulation of network neutrality. As power over Internet access becomes increasingly centralized, and fewer end-users participate in socially beneficial online activities, fewer spillovers occur, and society benefits less.

Because the Internet is a medium for commercial activity, as well as social and public activity, it is referred to as a "mixed infrastructure."[33] Social value created by the Internet, despite its propensity to go unmeasured, is of utmost importance in the neutrality debate because of its role in the Internet's "transform[ation of] our society."[34] However, social value is often not captured in market transactions, thus under a pure free-market regime, the Internet and its users may underproduce social goods, resulting in a net loss of societal benefit.[35]

The Internet facilitates widespread participation in socially beneficial activities.[36] Because it is decentralized, the Internet allows for volunteers to pool resources and contribute small pieces of an overall project (such as Wikipedia); this is called peer-production.[37]

---

28 For statistics on how much the Internet contributes to e-commerce, see *2008 E-Stats*, U.S. CENSUS BUREAU, 2 (May 27, 2010), http://www.census.gov/econ/estats/2008/2008reportfinal.pdf.

29 *See* Frischmann & van Schewick, *supra* note 1, at 399 ("[Socially productive uses of the Internet] too easily evade[] observation or consideration within conventional economic transactions.").

30 *See also* FRISCHMANN, *supra* note 5, at 298 ("[T]he value of the Internet as public and social infrastructure dwarfs its value as commercial infrastructure.").

31 This is because the Internet is managed as a commons. Commons management opposes a "property" system, in that common property has no single owner. BENKLER, *supra* note 5, at 60–61. There is no centralized power that controls the Internet the way a property owner controls real property. *Id.* at 60.

32 FRISCHMANN, *supra* note 5, at 298 ("The Internet's value to society is tied to the range of capabilities it provides for individuals, firms, households, and other organizations to interact with each other and to participate in various activities and social systems.").

33 Frischmann & van Schewick, *supra* note 1, at 398; *see also* FRISCHMANN, *supra* note 5, at 297 ("The Internet is perhaps the clearest example of an infrastructure resource that enables the production of a wide variety of public, private, and social goods.").

34 FRISCHMANN, *supra* note 5, at 298 ("[T]he value of the Internet as public and social infrastructure dwarfs its value as commercial infrastructure.").

35 *See* Frischmann & van Schewick, *supra* note 1, at 399; *see also* FRISCHMANN, *supra* note 5, at 294 ("[C]ompetitive markets . . . underproduce public and social goods.").

36 *See* Frischmann & van Schewick, *supra* note 1, at 398–99 ("Common nondiscriminatory access to [the Internet] facilitates widespread end-user participation in a variety of socially valuable productive activities. . . . End-users . . . engage in innovation and creation; they speak about anything and everything; they maintain family connections and friendships; they debate, comment, and engage in political and nonpolitical discourse; they meet new people; they search, research, learn, and educate; and they build and sustain communities.") (internal quotation marks omitted).

37 BENKLER, *supra* note 5, at 35–36. Benkler refers to this throughout his book as the "networked information economy." *See id.* at 3.

Contrast this with centralized infrastructures, such as newspaper, radio, and television, which facilitate only one-way information flow, in which the central entity chooses the news to report and readers either subscribe and passively absorb it, or do not subscribe and do not benefit from the knowledge.[38] The Internet gives users the ability to cooperate and coordinate with each another to produce information, and reduces the burden of the collective action problem.[39] The ideal example of peer-production is open source software. The programming of open source software is based on a decentralized model that allows for the input of multiple developers to complete,[40] and the finished product is given away for free.[41] Other programmers that wish to add or remove features may freely alter the code and then re-release it.[42] Through the actions of uncompensated open source developers, society has benefitted tremendously by free software alternatives and by increased competition in select software markets.[43]

A common thread throughout all this is that the Internet functions as a free expression infrastructure.[44] Because users can engage in any activity, they are free to express themselves. Such freedoms have allowed for the use of Facebook and Twitter in the Egyptian and Tunisian uprisings in 2009-11.[45] But, as the Internet becomes important for democratic discourse, it is also coming under the control of "powerful private corporations . . . [that] create and maintain the architectures . . . through which everyone else communicates."[46] Control of the Internet appears to be increasingly centralized at corporations and even governments, and this threatens the neutrality principle.[47]

Access providers are comparable to a company that builds the bridge that provides access to a beautiful state park. The park, managed as a commons, brings benefits to society including its aesthetics, the

38 *Id.* at 29–30.
39 *Id.* at 63 (the Internet provides for "more effective collective action practices").
40 *Id.*
41 VLC Media Player is often recognized as an open source success. *See generally* Nick Russell, *Open Video Conference: Everything You Wanted to Know About VLC*, NATIONAL ALLIANCE FOR MEDIA, ART, AND CULTURE BLOG (Oct. 11, 2010), http://www.namac.org/node/25286.
42 BENKLER, *supra* note 5, at 66–67.
43 Even big companies like Hewlett-Packard, Google, Amazon, and CNN.com, use Linux, an open source operating system, to run their servers. *Id.* at 64.
44 *See generally* Jack Balkin, *The First Amendment is an Information Policy*, §§ I-III, BALKINIZATION (Mar. 28, 2011), http://balkin.blogspot.com/2011/03/hugo-black-lecture-part-i.html.
45 *See id.* at § IV, http://balkin.blogspot.com/2011/03/hugo-black-lecture-part-ii.html.
46 Balkin, *supra* note 44, §§ I–III.
47 The Bay Area Rapid Transit train system in San Francisco shut down all cell phone service at some train stations in order to prevent protestors from communicating under the mistaken impression protestors were gathering there. Mike Masnick, *BART Turns off Mobile Phone Service at Station Because It Doesn't Want Protestors to Communicate*, TECHDIRT (Aug. 12, 2011, 2:59PM). The United Kingdom government wanted cell phone service shut off during riots that occurred in London in mid-2011. Nick Judd, *A Call to Curtail London Rioting Focuses on 'Encrypted' Mobile Messaging Service*, PERSONAL DEMOCRACY FORUM (Aug. 9, 2011, 1:02PM).

view, and the ability for the community to use it as much as they want. It also provides an open meeting area where people can gather for any and all reasons – including innocuous reasons (organizing a baseball game), or harmful reasons (plotting to steal a purse). But once bridge-builders (broadband access providers) start dictating what and who can and cannot be in the park (on the Internet), openness is undermined, fewer social spillovers occur, peer-production becomes more difficult to carry out, and the variety of benefits provided by openness and decentralization subside.

II. THE REPORT AND ORDER FOR PRESERVING THE OPEN INTERNET

The FCC recently published its Report and Order on Preserving the Open Internet in the Federal Register. The regulation establishes, in effect, four principles:

> - Transparency. Fixed . . . broadband providers must disclose the network management practices, performance characteristics, and terms and conditions of their broadband services;
> - No blocking. Fixed broadband providers may not block lawful content, applications, services, or non-harmful devices . . . .
> - No unreasonable discrimination. Fixed broadband providers may not unreasonably discriminate in transmitting lawful network traffic. . . .
> - [These principles are subject to a reasonable network management exception.][48]

The transparency principle requires "effective" disclosure of a provider's network management practices in order to promote competition by, among other things, increasing the likelihood of provider compliance with the open Internet rules.[49] If practices are disclosed to the public, it theoretically makes it easier for users and regulators to enforce the regulation.[50] The FCC believes "the best approach is to allow for flexibility in implementation of the transparency rule . . . ."[51] However, the Report also acknowledges that transparency alone will not adequately protect neutrality.[52]

"No blocking" is further defined by the Commission in the following way: "[A broadband service provider] shall not block lawful content, applications, services, or nonharmful devices, subject to

---

48 Report, 76 Fed. Reg. 59,192, 59,192 (Sept. 23, 2011) (to be codified at 47 C.F.R. pts. 0 and 8). This Note will not discuss the regulation as applied to wireless technology.
49 *Id.* at 59,203.
50 *Id.*
51 *Id.*
52 *Id.* at 59,204.

reasonable network management."[53] This part of the Report is relatively simple – once an access provider blocks lawful content, applications, services, or nonharmful devices, the provider must cease blocking.[54] Only limited fact-finding is required for this determination; if the complainant alleged an access provider blocked content, the provider would have only a limited chance to defend itself under the reasonable network management exception. It is admitted that "[m]ajor broadband providers represent that they currently operate consistent with this principle and are committed to continuing to do so."[55] Despite this claim, there are still opportunities for accusations and claims based on this principle.[56]

The "no unreasonable discrimination" principle lacks the rule-like clarity of the "no blocking" rule. The Report explains, "[a broadband provider] shall not unreasonably discriminate in transmitting lawful network traffic over a consumer's broadband Internet access service. Reasonable network management shall not constitute unreasonable discrimination."[57] The word "unreasonable" provides much uncertainty in that a reasonableness determination must be made,[58] which requires extensive fact-finding. The reasonableness standard also leaves future adjudicators with much discretion.

In an effort to increase clarity, the Report expressly allows for usage-based billing[59] and for discrimination that is not based on the application or content.[60] The Report also establishes a strong presumption against (but does not make per se illegal) the validity of commercial agreements involving the exchange of money for speed increases (also called "pay-for-priority").[61] Additionally, the Commission would be "concerned" about practices that harm competitors of the access provider, end-users, or free expression.[62] This

---

53 *Id.* at 59,205.

54 The Commission, in a similar manner, forced Comcast to cease blocking BitTorrent traffic in the 2008 Comcast case. *See 2008 Comcast Decision*, *supra* note 12, ¶ 54, at 13,059 ("Our overriding aim here is to end Comcast's use of unreasonable network management practices . . . .").

55 Report, 76 Fed. Reg. at 59,205.

56 Free Press accused (but did not file a complaint against) MetroPCS of violating the "no blocking" principle when the provider offered tiered access plans that restricted access based on the consumer's subscription rate. *See* Free Press Notice of Ex Parte, WC Docket 07-52, FED. COMM. COMMISSION (Jan. 10, 2011), http://fjallfoss.fcc.gov/ecfs/document/view?id=7021025487. For MetroPCS's response and denial of the accusations, see MetroPCS Notice of Ex Parte, WC Docket 07-52, FED. COMM. COMMISSION (Feb. 14, 2011), http://fjallfoss.fcc.gov/ecfs/document/view?id=7021029361.

