Net Neutrality is Not Open Internet

Data Foundry, Golden Frog and GigaNews have long been strong supporters of the Open Internet, and this has been expressed in both word and deed. Our policy publications consistently advocate for openness, freedom, liberty and privacy. Our products are entirely focused on providing a means for people to enjoy the immense benefits flowing from the Internet, individually exercise freedom and liberty and preserve their privacy. So when we state that we are glad the D.C. Circuit Court of Appeals has vacated the Federal Communications Commission’s Net Neutrality “nondiscrimination” and “no blocking” rules you may be perplexed or confused, especially given the moaning and gnashing of teeth you may have heard elsewhere. Allow us to explain.

Open Access is good, while Net Neutrality is actually bad. Net Neutrality is not “Open Internet” even though the “Net Neutrality rules themselves deceptively claim to be in place to preserve “the Open Internet.” The court’s vacatur of the nondiscrimination and no blocking portions of the FCC’s rules provides an opportunity for the Commission to once again embrace and preserve Open Access, which is the only practical and reasonable way to once again ensure Open Internet in the United States.

Open Access was accomplished through the original “service unbundling” paradigm instituted by the FCC in its seminal Computer Inquiry proceedings, along with the interconnection and “facility unbundling” concept put in place by the 1996 amendments adding §§251 and 252. It is then flavored and supplemented by other FCC competition-enhancing efforts with regard to customer premises equipment and inside wiring.

There is a significant difference between “Open Internet” (also known as “Open Access”) and “Net Neutrality” as that phrase has been applied in the United States. The FCC abandoned Open Access when it closed off competition by multiple access providers over the transmission facilities deployed by the incumbent telephone and cable companies. This radical about-face occurred in the late 1990s, and completed in the early 2000s through a series of cases involving how enhanced/information service providers obtained access to infrastructure, and then changing the regulatory classification for “broadband” provided by cable, telephone companies, wireless providers and broadband over powerline.\(^1\) They did this despite the fact that the current Communications Act was almost entirely built around competitive access to unbundled monopoly or duopoly transmission facilities, the epitome of “Open Access.” Much of the rest of the world followed the original U.S. model and embraced Open Access, and they retained it even after the FCC reversed course. That is why there is far more competition abroad, better and faster Internet capabilities and lower prices.

The Organisation for Economic Co-operation and Development (OECD)\(^2\) does not have a formal definition of “Open Access”\(^3\) but their publications do recognize some common elements:

---

2. The OECD is an international treaty organization focused on economic development that has its origins in the “Marshall Plan” that was used to rebuild Europe after World War II. See http://en.wikipedia.org/wiki/Organisation_for_Economic_Co-operation_and_Development. One of organization’s focus is encouraging the deployment of the Internet, and it has a primary policy of encouraging Internet freedoms. They have published a host of studies and policy recommendations on this topic. See http://www.oecd-ilibrary.org/ and use “Internet” as search term.
wholesale access to network infrastructure or services provided on fair and reasonable terms, for
which there is some degree of transparency and non-discrimination. For fixed networks, Open
Access policies usually take the form of mandated regulated access, such as local loop
unbundling, and other wholesale access products, sometimes up to the next layer (e.g.,
bitstream). Key access products include dark fiber services, access to ducts and in-building
wiring. Policy makers and regulators in most countries realize that these infrastructure elements
represent a major barrier for the entry of alternative operators.

Net Neutrality is a completely different thing. Indeed, Tim Wu, who is credited
with crafting the term and concept, took great pains to distinguish “Net Neutrality” from
“Open Access” in his original paper that introduced the topic.4 Open Access is about
opening essential infrastructure to competition. Net Neutrality accepts that there is no
Open Access, and begins to regulate the Internet rather than just essential facilities used
to access the Internet.

Wu, and the FCC (which largely adopted his principles as it closed off competitive access
and then promulgated the “Net Neutrality” rules”) basically concluded that retaining Open
Access as a regulatory policy would not provide sufficient incentives for the telephone
companies and cable companies to invest in broadband transmission. Then they came up with
“Net Neutrality” as a means to partially ameliorate the fact that this necessarily destroyed all
possibility for there to be competition in the Internet Access market, because the elimination of
Open Access meant that the incumbents had monopoly control of both the “transmission” market
and the adjacent “Internet Access” market.