57 Report, 76 Fed. Reg. at 59,205.

58 Under the NPRM, all discrimination was unlawful, not just unreasonable discrimination. NPRM, *supra* note 15, ¶ 103, at 13,104. The Report specifically declines to adopt such a strict rule because some forms of discrimination can be beneficial. Report, 76 Fed. Reg. at 59,207.

59 Report, 76 Fed. Reg. at 59,206. Metered billing allows access providers to charge users by time or bandwidth increments.

60 *Id.*

61 *Id.* The NPRM established that a ban on pay-for-priority arrangements, but the Report refused to adopt that hard-line approach. *Id.* at 59,206 n.86.

62 *Id.* at 59,206.

additional language may be an attempt to restrict future discretion, but the language of the Report assumes there might be certain situations that may rebut the strong presumption against pay-for-priority contracts; thus the Commission leaves the question open for future adjudications.

The reasonable network management exception (the focus of Part IV of this Note) also lacks clarity, despite the Report's express interest in the opposite.[63] The Commission writes:

> A network management practice is reasonable if it is appropriate and tailored to achieving a legitimate network management purpose, taking into account the particular network architecture and technology of the broadband Internet access service.
>
> Legitimate network management purposes include: ensuring network security and integrity, including by addressing traffic that is harmful to the network; addressing traffic that is unwanted by end users . . . such as by providing services or capabilities consistent with an end user's choices regarding parental controls or security capabilities; and reducing or mitigating the effects of congestion on the network.[64]

The Report is much clearer than the NPRM with regard to reasonable network management;[65] the Report provides specific examples and reduces the uncertainty of what constitutes a legitimate network management purpose.[66] However, the principle is still unclear, given the inclusive, rather than exclusive, nature of the list of legitimate network management purposes.[67]

Regarding legitimate network management purposes, the Report considers "spam, botnets, and distributed denial-of-service attacks" to be harmful to the network, and therefore cause for unequal treatment of content.[68] The Report also allows access providers to offer services consistent with end-user preferences, including parental controls.[69] Lastly, the Report gives a pithy description of network congestion that allows providers to ensure that heavy-bandwidth users do not block out

---

63 *Id.* at 59,208 ("The open Internet rules we adopt in this Order expressly provide for and define 'reasonable network management' in order to provide greater clarity to broadband providers, network equipment providers, and Internet end users and edge providers regarding the types of network management practices that are consistent with open Internet protections.").

64 *Id.*

65 The NPRM reasonable network management exception included a circular provision that swallowed the entire regulation. NPRM, *supra* note 15, ¶ 135, at 13,113 ("Reasonable network management consists of . . . (b) other reasonable network management practices.").

66 Report, Fed. Reg. at 59,208.

67 In fact, this is expressly stated. *Id.* at 59,210 ("We emphasize that reasonable network management practices are not limited to the categories described here, and that broadband providers may take other reasonable steps to maintain the proper functioning of their networks, consistent with the definition of reasonable network management we adopt.").

68 *Id.* at 59,209 n.102.

69 *Id.* at 59,209.

light-bandwidth users.[70] The Commission's emphasis on clarity is well-intentioned, but it may still be difficult for the regulated parties (access providers, content providers, and consumers) to conform to the Report pre-enforcement.

The Report will be enforced on a case-by-case basis.[71] This approach has been met with almost universal support.[72] Guiding principles in these proceedings include transparency, end-user control, and use-agnostic treatment.[73] In other words, discriminatory practices are more likely to be reasonable if disclosed to the public (transparent),[74] unwanted by end-users,[75] and not based on the specific use (use-agnostic treatment).[76] However, by adding extra factors and elements for future adjudicators to consider, requiring a case-by-case analysis may further reduce the clarity the Commission seeks because of pervasive uncertainty within the regulation.

The Report expressly rejects the narrowly tailored approach it announced in the 2008 Comcast Decision,[77] which required that a network management practice had to "further a critically important interest and be narrowly or carefully tailored to serve that interest" to be reasonable.[78] The Report reasons that the narrow tailoring requirement is "unnecessarily restrictive" and would overly constrain network engineer decisions.[79] The refusal to adopt this strict standard significantly reduces the burden on future access providers, and effectively increases the burden on the complainant, in future adjudications.

The Commission also provides procedural guidelines for filing a complaint within the FCC,[80] which look similar to requirements for filing a complaint in the court system.[81] Once a formal complaint is

---

70 *Id.* at 59,209–10.
71 *Id.* at 59,208.
72 *Id.* at 59,222.
73 *Id.* at 59,205–06, 59,209.
74 *Id.* at 59,205. This is because the Commission has previously found practices to be unreasonable because they were not disclosed to users. *Id.*
75 *Id.* at 59,205–06. End-user control is important because "letting users choose how they want to use the network enables them to use the Internet in a way that creates more value for them (and for society) . . . ." *Id.* (quoting Barbara van Schewick).
76 *Id.* at 59,206. Use-agnostic discrimination "is consistent with Internet openness because it does not interfere with end users' choices about which content, applications, services, or devices to use." *Id.*
77 *Id.* at 59,209.
78 *Id.* at 59,209 n.100.
79 *Id.* at 59,209.
80 The FCC outlines the procedure by which a complaint must be brought. *See id.* at 59,233-34. Complainants can bring either informal or formal complaints; however, informal complaints rarely lead to written Commission orders, which will reduce their precedential effect. *See id.* at 59,222.
81 There are a variety of requirements, such as a clear, concise, and explicit complaint (§ 8.13(a)(1)) that is supported by legal precedent (§ 8.13(a)(5)). It also gives general guidelines for complaints (§ 8.14(a)), answers to complaints (§ 8.14(b)), and replies (§ 8.14(c)). The Commission also has the discretion to order discovery (§ 8.14(f)) or refer the case to an administrative law judge (§ 8.14(g)). *Id.* at 59,232–34. Compare these requirements to FED. R. CIV. P. 7(a) (allowing complaints, answers, and counterclaims, among others), 8(a)(2) (requiring

filed, there might be an adjudicatory proceeding depending on, among other things, a prima facie showing of a violation, or whether the agency needs more facts.[82] The Report describes the adjudication process in the following way:

> [W]e require a complainant alleging a violation of the open Internet rules to plead fully and with specificity the basis of its claims and to provide facts, supported when possible by documentation or affidavit, sufficient to establish a *prima facie* [sic] case of an open Internet violation. In turn, the broadband provider must answer each claim with particularity and furnish facts, supported by documentation or affidavit, demonstrating the reasonableness of the challenged practice. At that point, the complainant will have the opportunity to demonstrate that the practice is not reasonable.[83]

The process looks familiar – the complainant proves its case, the access provider argues the exception applies, then the complainant argues that the exception does not apply. This process is important for a potential complainant to keep in mind when thinking about filing a formal complaint, as the requirements may be prohibitively costly.[84]

In addition, parties may request that proprietary information be kept confidential.[85] If the party makes the requisite showing under the disclosure exemption of the Freedom of Information Act, then that information will never be made public.[86] The Commission provided confidentiality protection for the benefit of access providers.[87] An added, though potentially unintended, benefit to providers is that the confidentiality rule might have the effect of hiding information that would be helpful precedent for future adjudications.[88]

The Report's overall goal of increased clarity is noble, but its use of equivocal language and curt descriptions actually allow for *increased*

---

short and plain statement of claim), and 11(b)(2) (requiring claim to be supported by law).

82 *Id.* at 59,223.

83 *Id.*

84 *See infra* Part III.c.

85 Report, 76 Fed. Reg. at 59,234.

86 *Id.* Only certain people will be able to access the information, including counsel of record, officers and employees of the parties, consultants or expert witnesses, the Commission and its staff, and court reporters and stenographers (§ 8.16(c)(1)–(5)). *Id.* In addition, all originals and reproductions of documents containing proprietary information must be returned to the producing party, and any work product derived from the information must be destroyed at the termination of the proceedings (§ 8.16(g)). *Id.* at 59,235.

87 *Id.* at 59,203 n.62 ("[T]o the extent [the Commission requires disclosure of proprietary information, the Commission] will ensure that such information is protected [through the] procedures for treatment of confidential information.").

88 *See* Free Press Reply Comments to Notice of Proposed Rulemaking, WC Docket 07-52, FED. COMM. COMMISSION, 21 (Apr. 26, 2010), http://fjallfoss.fcc.gov/ecfs/document/view?id=7020437465 ("Disclosure is the . . . primary source of information on which to base a complaint for violation of nondiscrimination or other open Internet rules. If [confidential information can be hidden], network operators will invent . . . 'confidential business information' rationales to hide . . . harmful behavior from the . . . public . . . substantially increasing the difficulty of enforcement.").

discretion by future adjudicators and therefore less pre-enforcement clarity.[89] This is not prudent; there should be clearer guidelines so future Commissioners and administrative law judges are more constrained in their analyses and less prone to bias,[90] and so users and content providers know what constitutes a violation before complaints are filed. This requires a rule-like regulation as opposed to the Report's current emphasis on standards.

III. NETWORK NEUTRALITY SHOULD FAVOR REGULATION BY RULE

In order to ensure the Internet continues to provide societal benefits, an open Internet regulation should be overprotective, not underprotective, of neutrality. In other words, it should leave less room for discretion in future proceedings. Being overprotective is preferred because it will deter discriminatory behavior while preserving neutrality, and it will leave less discretion to future adjudications, therefore, the costs of enforcement will decrease. These rationales can best be explained and understood through a discussion of the rules and standards distinction and the associated error costs.

A. *Rules Versus Standards and Error Costs*[91]

Rules and standards are not binary concepts; instead, they are viewed as being two ends of a spectrum.[92] Regulations, in general, are viewed as more "rule-like" or more "standard-like."[93] Fundamentally, the distinction is about the level of discretion given to an adjudicator (whether a judge or a Commissioner) in deciding future cases.[94] A rule gives less discretion to the adjudicator. Since there is less interpretation involved, the costs of litigation are reduced.[95] Additionally, rules are intended to "specify outcomes before particular cases arise,"[96] providing useful guidance.[97]

---

89 The attempt to provide clarity in the regulation is undermined by the use of equivocal language; terms like "would be concern[ing]" and "may need to take reasonable steps" offer some guidance, but ultimately, future adjudicators will be determining whether, under the circumstances, the behavior was *actually* unacceptable. Report, 76 Fed. Reg. at 59,209–10, 59,214.

90 "Open-ended standards invite judges to import their own biases and predispositions into legal decisionmaking." Connor N. Raso & William N. Eskridge, Jr., *Chevron as Canon, Not a Precedent: An Empirical Study of What Motivates Justices in Agency Deference Cases*, 110 COLUM. L. REV. 1727, 1744 (2010).

91 These concepts are borrowed from anti-trust law, as discussed *infra* Part III.b.2, but they can apply to any regulation.

92 Edward Lee, *Rules and Standards in Cyberspace*, 77 NOTRE DAME L. REV. 1275, 1294 (2002).

93 *Id.* To avoid confusion, this Note will simply use "rule" and "standard."

94 *Id.*

95 *See* Cass R. Sunstein, *Problems with Rules*, 83 CAL. L. REV. 953, 962 (1995) ("When rules are operating, an assessment of facts, combined with an ordinary understanding of grammar, semantics, and diction -- and of conventions and more substantive ideas on which there is no dispute -- is usually sufficient to decide the case.").

96 *Id.* at 961.

97 Continental T.V., Inc. v. GTE Sylvania, Inc., 433 U.S. 36, 50 n.16 (1977) ("Once established,

For example, speed limits are rules that impose liability when a person is driving in excess of the posted speed limit.[98] Speed limit signs allow people to align their behavior with the law.[99] It also means that it is obvious (to the violator) when she is in violation of the law.[100] However, rules can increase total costs to the system by discouraging acceptable practices.[101] A businesswoman who is rushing to her office because she is about to close the deal of her life is just as liable for exceeding the speed limit as a teenager rushing to the mall to be with her friends. Perhaps the businesswoman believes she is justified, and perhaps society thinks that as well. But unless there is an exception to the rule, the adjudicator will not take into account the reasonableness of the speeding.[102]

When interpreting a standard, it is often "not possible to know what" behavior is acceptable "in advance" of the action.[103] Standards require more fact-specific analyses that take into account the totality of the circumstances,[104] thus each proceeding gives an individualized assessment of the case.[105] As proceedings become more individualized, time demands and costs for the parties increase.[106] Standards, which require case-by-case determinations,[107] systematically favor those willing and able to pay the costs, and disfavor those who cannot.[108]

For example, fair use in copyright law is a standard;[109] what constitutes fair use is broadly defined by a list of purposes and factors, and any particular determination depends on a case-by-case analysis of the details and facts of the situation.[110] Having to prove a defense requiring a showing under a variety of factors, such as fair use, requires time and money, which can deter potential litigants that lack the resources to litigate.[111]

---

per se rules tend to provide guidance to the . . . community . . . .").

98 Kathleen M. Sullivan, *The Justices of Rules and Standards*, 106 HARV. L. REV. 22, 60 n.247 (1992).

99 This represents a relatively simple rule. Rules can be much more complex, such as "creating a formula for deciding who may drive," at what age, and what tests are required. Sunstein, *supra* note 95, at 962.

100 *See id*. at 976 ("When rules are at work, it is clear who is responsible and who is to be blamed if things go wrong.").

101 *See* Leegin Creative Leather Prod., Inc. v. PSKS, Inc., 551 U.S. 877, 895 (2007).

102 *See* Sunstein, *supra* note 95, at 962–63 (stating that rules are often accompanied by excuses, and even if not, are excused by necessity or emergency). Neither the necessity nor the emergency exception applies to the businesswoman or the teenager in this hypothetical.

103 *Id.* at 965.

104 Sullivan, *supra* note 98, at 59.

105 Lee, *supra* note 92, at 1294.

106 Sunstein, *supra* note 95, at 977.

107 Lee, *supra* note 92, at 1294.

108 Sunstein, *supra* note 95, at 977 ("It is also plausible to think that case-by-case judgments systematically favor the well-to-do. Litigation is extremely expensive, and for litigants to seek fine-grained, individualized judgments, they need resources. [This creates] a pervasive form of inequality, in which people without resources stand on the sidelines, or are unable to persuade officials that their case warrants favorable treatment.").

109 Lee, *supra* note 92, at 1295.

110 *Id.* at 1309 ("[S]tandards take into greater account the particular facts of a case . . . .").

111 *See* Herbert Hovenkamp, *Patents, Property, and Competition Policy*, 34 J. CORP. L. 1243,

In the network neutrality context, the Report consists of a rule, "no blocking,"[112] a standard, "no unreasonable discrimination," and a standard-like exception to both principles, "reasonable network management."[113] A consequence of a regulation emphasizing standards[114] is that future adjudications will require extensive fact-finding, and future adjudicators will have substantial discretion to determine the meaning of the guidelines provided by the regulation.[115]

When deciding to regulate with rules or standards, one should also analyze the error costs associated with choosing one form of regulation over the other. Error costs are costs incurred by incorrect outcomes.[116] They come in the following two forms: false positives – incorrectly imposing liability, and false negatives – incorrectly failing to impose liability.[117] Because rules are strict and do not require extensive fact-finding, rules are more likely to create error costs in the form of false positives, and will tend to be overinclusive.[118] Alternatively, standards are likely to emphasize false negatives because case-by-case analyses are meant to ensure correctness of outcome, but in an even-sided case, the emphasis on not incorrectly punishing behavior will favor the defendant.[119] Analyzing error costs can help determine which type (rule or standard) should be favored, because error costs clearly describe the tradeoffs between them.

False positives and false negatives should be minimized wherever possible; but short of ensuring no error costs, the question is how to balance the tradeoffs between the two.[120] Determining a preference requires a contextual analysis similar to the discussion in Part I.[121] That discussion provides convincing evidence that network neutrality regulation should reduce false negatives while allowing for more false positives; however, the Report emphasizes standards, which represents

---

1256 n.61 (2009).

112 "No blocking" is a rule because it requires limited fact-finding, and the strict language specifies outcomes before cases are brought. *See supra* note 53 and accompanying text.

113 Both regulations, "no unreasonable discrimination" and "reasonable network management," are standards because they require a reasonableness determination, which requires substantial fact-finding, and the adjudicator has substantial discretion. *See supra* note 64 and accompanying text.

114 Importantly, the FCC does not refer to the regulation in rules versus standards nomenclature. *See generally supra* note 15.

115 *See supra* notes 103–111 and accompanying text.

116 William McGeveran, *The Trademark Fair Use Reform Act*, 90 B.U. L. REV. 2267, 2280 (2010).

117 *Id*.

118 *See* William H. Page, *The Chicago School and the Evolution of Antitrust: Characterization, Antitrust Injury, and Evidentiary Sufficiency*, 75 VA. L. REV. 1221, 1265 (1989) (stating the Chicago school analysis tends to emphasize overinclusiveness, and thus false positives, associated with a per se rule).

119 *See id*. (stating the Court, in Arizona v. Maricopa Cnty. Med. Soc'y, 457 U.S. 332 (1982), emphasized the false negatives associated with rules of reason (standards)).

120 Brett M. Frischmann, *Error Costs vs Accuracy Benefits*, MADISONIAN.NET (Jan. 16, 2008), http://madisonian.net/2008/01/16/error-costs-vs-accuracy-benefits.

121 Sunstein, *supra* note 95, at 959 ("Rules cannot be favored or disfavored in the abstract; everything depends on whether, in context, rules are superior to the alternatives.").

a systemic preference for reducing false positives while allowing for more false negatives.[122] There are consequences of this form, including favoring those with abundant resources (access providers) over those with fewer resources (users and regulators),[123] and allowing discriminatory behavior to go unpunished when it should have been punished. These two reasons illustrate that network neutrality regulation, in balancing the potential solutions, should favor false positives, not false negatives; in other words, the regulation should accept placing incorrect blame in order to reduce discriminatory behavior by access providers.

B. *The Report Imposes Significant Costs on Complainants*

A rule against discrimination will reduce the costs to a complainant (typically a user) in a neutrality proceeding.[124] As noted above, rules have the benefit of specifying outcomes before cases arise.[125] A plain rule will provide enough clarity for users and content providers to understand when their access provider is violating the regulation, and, more importantly, what type of behavior constitutes a violation.[126] Additionally, the ability for access providers to block or discriminate against content that constitutes speech and expression of ideas means that "specificity and predictability are especially critical."[127]

On the other hand, the Report, with its emphasis on standards, accomplishes none of these ends because it does not take into account the realities of the market and of enforcement of the regulation. The Report will increase costs to potential complainants because users will find it difficult to determine neutrality violations in the first place, and the costs to the user of enforcing neutrality regulations through the Commission's process will likely outweigh the benefits.

1. The Difficulty in Determining Neutrality Violations

Discriminatory behavior is not obvious to detect,[128] making

---

122 The Report endorses case-by-case determinations, which are designed to reduce false positives. Report, 76 Fed. Reg. 59,192, 59,208 (Sept. 23, 2011) (to be codified at 47 C.F.R. pts. 0 and 8), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-09-23/pdf/2011-24259.pdf.

123 *See* Sunstein, *supra* note 95, at 977 ("It is also plausible to think that case-by-case judgments systematically favor the well-to-do.").

124 Continental T.V., Inc. v. GTE Sylvania, Inc., 433 U.S. 36, 50 n.16 (1977) ("Once established, per se rules tend . . . to minimize the burdens on litigants and the judicial system . . . .").

125 *See* Sunstein, *supra* note 95, at 961.

126 *Id.*

127 McGeveran, *supra* note 116, at 2290. While this argument is made specifically in the free speech context, it applies equally to the Internet and to the potential suppression of ideas and speech by access providers. It becomes increasingly important because access providers have the incentive to limit Internet openness. Report, 76 Fed. Reg. 59,191, 59,195-98 (Sept. 23, 2011) (to be codified at 47 C.F.R. pts. 0 and 8), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-09-23/pdf/2011-24259.pdf 5.