They were wrong. The elimination of Open Access and then the instruction of Net
Neutrality rules led to the worst of both worlds. The Net Neutrality “cure” only led to more
disease. The FCC wrongly succumbed to the incumbents’ threat to not invest in infrastructure
unless they were given complete monopoly control over all use of the facilities and allowed to
extract more value from the communications flowing over them. The Net Neutrality “fix” was
half-hearted, had no real meaning or enforcement teeth, and it actually made things worse,
especially when it comes to the privacy of users’ information.

We explain those charges below, but will first briefly challenge the whether the
incumbents would not have deployed broadband if they were not allowed to off to all
competition in return. It is not true. The incumbents robustly improved the telecommunications
network for decades even after Open Access principles were developed beginning in the 1960s.
The FCC embraced Open Access as a means to facilitate competition in a series of cases related
to interconnection, customer premises equipment, inside wiring and enhanced/information
services. The incumbents had no real choice but to continue investing, because their profits came
from a “return on investment” under traditional regulatory principles; if they failed to make new
investment they earned less profit.

Besides, set aside all the jargon and look at it from a practical perspective: if you are a
wires company then you will survive only if you keep making new wire. The rest of the world

4 Wu, Tim, Network Neutrality, Broadband Discrimination, Journal of Telecommunications and High Technology
were promulgated through the FCC’s Report and Order, In re Preserving the Open Internet, 25 FCC Rcd. 17905
understands this, and investment overseas has been made at far greater levels than in the United States in recent years even under Open Access. The FCC simply lacked the will to actually enforce its longstanding Open Access rules – so it got rid of them in a magnificent example of “regulatory capture.”6 The incumbent controllers dislike Open Access, and the captured regulator did their bidding by killing it. We are all now suffering the consequences from the FCC’s decision to put the incumbents’ interests over the public’s interest. The new administration should accept that this was a huge mistake, and re-embrace Open Access.

The FCC’s earlier pro-competitive policies most pertinent to the Internet were made in the “Computer Inquiry” proceedings, where the FCC specifically and expressly idealized the rise of unregulated “Value Added Networks” that had specific rights to access facilities and services such as local plant so they could provide “enhanced service.” The Computer Inquiry rules were Open Access if you use the OECD’s recognized elements. Those decisions directly and inexorably led to the rise of the Internet; indeed, the FCC itself – until relatively recently – repeatedly emphasized that the Internet as we know it would not exist but for the Computer Inquiry Open Access rules.7 Net Neutrality was “needed” only because the FCC decided to abandon the prior Open Access rules that had been in place for almost 40 years and were a prime reason the Internet arose as a primary communications tool.

There are too many reasons why the Net Neutrality rules (as opposed to open access) are misguided, misconceived and counterproductive than can be discusses in this piece. But the following discussion of only some of the major problems shows that the Net Neutrality “fix” was half-hearted, had no real meaning or enforcement teeth, and it actually made things worse, especially when it comes to the privacy of users’ information. The approach – regulating “Internet Access” rather than mandating open access to infrastructure – was misguided, and consigned to inevitable failure.

---

6 See http://en.wikipedia.org/wiki/Regulatory_capture: “Regulatory capture is a form of political corruption that occurs when a regulatory agency, created to act in the public interest, instead advances the commercial or special concerns of interest groups that dominate the industry or sector it is charged with regulating. Regulatory capture is a form of government failure; it creates an opening for firms to behave in ways injurious to the public (e.g., producing negative externalities). The agencies are called ‘captured agencies.’” The Wikipedia article specifically lists the FCC as one of several U.S. “captured agencies.”