128 *See* VAN SCHEWICK, *supra* note 3, at 260.

enforcement difficult.[129] When particular applications or content are slowed down, the user's satisfaction will decrease, but she is unlikely to know the true cause of the discrepancy.[130] There are other reasons applications and content could be slow, including bad programming, server overload, or slow Internet transport.[131] All of these reasons manifest in the same way – slow speeds. This may lead users to misplace blame for slow access to content on the owner of the content, or the creators of the game or application, when the true cause is discriminatory behavior of the access provider.[132] In this sense, access providers are taking advantage of the information asymmetry as to the true source of poor performance between providers and users.[133]

The Report's response is to require access provider transparency.[134] The transparency requirement merely provides guidelines for what network practices to disclose and how to disclose them.[135] The transparency requirement, however, allows for providers to be vague, and potentially avoid disclosure of information that is "competitively sensitive."[136] Putting aside the fact that many users would not understand the technical information provided in the provider disclosures,[137] this could create problems for potential complainants because vague descriptions of network management practices will not help determine *when* an access provider is actually engaging in those practices. In addition, if the provider feels the information is competitively sensitive, it may choose not to disclose at all, or at least not at a time relevant for user policing. As mentioned above, access providers can take advantage of information asymmetry as to the true source of poor performance,[138] and the user may simply assume the slow speeds have some other cause, which exonerates the access provider because it took advantage of the information asymmetry

---

129 *See* NPRM, *supra* note 15, ¶ 124, at 13,110 ("In the absence of disclosure rules, [the FCC has] no way of knowing the full extent of these practices. Nor do users."); Free Press Comments to Notice of Proposed Rulemaking, WC Docket 07-52, FED. COMM. COMMISSION, 113 (Jan. 14, 2010), http://fjallfoss.fcc.gov/ecfs/document/view?id=7020378792 [hereinafter FP Comments] ("[S]ervice providers generally fail to provide any meaningful information on their network management practices, making it more difficult for users and for the Commission to identify any potential violations or to attribute accurately any usage problems to the network operator or to an end node in the communication.").

130 *See* VAN SCHEWICK, *supra* note 3, at 260; s*ee also* FP Comments, *supra* note 129, at 114 ("In the absence of proper disclosure, consumers may be left with the false impression that electronic equipment or software is to blame for an altered user experience that is actually caused by the network operator.").

131 VAN SCHEWICK, *supra* note 3, at 260.

132 *Id*.

133 *Id*. For example, when Comcast discriminated against BitTorrent, it chose its software because the method the software used was less detectable by users. *Id*.

134 Report, 76 Fed. Reg. 59,191, 59,202 (Sept. 23, 2011) (to be codified at 47 C.F.R. pts. 0 and 8), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-09-23/pdf/2011-24259.pdf.

135 *Id.* at 59,203; *see also* notes 49–52 and accompanying text.

136 Report, 76 Fed. Reg. at 59,203.

137 Free Press refers to these users as the "general audience." FP Comments, *supra* note 129, at 112.

138 VAN SCHEWICK, *supra* note 3, at 260.

between it and the user.

2. Cost-Benefit Analysis of Enforcement

Once discrimination is discovered, the lack of clarity provided by the Report will vastly increase the costs to a potential complainant. To its credit, the Commission has tried to reduce up-front costs to users by allowing for informal complaints.[139] While this is an important step in the right direction, the language used in the Report places reduced importance on informal complaints. For instance, informal complaints do not typically lead to written Commission orders, meaning these complaints will rarely have precedential effect.[140]

The formal complaint process requires a substantial factual showing as discussed in Part II.[141] From a user's perspective, the proceeding can appear very costly. Obviously, a user filing a complaint would like to be successful, but she has to be successful potentially twice: once to prove discrimination, and again if the access provider succeeds in proving its behavior was reasonable.[142] This requires a lot of resources, and also increases the likelihood of failure on the user's part because there are two chances for the Commission to find against her. Additionally, because of the possibility that precedential information is confidential, precedent will be slow to develop, and, at least early in the regulation's life, there will be no precedent on which to rely. This could place yet another barrier between the user and successfully enforcing the regulation. While the Commission has the authority to initiate enforcement on its own motion,[143] it is unclear whether users can rely on that enforcement mechanism to effectively protect them against illegal discriminatory practices.

The Report includes a broad standard (no unreasonable discrimination) with a broad and vague exception (reasonable network management), both of which will effectively allow for more false negatives as discussed above. This format gives access providers two opportunities to argue their behavior was reasonable; in other words, access providers have two bites at the apple. First, they can argue it was "reasonable" discrimination, and as such, it does not violate the "no unreasonable discrimination" standard.[144] Second, they can argue that

139 Report, 76 Fed. Reg. at 59,222. Informal complaints require no filing fee. *Id.*
140 *Id.*
141 *See supra* note 83 and accompanying text.
142 Also, during the proceeding and before the adjudicator's final order, the access provider will likely continue the discriminatory behavior. Proceedings can take over two years, as the 2008 Comcast Decision showed. The first test to determine if Comcast was throttling BitTorrent was done in October 2007. *See* Declan McCullagh, *Comcast Really Does Block BitTorrent Traffic After All*, CNET NEWS (Oct. 19, 2007, 11:06 AM), http://news.cnet.com/8301-13578_3-9800629-38.html. The subsequent D.C. Circuit Court of Appeals final decision was released April 6, 2010. Comcast Corp. v. FCC, 600 F.3d 642 (D.C. Cir. 2010).
143 Report, 76 Fed. Reg. at 59,223.
144 There are many arguments to be made within the standard, including the following: a) the behavior did not discriminate based on the use of the network (*Id.* at 59,206); b) the behavior

the behavior was reasonable network management.[145] Because both of these prongs are standards, each determination will require the adjudicator to look closely at the facts of the situation and to make an individualized assessment based on her substantial discretion. By enacting a standard-like regulation, the Commission has reduced the likelihood of a complaint being filed in the first instance because the augmented proceedings required for enforcing the standard represents a significant additional cost to the complainant.

Compare these mounting costs to the relatively low payout. A user who successfully enforces the neutrality regulation will realize largely intangible benefits. The user may feel a particular sense of satisfaction for enforcing the regulation for its own sake, or for taking down her access provider for acting illegally. The user may also experience an incrementally faster access speed to the content that was previously the subject of discrimination, as it is no longer subject to discrimination.[146] Though, from a rational perspective, incurring substantial costs (by attempting to enforce the regulation) in the form of time and money for a largely intangible payout suggests the regulation will rarely be enforced. In addition, because the user still does not know whether the access provider is continuing to discriminate because of information asymmetry, the access provider could still continue discriminating in different ways.[147]

Some argue that the complainant should also have to prove unreasonableness of the behavior and an anticompetitive effect[148] before

---

conformed with best practices in the industry (*Id.*); c) the behavior did not harm end-users, competitors, or did not impair free expression (*Id.*); or d) the behavior targeted unlawful content (*Id.* at 59,205), among others.

145 Normal statutory interpretation principles state that similar words used in regulations are not to be interpreted as redundant; therefore, the two reasonableness inquiries will likely be separate. *See* Bailey v. United States, 516 U.S. 137, 146 (1995) ("[W]e assume that Congress used two terms because it intended each term to have a particular, nonsuperfluous meaning.").

146 Admittedly, if the relevant content was a video service or some other application requiring fast response times, the benefit may be more pronounced.

147 *Cf.* VAN SCHEWICK, *supra* note 3, at 260 ("Thus, by using discrimination, a network provider can exploit customers' incomplete information about the true source of poor performance."). This is assuming there is no on-going tracking or monitoring of the access provider imposed by the FCC. It is unclear at this time whether this kind of punishment would be imposed.

148 There has been debate over how to define anticompetitive behavior in the net neutrality debate. Comments of Barbara van Schewick, *Net Neutrality: What a Non-Discrimination Rule Should Look Like*, FED. COMM. COMMISSION, 2-3 (Sept. 20, 2010), http://fjallfoss.fcc.gov/ecfs/document/view?id=7020913189 [hereinafter van Schewick Comments]. If the definition is imported from U.S. antitrust law, it will be defined too narrowly for the purposes of net neutrality, as the action must "harm[] competition." Barbara van Schewick, Professor at Stanford Law School and an information law expert, uses the following example: If a provider wants to block BitTorrent from its network, it constitutes "anti-competitive" behavior under U.S. antitrust law only if the action creates a "dangerous probability of success" that the Internet service provider will monopolize the nationwide market for BitTorrent-like applications. *Id.* In the context of the 2008 Comcast decision, the blocking of BitTorrent would have been irrelevant under antitrust law. However, it is very relevant in a net neutrality debate. Antitrust laws also have stringent market power requirements, whereas net neutrality proponents care about discrimination regardless of market power. *Id.*

the provider would be liable.[149] This argument is simply a way to continue to shift the burdens and costs away from access providers, who are the subjects of the regulation. Further shifting the costs in this manner is unacceptable, as such a showing would be even more prohibitively burdensome on users, especially given the confusion over the definition of anticompetitive behavior and the complexities of anti-trust law. This argument essentially creates a presumption out of the exception, defeating its purpose.

Without a doubt, the Report will impose costs on users in the form of significant time and cost burdens, as well as general uncertainty. When compared to the low payouts of winning, there is a heavy weight on the cost side that will undoubtedly deter many potential complainants. When combined with standard-like language that increases costs to the users in the adjudicatory stage, and the emphasis on not placing incorrect blame on defendants, this will lead to a severe disincentive to filing complaints in general, and a severe under-enforcement of the regulation. In the end, it will allow more discriminatory behavior, and will reduce positive spillovers that result from the openness of the Internet.

C. *Favoring False Negatives May Incent Access Providers to Discriminate*

When regulating by rule, the obviousness of a rule violation will deter the behavior.[150] Similarly, in the context of network neutrality, a clear rule against blocking and discriminating against content would deter that behavior, even if it might be acceptable in some circumstances.[151] Any proceeding requiring interpretation of a rule will be less protracted, the legality of the behavior will be clearer, and the user would be more likely to be able to force a settlement, if right, or be forced out of the proceeding early, if wrong.[152] From a planning perspective, all parties would be better off because the regulation would be easier for access providers to comply with, and users could more

---

149 Essentially, those that make this argument argue for a presumption that discriminatory behavior is reasonable, and then place the initial burden on the complainant to prove unreasonableness and anticompetitiveness. *See* Comcast Comments to Notice of Proposed Rulemaking, WC Docket 07-52, FED. COMM. COMMISSION, 56 (Jan. 14, 2010), http://fjallfoss.fcc.gov/ecfs/document/view?id=7020375772; Cablevision Reply Comments to Notice of Proposed Rulemaking, WC Docket 07-52, FED. COMM. COMMISSION, 11 (Apr. 26, 2010), http://fjallfoss.fcc.gov/ecfs/document/view?id=7020437092 [hereinafter Cablevision Reply]; Time Warner Cable Comments to Notice of Proposed Rulemaking, WC Docket 07-52, FED. COMM. COMMISSION, 72 (Jan. 14, 2010), http://fjallfoss.fcc.gov/ecfs/document/view?id=7020375997 [hereinafter TWC Comments].

150 *See* Lee, *supra* note 92, at 1314 (stating that rules allow for greater predictability of the law, and for easier planning of behavior that conforms to the law). For instance, if the Report simply stated, "no content discrimination is allowed," access providers would be much less likely to discriminate based on content.

151 *See* Sunstein, *supra* note 95, at 976 ("When rules are at work, it is clear who is responsible and who is to be blamed if things go wrong.").

152 *See supra* notes 92–102 and accompanying text.

easily (and will have fewer barriers to) enforce the regulation if violations occur.

As discussed above, there is little incentive to file a complaint. The fact that providers can argue twice for the reasonableness of their actions will increase the costs (mainly time and money) to complainants to maintain and argue the complaint, and will reduce the likelihood of settlement or summary judgment because access providers need merely a reasonable explanation.[153] Because of the decreased likelihood of complaints, access providers may increase discrimination because they are unlikely to get caught. This will ultimately allow for more discriminatory behavior, and will likely allow for neutrality violations.[154]

In general, false negatives are preferred over false positives because the market will punish false negatives;[155] the theory is that if the public disapproves of the behavior, even if the court does not, the market will reflect that disapproval.[156] However, to make a similar argument in the network neutrality context would be to ignore or misunderstand the nature of the access provider market. There is little competition in the market for broadband access providers.[157] In addition, the barriers to entry in the market are very high.[158] As a result, the access provider market is extremely unlikely to act in a similar manner as other markets, and access providers will not be punished

153 The Report itself actually encourages parties to settle. Report, 76 Fed. Reg. 59,192, 59,222 (Sept. 23, 2011) (to be codified in 47 C.F.R. pts. 0 and 8), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-09-23/pdf/2011-24259.pdf. However, with such open-ended language, it is difficult to understand why an access provider would want to settle if they had any possible justification for its behavior, or if it could outspend the complainant.

154 van Schewick Comments, *supra* note 148, at 21 ("[B]ehavioral economics suggest that discriminatory behavior is more likely to be allowed under case-by-case adjudication than under an ex ante [rule-like] scheme.").

155 Salil Mehra, *Building Antitrust Agency Capacity in Context*, 103 NW. U. L. REV. COLLOQUY 310, 314 n.18 (2009) (stating that costs imposed by false positives are more than the costs imposed by false negatives because the latter is more likely to be corrected by the market).

156 *See* Frank H. Easterbrook, *The Limits of Antitrust*, 63 TEX. L. REV. 1, 3 (1984).

157 *See* VAN SCHEWICK, *supra* note 3, at 452 n.42 ("For residential high-speed Internet access service, the relevant market is local. . . . According to FCC data, 34% of ZIP codes have one or less cable or []DSL provider who serves at least one subscriber living within the ZIP code as of June 2007 . . . ." The endnote continues, "this measure . . . overstates the level of competition to individual households."); *see also* Nate Anderson, *Deep Packet Inspection Meets 'Net Neutrality, CALEA*, ARS TECHNICA (July 25, 2007, 11:10 PM), http://arstechnica.com/hardware/news/2007/07/Deep-packet-inspection-meets-net-neutrality.ars/3 ("We've been pointing out for years that Americans are generally locked into one or two [Internet service] providers, so most people are hardly spoiled for choice.").

158 For an overview of the various barriers to entry in the broadband market, see Richard S. Whitt, *Evolving Broadband Policy: Taking Adaptive Stances to Foster Optimal Internet Platforms*, 17 COMMLAW CONSPECTUS 417 (2009). More proof is that the number of cable modem providers and DSL providers has stagnated since 2005. *See Internet Access Services: Status as of December 31, 2009*, FED. COMM. COMMISSION 32 (Dec. 2010), http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-303405A1.pdf. The Internet Access Services report does show, however, that the number of providers of Fiber-to-the-Premises (FTTP) has increased. This could be because already existing access providers have adopted FTTP services; however, the report does not specify.

when conventional wisdom says they should be.[159] Because access providers likely know switching costs[160] are high and there is little to no competition in the broadband market, they are unlikely to be deterred by loss of market share. This, again, will allow providers to treat content unequally.

Along the same lines, some argue that competition alone will deter access providers from discriminating.[161] However, competition is an illusory solution.[162] Without knowledge of discriminatory practices, competition is not useful because users will not know when their provider is treating content unequally. Competition would be helpful only if the access provider were forced to adequately disclose its management practices, users knew about the disclosure, and users understood its implications so she could determine whether she would like to switch providers.[163] In addition, the user must value content neutrality enough such that switching costs would not prohibit the user from switching providers; this value can often be misunderstood given that individual users are unlikely to understand the benefits they receive as a result of neutrality, which mostly come in the form of positive externalities, as explained above. Only if these factors were true would competition be helpful. However, because very little competition in the broadband access provider market actually exists, and even where it does, information asymmetry negates the benefits provided by it, these arguments represent a misunderstanding of the reality of the broadband

---

159 If broadband access providers were subject to Title II common carriage regulations (under the 1996 Telecommunications Act), they would be forced to provide competitors with access to their networks, so-called "open access," thereby increasing competition. *See* Reza Dibadj, *Toward Meaningful Cable Competition: Getting Beyond the Monopoly Morass*, 6 N.Y.U. J. LEGIS. & PUB. POL'Y 245, 262 (2003). This requirement would reduce at least some barriers to entry, allowing for start-ups to access big telecom networks. Open access was mandated in the AOL/Time Warner merger in 2001, but has not been a requirement since 2002, when the FCC reclassified broadband access to an "Information Service," regulated under the lenient Title I regulations. *See id.* at 258.

160 Switching costs are the costs incurred by a user by switching service providers. These may include early termination fees, installation of the new service, any new equipment required, the loss of discounts previously received, and time and effort to make the switch (which can be costly). VAN SCHEWICK, *supra* note 3, at 261–62. Studies in behavioral economics show that "even very small costs may prevent customers from switching . . . [because of a] 'status quo bias' . . . ." *Id*. at 264.

161 Gary S. Becker et al., *Net Neutrality and Consumer Welfare*, 6 J. COMPETITION L. & ECON. 497, 505 (2010) ("[B]roadband access providers typically face significant competition, and a wide range of firms are entering and/or upgrading their service offerings. Given these alternatives, access providers that fail to satisfy consumers' preferences risk losing substantial numbers of subscribers to rivals. These circumstances reduce the risk that attempts by broadband access providers to engage in discrimination would succeed in impairing competition and further suggest that the net neutrality proponents' competitive concerns are overstated."); *see also* Christopher S. Yoo, *Network Neutrality, Consumers, and Innovation*, 2008 U. CHI. LEGAL F. 179, 245 (2008)

162 *See* FRISCHMANN, *supra* note 5, at 293 (labeling competition a "red herring" in the network neutrality debate).

163 *Id*. at 228. Disclosure might create the opposite problem, that of constantly blaming the provider when slow speeds are actually attributable to bad programming or poor server performance.

market.[164]

Because the Open Internet regulation emphasizes standards and not rules, discriminatory behavior will likely be allowed. The difficulty in pinpointing discriminatory behavior and the incredibly high costs for potential complainants will create a system that presumptively allows content discrimination because enforcement will be rare. Alternatively, a *rule* proscribing discriminatory behavior will decrease incentives for access providers to engage in such activity because the cost of bringing a complaint will be reduced as violations become more obvious.[165]

D. *Favoring False Positives Requires Tradeoffs*

As stated before, favoring either false positives or false negatives is a tradeoff; favoring one over the other necessarily has costs. Richard Bennett, a technology expert working for the Information Technology and Innovation Foundation, argues that unequal treatment of content has beneficial uses, and that any regulation of network neutrality should allow for these benefits.[166] Until recently, Bennett says, the network has been routing packets for applications that generally have the same bandwidth and other technical requirements (e-mail, Internet browsing, and others).[167] With new applications becoming more bandwidth-heavy and popular (IP telephony applications such as Skype, peer-to-peer transaction applications such as BitTorrent), networks have to differentiate in order to provide good service.[168] DPI is very good at reducing delay when it is needed, and any regulation should allow for such a benefit.[169] Specifically, Bennett says that the "sensible way to manage the Internet [application] diversity is to identify application needs and try to meet them, to create 'the greatest good for the greatest number' of people."[170]

---

164 *See supra* text accompanying note 157. It is also important to note that those pointing to the effectiveness of competition argue that competition exists because users have a choice between cable, DSL, satellite, and wireless services. Becker, *supra* note 161, at 502. This argument assumes that consumers are willing to accept that moving to competing services may include a significant speed decrease, and less access to innovations such as Netflix, Hulu, and other services that require higher bandwidth. VAN SCHEWICK, *supra* note 3, at 262 ("Internet-service offerings of various providers differ substantially in price, quality, and other characteristics. Therefore, they are not interchangeable."); Peter Bowen & Shawn Hoy, *Broadband Performance* 13 (Fed. Commc'n Comm'n, Technical Paper No. 4, 2011), *available at* http://download.broadband.gov/plan/fcc-omnibus-broadband-initiative-(obi)-technical-paper-broadband-performance.pdf (last visited Mar. 27, 2011) (showing, in exhibit 15, that advertised connections speeds of cable access are between two and three times as fast as DSL speeds, and even more so for satellite and wireless connection speeds).

165 The difficulty in pinpointing discrimination would still be a problem under a rule-like regime, but that is generally a question of establishing strong transparency requirements, and subsequent user knowledge of the disclosures and the enforcement mechanisms in the regulation.

166 *See* Richard Bennett, *Shutting Down the Internet*, RICHARD BENNETT BLOG (Mar. 19, 2009), http://bennett.com/blog/2009/03/shutting-down-the-internet.

167 *Id.*

168 *Id.*

169 *Id.*

170 *Id.*

Bennett's greatest good for the greatest number theory is problematic. First, it is unclear what constitutes "the greatest good." Surely it does not mean prioritizing Skype, peer-to-peer, and video game packets over every other type of packet simply because those applications require the least delay. This could potentially create a two-tiered Internet where access providers could favor their own content, or content under a commercial agreement.[171] The "greatest good" could be interpreted to mean many things, and it probably means something different to access providers as opposed to their customers. Second, it is unclear what constitutes "the greatest number." It cannot mean prioritizing Google Video Chat over Skype so long as more of the provider's customers use Google Video Chat. This could also lead to a two-tiered Internet where applications used by a majority of the provider's customers are favored, and those who use other applications are disfavored.