7 A fine collection of such observations appears in The FCC and the Unregulation of the Internet, FCC OPP Working Paper 31, July 1999, available at http://transition.fcc.gov/Bureaus/OPP/working_papers/oppwp31.pdf: Open access across the telecommunications network has driven the deployment of innovative and inexpensive Internet access services. … the growth and continued success of the Internet, and the ability of market forces to sustain and encourage that growth, can be attributed to one basic attribute: the openness of both the Internet and the underlying telecommunications infrastructure. … To the extent that the Internet has relied on the openness of this nation’s communications infrastructure to reach all corners of this nation, this ingredient in its success has not been an accident. The FCC has taken numerous steps since the early days of the telecommunications data services industry three decades ago to permit competitive forces, not government regulation, to drive the success of that industry. As discussed in greater detail below, the success of the Internet today is, in part, a direct result of those policies. … First, the Commission noted that data processing services required common carrier facilities and services as necessary inputs, and common carriers that offered their own data services would have the ability and incentive to discriminate against unaffiliated data service providers by denying them access to fairly priced telecommunications services. Second, the Commission noted that common carriers might improperly cross-subsidize their unregulated data processing services with rate-regulated common carrier revenues.
The FCC committed a logical error. The “problem” did not reside with those who provide “Internet”; it arose because transmission is still a monopoly (or a duopoly). From a technical and economic perspective “transmission” and “Internet Access” are two separate markets, although they are adjacent. Once again, the FCC recognized this very thing in Computer Inquiry; indeed the very purpose of that proceeding was to isolate monopoly components, and impose regulation on the monopoly activity, while deregulating potentially competitive “enhanced” services.

The “Internet Access” service sector could quite easily be fully competitive, if only the underlying bottleneck transmission components remained available on a common carrier basis to all potential purchasers. That is precisely how it worked in the “dial-up” days and the move to “broadband” does not justify a different result. If we returned to Open Access and allowed competition to return to the Internet Access market then any “Internet Access” provider that failed to act consistent with consumer expectations would quickly be faced with alternative providers that offered price and other terms that users really want. As it stands, however, the “last mile” transmission input is available only to the telephone and cable companies for “Internet Access.” They therefore can now monopolize (or duopolize) both the transmission and the “Internet Access.” As the FCC had recognized for 40 years, this kind of vertical integration and leveraging inexorably leads to discrimination and rationing as a means to keep prices artificially high, and therefore profits greater than would prevail in a competitive market.

There’s a reason that the incumbents fought so hard to leverage their dominant position over infrastructure into control over the adjacent “Internet Access” market. They get to extract monopoly rents from both sectors. Now they can create toll roads on the data freeway that, rather than charging by the mile (or gigabyte), engage in pricing that varies depending on the provider’s perceived value of the content rather than the cost of delivering the bits.

The cost of delivering a megabyte or gigabyte does not vary depending on the “value” of the “content.” No provider could impose “value” pricing in a competitive Internet Access market where a host of different ISPs could obtain open access to the incumbents’ wires in a given area and would have to compete with each other through lower prices and/or better respect for customer desires. But it is entirely possible when there is only the telco and the cable company. The FCC’s Net Neutrality rules – despite all of the high-minded words and concepts – accept a duopoly for both transmission and Internet access, and pretend to band-aid some of the downsides. But they are toothless and ineffective. And they do nothing to control price levels, which would certainly be lower in a competitive market.

Another problem is that “Net Neutrality” concepts were based on premises that simply do not apply to “the Internet.” The bureaucrats don’t understand what the Internet really is. They think it is merely a fancy phone or cable network. Martin Geddes recently explained the basic problem:

---

8 “Internet Access” depends on transmission service inputs, but they are logically and practically separate markets. From an antitrust perspective the FCC basically allowed the incumbents to engage in monopoly leveraging and then a tying arrangement.

9 Many of the activities identified as “problems” in this entire debate would not much of a concern if there was a competitive market. A provider’s attempt to impose “content value” pricing, or even “discrimination” simply would not succeed if there were alternatives – unless consumers decided that is what they actually want. If that is what they want, then the activity is merely fulfilling consumer desires and that is a good thing. The problem arises when the two dominant providers impose these results, despite rather than because of consumer desires.
The neutrality concept takes as its starting point a reasonable desire: fair user access to the network, on fair terms, and at a fair price. However, it then engages in a philosophical error: it anthropomorphises packets – as if they were people or physical packages. This creates a false equivalence between what are arbitrary divisions of flows of data. This mistaken treatment then results in an inappropriate application of previous common carriage principles to a fundamentally incompatible type of communications system. The net effect of network neutrality is to enforce the highest possible cost structure and the worst possible quality of experience onto users.¹⁰

In addition, Net Neutrality proponents simply refused to accept that the nondiscrimination rule cannot work as advertised because it in fact still allows and sometimes even requires the access provider to discriminate. It sounds strange, but is true. The Order implicitly recognized this in paragraph 77 when it says that “A strict nondiscrimination rule would be in tension with our recognition that some forms of discrimination, including end-user controlled discrimination, can be beneficial.” No normal human being can parse that statement and come to any conclusion other than the alleged “ban” on discrimination is no such thing. In application, and in particular when the huge loophole created by the “reasonable network management” exception is also considered, the rule expressly allows, and sometimes even requires, discrimination.