Essentially, Bennett's argument advocates for an optimized network. An optimized network is a network that is very good at running applications that are currently available, but is not good at adapting as applications and content evolve.[172] Of course, bandwidth-intensive programs like Skype and World of Warcraft (a massively-multiplayer online role playing game) would be faster and provide a better experience for users if access providers could give each program the boost it needs to work with minimal interruption.[173] But the lack of evolvability in an optimized network means the next-generation application will not be optimized, and as time goes on, the same argument will be rehashed and networks will have to be re-optimized.[174] This is unnecessary; preserving the evolvability of the network by refusing to allow for optimization will prevent future access providers from having to manually re-optimize the network for next-generation applications and technology, and it will reduce the likelihood of a two-tiered Internet.

Another potential consequence of favoring false positives is that investment in the telecommunications sector will decrease because the returns on investment in broadband infrastructure for the access

---

171 *See* Michael Geist, *Towards a Two-Tier Internet*, BBC NEWS, http://news.bbc.co.uk/2/hi/technology/4552138.stm (last updated Dec. 22, 2005).

172 VAN SCHEWICK, *supra* note 3, at 68.

173 Surprisingly, the company that used to market Skype prefers strong network neutrality regulation because the program runs well on the current best-efforts system. Panel Transcript, *The Federalism*
Society for Law and Public Policy: Broadband Policy: One Year in: 2009 National Lawyer's Convention, 7 SETON HALL CIRCUIT REV. 27, 56 (2010) (quoting Professor Marvin Ammori, University of Nebraska-Lincoln College of Law). This potentially undermines the argument that networks need to increase packet travel speed of high-bandwidth uses.

174 *Cf.* VAN SCHEWICK, *supra* note 3, at 68 (quoting David Reed, one of the authors of the seminal paper on end-to-end architecture: "Non-end-to-end designs [of networks] usually fail to meet future needs quickly.").

providers will decrease.[175] However, this assertion is not clearly true. Free Press, a non-profit entity specializing in media reform,[176] states that investment decisions are influenced by many factors, and to say that mandating network neutrality will automatically reduce investment is incorrect.[177] Additionally, Free Press used historical data to show that investment has remained high in other contexts when network neutrality was enforced, and this may continue even after regulations are passed.[178]

Lastly, some argue that because the regulatory impact on consumers is speculative, any network neutrality regulation should give the benefit of the doubt to access providers, and strict rules should be enacted only after empirical evidence shows that consumers are harmed by a lack of neutrality enforcement.[179] The reasoning for giving providers the benefit of the doubt is that there is potential for content prioritization to benefit consumers, including increased competition at the last-mile (by increasing providers' ability to "differentiate themselves"),[180] increased innovation (especially of high-intensity bandwidth applications),[181] and increased price signaling that rewards quality content,[182] among others. As a result, some argue that anti-trust law provides an adequate regulatory framework for network neutrality that serves to prevent those with market power from using their market power to reduce competitiveness.[183]

These arguments represent a very narrow economic view of the problems presented by network neutrality. First, the analysis

---

175 This was used as a justification by the House of Representatives in its recent vote to overturn the FCC's Report. *See* Joelle Tessler, *House Republicans Move to Block FCC Internet Regulations*, HUFFINGTON POST (Feb. 18, 2011, 12:07 AM), http://www.huffingtonpost.com/2011/02/18/house-republicans-block-net-neutrality_n_824917.html.

176 *Beginner's Guide*, FREE PRESS, http://www.freepress.net/resources/beginners_guide (last visited Aug. 20, 2011).

177 *See* S. Derek Turner, *Finding the Bottom Line: The Truth About Network Neutrality & Investment*, FREE PRESS, 2 (Oct. 2009), http://www.freepress.net/files/Finding_the_Bottom_Line_The_Truth_About_NN_and_Investment_0.pdf.

178 *Id.* Free Press specifically uses AT&T as an example. In 2006, AT&T merged with BellSouth and was required to follow neutrality principles for two years. During that period, investment increased more than any other access provider in the United States. *Id.* at 5–8.

179 Yoo, *supra* note 161, at 217 ("So long as some plausible argument exists that a practice might be socially beneficial, the better course is to establish rules that give network providers the flexibility to experiment with that practice until its precise impact on consumers can be determined.").

180 *Id.* at 213. The ability to differentiate yourself, plus the possibility of creating new protocols, could allow for three distinct last-mile broadband networks to exist: one optimized for low-intensity bandwidth applications like e-mail and website access, one optimized for commercial transactions, and one optimized for high-intensity bandwidth applications. *Id.* at 214.

181 *Id.* at 229.

182 *Id.* at 234–38 (stating that allowing network providers (or consumers) to pay a higher price for higher quality content rewards that content).

183 *Id.* at 245–46 (stating that the law regarding vertical constraints is all that is required because it addresses the same concern of network neutrality proponents: "that a firm operating at one level of a chain of production will exercise its market power to reduce the competitiveness of an adjacent level of production").

completely ignores the vast spillover effects and social benefits conferred by the end-user's ability to engage in almost any activity.[184] An analysis that does not take these benefits into account is, arguably, an incomplete analysis that disproportionately emphasizes the effectiveness of market mechanisms.[185] Second, as discussed before,[186] anti-trust law covers a narrower subset of issues than network neutrality. Contextually, network neutrality analysis should include the vast spillovers and social benefits provided by the open nature of the Internet, but anti-trust law's emphasis on monopoly markets and consumer harm may even ignore positive externalities associated with the infrastructure.[187] Additionally, a perfectly competitive market will underproduce positive externality-producing goods, which includes socially beneficial spillovers, that are not part of the market analysis.[188] "The social opportunity costs of allowing network owners[] to dismantle the Internet's infrastructure commons may be tremendous but incredibly difficult to measure precisely because so much of the value generated by Internet users is not fully captured in market transactions."[189] Because applying only anti-trust law to the network neutrality framework necessarily assumes away the positive externalities associated with the Internet's infrastructure, it cannot and should not provide the sole mechanism through which neutrality is enforced.

It is clear that ex ante rules favoring false positives come with potential costs. However, because the beneficial spillovers provided by the Internet, though immeasurable, are vast and important, neutrality regulation should err on the side of too much neutrality, rather than not enough. This will ensure the continued societal benefit provided by the open Internet.

* * * *

Determining what form a regulation should take requires tradeoffs. The tradeoffs are best couched in terms of the rules versus standards distinction, and whether to favor false positives or false negatives. There are strong arguments that regulating network neutrality should favor rules and tolerate false positives over false negatives. First, cabining the discretion of future adjudicators will decrease costs of enforcement to complainants; second, being overprotective of neutrality

184 *See generally* Frischmann & van Schewick, *supra* note 1, at 398–99, 402. Some view caps on usage as an adequate fix, but caps on usage would make it more difficult for high-bandwidth innovations to become successful, as users would be afraid of going over their cap.
185 See *id.* (stating that end-users engage in a variety of spillover-rich activities, and that this value "too easily evades observation or consideration within conventional economic transactions").
186 *See supra* note 148 and accompanying text.
187 *See* van Schewick Comments, *supra* note 148.
188 FRISCHMANN, *supra* note 5, at 294 (stating that competition will not alleviate demand-side concerns, and may serve to reduce demand-side benefits if exclusively relied upon).
189 Frischmann & van Schewick, *supra* note 1, at 428.

will ensure that the openness of the Internet continues to benefit society in the same manner it has for the past decade and even before that. Under an ex ante regime, all parties benefit through clear and understandable regulations. Based on this reasoning, the reasonable network management exception, specifically, should also take the form of a rule.[190]

IV. THE REASONABLE NETWORK MANAGEMENT EXCEPTION REQUIRES RULE-LIKE WORDING

As discussed above, regulating by standard in the network neutrality context does not provide enough guidance to be an effective deterrent to discriminatory behavior. By leaving substantial discretion to future adjudications, access providers, consumers, and content providers are worse off. The parties will feel the burden as future adjudicators struggle to find meaning in the regulation.[191] If access providers had legitimate reasons for broad, potentially overinclusive language, the exception's overbreadth would be easier to understand and justify. However, neither the FCC, nor access providers, have successfully demonstrated that a standard-like exception is required.

A. *The FCC's Deference to Future Technology Does Not Justify Subversion of Neutrality*

The FCC justifies taking a broad, case-by-case approach by stating it prefers to defer to the novelty of future technological advances,[192] and will defer to future actions taken by access providers in order to experiment, innovate, and reasonably manage their networks as issues arise.[193] Granted, no one can predict the future of technology, but this does not justify a broad exception that sweeps in potentially unwarranted discrimination, even from technology that does not yet exist.[194] Taking this justification at face value, the FCC should err on the side of *too much* neutrality; future technology could benefit or harm consumers, and deference to its use might not be in the public interest.

---

190 Whether the "no unreasonable discrimination" standard should similarly be reworked is a question for another article.

191 These burdens might include additional fact-finding, discovery, referral to administrative law judge, and the inevitable appeal once a determination has been made. Report, 76 Fed. Reg. 59,192, 59,232–35 (Sept. 23, 2011) (to be codified at 47 C.F.R. pts. 0 and 8), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-09-23/pdf/2011-24259.pdf.

192 *Id*. at 59,208 (stating the regulation takes into account the "novelty of Internet access and traffic management questions, the complex nature of the Internet, and a general policy of restraint in setting policy for Internet access service providers . . .").

193 *Id*. at 59,210 ("Broadband providers should have flexibility to experiment, innovate, and reasonably manage their networks.").

194 It is fair to assume future technology will only become cheaper and more efficient. Moore's law, which says that the number of transistors that fit cheaply on a computer chip doubles roughly every two years, essentially guarantees this. *See* John O. McGinnis, *Accelerating AI*, 104 NW. U. L. REV. 1253, 1257 (2010). If deep-packet inspection technology will only get cheaper and more efficient, the FCC should not defer to it when it could potentially erode neutrality.

According to the Report, access providers "have the incentive and ability to limit Internet openness" and they have acted upon this incentive.[195] If access providers have the incentive to discriminate now, without strict regulations that apply to them, enacting standards with a broad exception does not incent them to refrain from discrimination. Rather, access providers will now argue that any discrimination, regardless of reason, is a reasonable network management practice.[196]

Additionally, the FCC does not want to micromanage access providers by telling them how to manage their networks; usage patterns and technology will be changing in the future, and access providers should be able to deal with this through "experiment[ation], innovat[ion], and reasonabl[y] manag[ing] their networks."[197] In essence, this is an argument for access provider innovation – because a strict rule would prevent access providers from innovating with new ways to effectively alleviate network issues, the FCC would prefer standard-like regulations with a case-by-case approach to solving individual cases of discrimination.

The FCC's arguments for why it imposes a broad standard do not adequately justify a violation of the neutrality principle. The FCC appears to be making convenience arguments. Because it is more *convenient* for the FCC and access providers to respond to technological change (that may cause congestion, or may be a harmful virus) through unequal treatment of content instead of upgrading capacity or providing independent software, providers would like the privilege to manage the network excessively. However, it should take a more compelling argument than convenience to subvert the neutrality principle.

Access provider innovation is important, but it should not come at the cost of end-user innovation and the beneficial spillovers it creates. Providers would like the ability to innovate at their level in order to better service their customers, perhaps through virus protection that is integrated into user connections, or through stopping spam at its source.

---

195 *See* Report, 76 Fed. Reg. at 59,195-99; *see also* VAN SCHEWICK, *supra* note 3, at 281 ("[A] network provider has an incentive to use the power provided by the architecture to engage in noncooperative strategic behavior in order to increase profits.").

196 For example, Comcast went so far as to *admit* treating content unequally in the 2008 Comcast Decision, *see supra* note 12, ¶ 42, at 13,051, but it thought its behavior was justified under the reasonable network management exception, which, at the time, was undefined. Though reasonable network management has become more defined, *see* Report, 76 Fed. Reg. at 59,208–10, ambiguities still exist, and access providers that must defend their actions will likely argue reasonable network management.

197 Report, 76 Fed. Reg. at 59,210. Others have made this claim. *See, e.g.*, Time Warner Cable Reply Comments to Notice of Proposed Rulemaking, WC Docket 07-52, FED. COMM. COMMISSION, 84–85 (Apr. 26, 2010), http://fjallfoss.fcc.gov/ecfs/document/view?id=7020437390 [hereinafter TWC Reply Comments] (stating that flexibility is necessarily to "allow network operators to experiment and innovate as user needs, usage patterns, and technology change (often rapidly) over time"); Verizon Comments to Notice of Proposed Rulemaking, WC Docket 07-52, FED. COMM. COMMISSION, 82 (Jan. 14, 2010), http://fjallfoss.fcc.gov/ecfs/document/view?id=7020378523 (stating that there is a variety of harm that can befall a network, and network operators must "be able to act dynamically and quickly in the face of . . . evolving threats.").

However, as access providers increasingly treat content unequally (especially through commercial agreements),[198] the less likely end-users will want to innovate because costs of innovation increase.[199] The question then becomes which type of innovation to prefer. As discussed above, the social benefits conferred by user-generated content[200] are enormous, and there is no evidence related to access provider innovations having a similar effect on society.[201]

Though it may be difficult to sympathize with the convenience argument, the FCC found it at least somewhat persuasive, as the Report gives access providers much latitude by its use of broad standards. To see why the FCC was convinced, a closer examination of the arguments put forth by access providers regarding the necessity of loose standards is required.

B. *Access Provider Business Models Do Not Justify Subversion of Neutrality*

Access providers argue, for a variety of reasons, that they need a broad exception so they can deal effectively with network issues as they arise without violating regulations.[202] The first reason is congestion management. Because Internet use is exploding,[203] without being able to manage networks, they can become congested and negatively impact other users' experiences.[204] Access providers argue they should be able to ease congestion problems without having to resort to expensive broadband capacity upgrades,[205] and those costs would then be passed to the customer.[206] In addition, Time Warner Cable claims "traffic that primarily causes congestion problems soaks up *all* bandwidth."[207]

198 Report, 76 Fed. Reg. at 59,195, 59,196.
199 VAN SCHEWICK, *supra* note 3, at 289–95 (discussing generally the effects on incentives to innovate at the end-user level when the network becomes increasingly centralized and controlled by network providers).
200 This even includes Facebook status updates, Twitter tweets, blog entries, as well as applications themselves such as Skype, Netflix, YouTube, and open source software.
201 VAN SCHEWICK, *supra* note 3, at 272 ("[U]nder the conditions present in today's Internet the increase in application-level innovation by network providers cannot offset the reduction in innovation by independent producers.").
202 *See, e.g.*, Cablevision Reply, *supra* note 149, at 11.
203 *See Internet Usage Statistics*, *supra* note 19; *see also* Bennett, *supra* note 166 (stating Skype requires millisecond delivery time and peer-to-peer transactions "can run for hours and involve gigabytes of data").
204 *See, e.g.*, Cablevision Reply, *supra* note 149, at 9; Comcast Reply Comments to Notice of Proposed Rulemaking, WC Docket 07-52, FED. COMM. COMMISSION, 36 (Apr. 26, 2010), http://fjallfoss.fcc.gov/ecfs/document/view?id=7020437448 ("Adding capacity to a network takes time, while congestion must be dealt with immediately.").
205 *See* Press Release, National Cable & Telecommunications Association, New Study Shows Cable Industry Contributes 1.8 Million Jobs and $251 Billion to U.S. Economy (Mar. 7, 2011), http://www.ncta.com/ReleaseType/MediaRelease/New-Study-Shows-Cable-Industry-Contributions-to-U-S--Economy.aspx (stating that the broadband industry has invested over $170 billion in broadband infrastructure during the last fifteen years).
206 TWC Reply Comments, *supra* note 197, at 84.
207 *Id.* at 86; *see* TWC Comments, *supra* note 149, at 66–67 (discussing applications that are designed to "consume all available bandwidth"); *see also* AT&T Comments, *supra* note 20, at 183.

Providers argue that in order to provide fair allocation of bandwidth to all subscribers, as well as keep prices down, unequal treatment of content is required.[208]

This assertion is inadequately supported. While an increase in broadband users and bandwidth-intensive uses could potentially cause congestion where amount of traffic exceeds available bandwidth, this merely represents an increase in demand for that bandwidth. Access providers should increase supply to meet the demands, and to do that, they should invest in capacity upgrades.[209] The costs of capacity upgrades may be recouped by access providers, without unequal treatment of content, from those using the capacity.[210] Though this represents a de facto subsidization of heavy users by light users,[211] this is comparable to consumer surplus in other markets. Some consumers are willing to pay a higher price for a particular good, but because they do not have to, they are effectively being subsidized by those that are only willing to pay less. Those only willing to pay below market value do not purchase the good, nor would they purchase Internet access from a broadband provider under the same rationale. In addition, light users share in the positive spillovers just as heavy users do.

Beyond congestion, access providers argue that they should be able to prioritize content if it is "unwanted" by end-users, such as pornographic material.[212] Providers reason that this is acceptable because the user, not the provider, is discriminating.[213] Additionally, the Report allows access providers to offer specialized services on top of Internet access that block harmful traffic, or provide built-in parental controls.[214]

Importantly, these issues have brought about a market for anti-virus and anti-malware software,[215] which allows users to protect

---

208 *See, e.g.*, TWC Comments, *supra* note 149, at 67–68.

209 FRISCHMANN, *supra* note 5, at 314 ("Congestion on the Internet should be managed primarily through expanding capacity and implementing usage-sensitive or congestion pricing, rather than accepting prioritization and encouraging persistent congestion.").

210 This could occur through usage-based pricing rather than service provider imposed discrimination.

211 *See* Yoo, *supra* note 161, at 203.

212 TWC Comments, *supra* note 149, at 72; Verizon-Google Legislative Framework Proposal, GOOGLE, 1, http://docs.google.com/viewer?url=http://www.google.com/googleblogs/pdfs/verizon_google_legislative_framework_proposal_081010.pdf&pli=1 (last visited Sept. 3, 2011). This was ultimately adopted by the FCC. Report, 76 Fed. Reg. 59,192, 59,209 (Sept. 23, 2011) (to be codified at 47 C.F.R. pts. 0 and 8), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-09-23/pdf/2011-24259.pdf.

213 *See* TWC Comments, *supra* note 149, at 72-73 (stating that access providers should be allowed to block things such as pornography and peer-to-peer file sharing applications so long as the "subscriber expressly approves of them"). There is a variety of traffic harmful to users that would probably benefit users to have filtered out by their access providers, including viruses, trojans, and spam.

214 The FCC realizes plans like these have the potential to be overinclusive, so it requires that users have the option to opt-in or out of any service the access provider provides. Report, 76 Fed. Reg. at 59,209.

215 Norton Internet Security, McAfee Security, AVG Anti-virus (a free anti-virus program),

themselves rather than requiring access provider intervention. In addition, access providers provide their own, sometimes free, anti-virus software to their consumers.[216] The variety of options available to consumers to protect themselves seems to obviate the need for access providers to discriminate in this context. The software market has protected Internet users from security threats for many years, which adequately protects consumers and militates against allowing access providers to manage the network.[217]

Additionally, access providers argue that network security breaches and other harmful traffic targeted at the network itself requires that they manage the network. According to access providers, there are severe network- and security-related problems that arise for engineers, for instance, hardware and network failures.[218] AT&T calls cybersecurity threats "[p]erhaps the most pressing network management challenge of all . . . ."[219] Because of increases in hacker activity, and the ever-present threat of natural disasters, networks themselves could potentially be at risk.[220] Giving access providers the ability to protect themselves and their investment is a good idea, especially given the potential commercial and societal consequences of allowing the network itself to fail. Therefore, such an exception can be stated as a rule, which might say if an access provider is confronting traffic that is harmful *to the network itself*, then that is acceptable network management. However, the Report is still too broad in its description of network security and integrity issues.

The reasonable network management exception currently allows

Kaspersky anti-virus, Symantec, and Webroot are all designed to block viruses and malware. Additionally, pornographic material can be blocked via software.

216 *E.g.*, *Constant Guard from XFINITY*, COMCAST, http://xfinity.comcast.net/constantguard/?cid=NET_33_640 (last visited Sept. 3, 2011).

217 This has privacy implications as well. In order for an access provider to determine if a packet contains a portion of a virus, spam, malware, or pornography, it must necessarily look into *all* packets to determine if it contains a piece of the harmful traffic. This creates serious privacy concerns; access providers can see and store everything a user does, and the user may not fully understand that this is a consequence of having her access provider block certain traffic. *See generally* Ohm, *supra* note 8.