The best example of this is the FCC’s explanation that “packet prioritization” as part of service to consumers is “likely” not unreasonable discrimination” (¶71). First, you must understand that the FCC’s (and the incumbents’) version of “packet prioritization” is not based on class-based Differentiated Services (“DiffServ”),¹¹ which allows a customer to provide priority instructions in the “DS field” of the IP header, or flow-based Integrated Services (“IntServ”), which also uses customer-specified instructions in specified headers.¹² Their version is something completely different. It stems from the overarching requirement that access providers not discriminate between “lawful” applications, services, or non-harmful devices, and the permission to give priority to “latency sensitive” applications. While these sound nice and high-minded, they once again misunderstand how the Internet works.

Allowing or requiring an access provider to classify and prioritize packets by “application” so that “latency-sensitive applications” receive favored treatment, and “latency-insensitive applications” can be given lower priority is wrong if it uses any provider-chosen

Net Neutrality is Not Open Internet

mechanism other than DiffServe and/or IntServ. The inferential methods allowed by the FCC use things like port, source and destination information. These are unreliable and can be easily manipulated. They do not, in fact, tell you much about the application type or any notional sensitivity to latency.

But it gets worse. Classification by type for network provider prioritization can only be accomplished through deep packet inspection of content, which presents severe privacy and security problems. That is discussed below. There are other problems as well. Any regulatory regime that requires or allows network providers to classify “applications” for packet prioritization – and particularly one that requires “similar” applications to receive “like” treatment – will be extraordinarily contentious and lead to constant disputes. Classification by “application type” tells the provider to classify each application by “type.” They could, for example, refuse to recognize a new application “type” until it becomes mainstream or sufficiently popular. Further, this would mean that the Internet Access providers can ignore or simply overrule Internet standards (consensus) efforts.

Two hypothetical examples demonstrate the problem.

A. Someone devises a new application, let’s say something called “instant messaging” or “IM.” This application allows parties to send text messages, exchange live audio and video, do whiteboards, and swap files. It is brand new and this is the first application that has these functionalities, so there is no as-yet recognized “IM” market or class of similar applications. It depends on low latency and is sensitive to jitter. Each provider, under the gun to assign priority that is the same as other “like” applications has to classify. Let’s get our committee of telco blind men and have them figure out what that elephant is. “This part feels like ICQ.” “That part smells like video.” “There’s a portion that sounds like ‘voice’” “This part stomps around like email.” “No, it’s shaped just like FTP or Telnet, only different.” The Internet Access provider gets to choose which of the above “application types” “IM” is “like,” but it has no requirement to ever create a new category called “IM” – even when several other folks create similar competing products. All subsequent “IM” clients are categorized the same way as the first for “nondiscrimination” and “network management” purposes, even if they have different or unique characteristics and may be either more or less sensitive to latency or jitter.

B. Someone devises a new application for audio. It lets users create and merge audio from multiple sources, do mashups, and has a mixer. People can share and collaborate on-line, sort of like Google Docs and Spreadsheets. It can stream, or not stream. It uses unique file extensions. It also has a “voice” capability, both real-time and store and forward. At what point does the provider have to “recognize” this new application type so as to classify and prioritize it the same way as all the others that are arguably like, and differently from those that are not like? What are the criteria for determining “likeness”? What if the important distinctions and similarities are subjective, not objective, and thus the determination varies based on each individual’s preferred grounds of distinction? Is it really the place of either the government or the network provider (as opposed to the market) to make these classification decisions and therefore decide it is unique and belongs in its own poorly-treated or, alternatively, preferred, class?