218 AT&T Comments, *supra* note 20, at 183–84; *see* Comcast Reply Comments, *supra* note 204, at 35 (hardware and network failures include cable cuts, natural disasters, and other disruptions). For example, the recent earthquake in Japan cut access over many broadband cables. *See* James Cowie, *Japan Quake*, RENESYS BLOG (Mar. 11, 2011, 7:20 PM), http://www.renesys.com/blog/2011/03/japan-quake.shtml (stating that the Japan earthquake has had "surprisingly limited impacts on the structure and routing dynamics of the regional Internet. . . . Despite terrible fires, floods, and power outages, traffic from Japanese clients just keeps going."). This disaster may even cut against the argument that access providers need to be able to prioritize traffic to deal with natural disasters; however, it may just be a coincidence that this natural disaster had a small impact.

219 AT&T Comments, *supra* note 20, at 184 ("The [Government Accountability Office] reported a *206 percent* increase in reported cybersecurity incidents between 2006 and 2008. AT&T's network engineers report almost 39 million hacker indicators *each month*.").

220 For a variety of risks to cyber security, see *Cyber Security*, PUBLIC SAFETY AND HOMELAND SECURITY BUREAU OF FCC, http://www.fcc.gov/pshs/emergency-information/cybersecurity.html (last visited Mar. 27, 2011).

management based on ensuring "network security and integrity."[221] The Report lists the following as conforming to that end: spam, botnets, and distributed-denial-of-service ("DDoS") attacks.[222] The case has not been made that these are actually harmful to the *network itself*. While this traffic may harm end-users, and in great numbers,[223] there are end-user solutions for most of these problems.[224] DDoS attacks are arguably rare,[225] and the reasonable network management exception should not be made overbroad in order to accommodate tactics to fix a relatively rare occurrence.

Jonathan Zittrain, a Harvard Law School Professor and an Information Law scholar,[226] makes the argument that a substantial contingent of compromised end-systems can create vulnerabilities that can lead to a "catastrophic security attack"[227] of the network itself. However, the severity of this potential threat is unclear, and without more evidence that such an attack is more than simply theoretical, or has the potential to undermine the Internet generally, the regulation should not provide for such an overbroad exception.[228] The societal impact of eroding network neutrality is not justified by such hypothetical arguments, though the regulation could be reworked if further evidence were presented.

---

221 Report, 76 Fed. Reg. 59,192, 59,208 (Sept. 23, 2011) (to be codified at 47 C.F.R. pts. 0 and 8), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-09-23/pdf/2011-24259.pdf.

222 *Id.* at 59,209 n.102. A distributed-denial-of-service attack is defined as the following:

> In a distributed denial-of-service (DDoS) attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He or she could then force your computer to send huge amounts of data to a website or send spam to particular email addresses. The attack is 'distributed' because the attacker is using multiple computers, including yours, to launch the denial-of-service attack.

Mindi McDowell, *National Cyber Alert System: Cyber Security Tip ST04-015*, UNITED STATES COMPUTER EMERGENCY READINESS TEAM, http://www.us-cert.gov/cas/tips/ST04-015.html (last updated Nov. 4, 2009).

223 For example, one virus, known as "Kneber botnet" breached almost 75,000 computers. Sakthi Prasad, *New Computer Virus Has Breached 75,000 Computers – Study*, REUTERS (Feb. 18, 2010, 6:10 AM), http://www.reuters.com/article/2010/02/18/computervirus-idUSSGE61H0D820100218.

224 See *supra* note 215 for a non-exhaustive list of software designed to deal with traffic harmful to end-users.

225 *Compare Understanding and Combating DDoS Attacks*, DELL SECUREWORKS, http://www.secureworks.com/research/articles/combatddos (last visited Sept. 3, 2011) (stating DDoS attacks are rare), *with* Audrey Watters, *DDoS Attacks Make Headlines, but How Common Are They?*, READWRITEWEB (Dec. 13, 2010, 3:39 PM), http://www.readwriteweb.com/archives/ddos_attacks_make_headlines_but_how_common_are_the.php (stating DDoS attacks are growing).

226 Jonathan Zittrain, BERKMAN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY, http://cyber.law.harvard.edu/people/jzittrain (last visited Mar. 29, 2011).

227 JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET – AND HOW TO STOP IT 165 (2008); *see also* FRISCHMANN, *supra* note 5, at 316.

228 *See* FRISCHMANN, *supra* note 5, at 316 ("The jury is still out on this issue, and there may very well be innovative solutions developed and implemented by end-users, including firms or other organizations acting on behalf of and in the interest of individual end-users.").

C. *Is a Standard-like Regulation Better than No Regulation?*

Edward Felten, the Director of the Center for Information Technology Policy and Professor of Computer Science at Princeton,[229] makes the argument that simply the threat of network neutrality regulation is better than regulating it.[230] He reasons that if access providers begin discriminating now, it will only appear to make regulation more necessary. In addition, it avoids the complicated line-drawing and enforcement problems inherent in network neutrality regulation.[231] Access providers would prefer to have no specific rules set, as regulation may only constrain them.[232] As a result, according to Felten, access providers should be on their best behavior in order to give the impression that regulation is not required.[233]

While this may have been true in 2006 when the argument was first made, it is less true today. If regulators had taken this advice and only threatened regulation, it is likely that access providers would have started to treat content unequally because, eventually, they will need to know what is allowed. It should be noted that the year after Felten's paper was published, Comcast blocked BitTorrent on the theory that it was reasonably managing its network.[234] Clearly, the threat of neutrality regulations did not work for Comcast, and it would eventually spur more experimentation by other access providers as well.

Continuing to threaten regulation but never passing any would have been cause for concern. During the Open Internet proceedings, the FCC was repeatedly criticized for its delay in regulating neutrality.[235] The Verizon-Google Legislative Framework was written *because* of agency inaction.[236] Threatening providers with regulation will only work in the short-term because eventually the FCC's hand will be forced by an impatient public.

* * * *

While there are many purported justifications for a flexible, broad, standard-like regulation, few of them are compelling enough to allow the systematic subversion of one of the central tenets of the Internet.

---

229 Edward W. Felten, http://www.cs.princeton.edu/~felten (last visited Mar. 29, 2011).
230 Edward W. Felten, *Nuts and Bolts of Network Neutrality*, REGULATION2POINT0, 11–12 (2006), http://regulation2point0.org/wp-content/uploads/downloads/2010/04/php9e.pdf.
231 *Id.*
232 *Id.* at 11.
233 *Id.*
234 *See 2008 Comcast Decision*, *supra* note 12, ¶ 42, at 18,302.
235 Press Release, Free Press, FCC Delays Rulemaking on Net Neutrality Again (Sept. 1, 2010), http://www.freepress.net/press-release/2010/9/1/fcc-delays-rulemaking-net-neutrality-again; Elizabeth Woyke, *FCC Requests More Comments on Net Neutrality, Gets Criticized*, MEDIA ACCESS (Sept. 1, 2010), http://www.mediaaccess.org/2010/09/fcc-requests-more-comments-on-net-neutrality-gets-criticized (quoting Free Press Research Director S. Derek Turner).
236 *See* Richard Whitt, *Facts About Our Network Neutrality Policy Proposal*, GOOGLE BLOG (Aug. 12, 2010, 10:57 AM), http://googleblog.blogspot.com/2010/08/facts-about-our-network-neutrality.html ("We're simply trying to offer a proposal to help resolve a debate which has largely stagnated after five years.").

Neutrality has allowed for immense social and commercial value, as well as personal value for the end-user. The freedom to see, read, write, and accomplish almost anything gives the Internet its value and power in our society, and much of that benefit goes unmeasured because positive externalities are not quantifiable. Any justification that argues convenience, cost-savings, the unknown nature of future technology, or customized user experience does not justify casting aside the neutrality principle.

The interest of network integrity and security, however, *can be* justifiably invoked to allow for network management. However, as stated above, the Report's language regarding this principle needs to be reworked.

V. A PROPOSED RULE-LIKE EXCEPTION

Based on the discussion above, the only justification for a network management exception is for network security and integrity. As such, this Note suggests to avoid the "reasonable" terminology that requires an augmented proceeding, and instead to create an exception that deals specifically with network security and integrity. Wording for such an exception could consist of the following:

> An access provider may manage its network if the management technique is narrowly aimed at ensuring network security or network integrity. Network security relates to harm to the network caused by cybersecurity threats, hackers, or other harmful attacks designed to undermine the security of the network itself. Network integrity relates to problems with the physical network infrastructure, including natural disasters.

This proposal removes the reasonableness standard, and simply states that if the management practice is narrowly aimed at alleviating a network security or integrity issue, then the practice is acceptable. The proposal removes congestion management and end-user requested content discrimination as acceptable behavior. Congestion should be dealt with through increasing the supply (investing in capacity upgrades) to meet the demand of users, and end-users will have to purchase software or find another way to block particular content if they wish to do so.[237] DDoS attacks may be included within the exception if it is proven that it is a harmful attack directed at the network itself.

This proposed exception does not remove all future discretion, as the proposal does not define every term. However, it does favor false positives and thus will reduce discriminatory behavior in that it provides a narrower purpose, making the exception more rule-like. This proposal will serve both providers and users well.

---

237 *See supra* note 215 and accompanying text.

CONCLUSION

Regulating network neutrality is difficult. There are a variety of tradeoffs having to do with regulating by rule or standard, and whether to favor false positives or false negatives. There are a lot of interests at stake, and balancing those interests is required. An appropriate balance can be accomplished by looking at the context of the particular problem, and the realities of enforcement and competition. Because neutrality has provided significant benefits to society, the neutrality principle's importance is paramount to many countervailing interests such as reduced investment, reduced ability to optimize the network for certain applications, or reduced opportunity for access provider innovation.

As it stands now, the broad reasonable network management exception provides a likely vehicle for access providers to justify their behavior, *if* a complaint is even filed. As such, a confined, more rule-like, exception that removes the reasonableness inquiry is suggested. A more standard-like and broad exception would serve to unnecessarily favor access providers over other parties and participants in the debate.

There is a common, and apt, axiom in today's lexicon: if you give an inch, they take a mile. But the FCC, in this context, appears to be giving access providers the whole mile, allowing providers the ability to request and receive even more miles. Neutrality deserves more protection than that.

Eric Null[*]

[*] Senior Articles Editor, CARDOZO ARTS & ENT. L.J. (2011-2012); J.D. Candidate, Benjamin N. Cardozo School of Law (2012); B.A., University of Vermont (2009). A special thanks to Professors Susan Crawford and Brett Frischmann for your invaluable help and guidance. I thank my notes editor, Jennifer Haberman, as well as Barbara Kessler and Nick Russell for your time and effort, and I thank Julia Kessler for your support in this process. Lastly, thank you to the *Cardozo Arts & Entertainment Law Journal* editorial board for your hard work.