The attempt by some to appear reasonable by conceding the ability to prioritize by “type” while prohibiting “discrimination” of “like” applications is an invitation for constant disputes and allows the government and/or the dominant providers to shape the market. The incumbents
have the incentive and ability to act in anti-competitive ways – and quite often do so. Why then would we give them this kind of power when we know they will abuse it? The government too has its own biases.

The discussion about some applications’ (especially those involving “video” or “voice”) latency sensitivity and need is misplaced. Despite what you may have heard, from a practical perspective there are no “latency-insensitive applications.” There are only transitory instances where individual users are not as concerned that particular information may be delayed or subject to jitter. Some applications, in comparison to other applications, do not satisfactorily function when there is considerable latency or jitter. But no application is “insensitive” to latency. Users get annoyed when particular datagrams are delayed regardless of whatever application they are using. Latency effects every application and every user.

The FCC said that Internet Access providers can pick one application over another, and in particular can “prioritize” “voice” or “video” to the detriment of other applications like “web browsing.” They seem to think users do not get irritated when their web page loads slowly, but that is clearly not true. There is an entire market niche for “CDNs” such as Akamai whose entire business is about supporting faster loads for “simple web browsing” by reducing the latency for web traffic. The Net Neutrality rules could easily be applied in a way that wholly eliminates the benefit of CDNs. The “web” user suffers while the “voice” and “video” users get priority.13

We have saved the best for last. The main reason we oppose Net Neutrality is that it absolutely destroys privacy. The FCC and the providers of course will not tell you this, but the “Net Neutrality” rules can only be implemented through extensive Deep Packet Inspection. Let’s just pick one example, although there are many more.

One of the Net Neutrality rules is 47 C.F.R. §8.9(b), which says “Nothing in this part prohibits reasonable efforts by a provider of broadband Internet access service to address copyright infringement or other unlawful activity.” Ask yourself: how can an Internet Access provider detect whether any given group of datagrams represents content that is “copyright infringement” or “unlawful activity” unless they can see the content? This rule tells the Internet Access provider that it can look at your content. As a practical matter this means they can make a copy and store it to allow some human to decide whether it is infringing or unlawful. If they decide it is infringing or unlawful what will they then do? Why, of course they will turn it over to the authorities. But even if they don’t initiate the conversation with the government the government itself can independently ask the provider to give up your content and allow the government to decide if you have sent or received “unlawful” content.

But, you say, they’d have to get a warrant. Not true. American Internet Access providers can choose to voluntarily turn over your content, without any kind of “due process.” Under 18 U.S.C. §2701(c) a provider can choose to hand over your content at its whim, without notice to

13 Once again, however, if this were under user control, a user that is doing both web browsing and using a VoIP client could self-prioritize between the two applications she is running through DiffServe and IntServ. But the Net Neutrality rules don’t use this method. The rules in fact encourage and sometimes even mandate that the provider discriminate between applications because they expressly contemplate that Internet Access provider will unilaterally assign relative priority between applications and users without regard to – in fact sometimes despite – the users’ preferences.
you, without any kind of due process and wholly without any subpoena, judicial order or warrant.\(^{14}\)

At this point maybe you have grasped that all the prominent public officials who proclaim that the government does not and cannot get your content without due process are not telling you the truth. And maybe you now understand why AT&T, Verizon, Time Warner and Comcast have been fairly silent about things like the Snowden revelations. But we will tell you the truth: everything you send or receive on the Internet can be captured and stored somewhere. It is available to the provider and the government any time they want to look at it. The FCC’s “Net Neutrality” rules were carefully designed to ensure this very result. One might plausibly conclude that the FCC ended Open Access and replaced it with “Net Neutrality” to, among other things, support the U.S. government’s overall efforts to institute a surveillance state. The government and its duopoly cronies have rigged the game, and you lose.

This was not just bureaucratic incompetence or inattention; to the contrary. We saw all of this coming and our lawyers (along with a few others\(^{15}\)) carefully and repeatedly explained to the FCC, the FTC and Congress during the entire time that what they were doing would end

---

\(^{14}\) The law does say the provider can refuse a government request, at which point some due process is required. But nothing requires them to insist that the government secure a subpoena, order or warrant. You are at the mercy of the duopoly players. If there was still Open Access, however, an independent ISP could provide the Internet Access and distinguish itself from the incumbents on the basis that it will never voluntarily turn over content without a warrant. Users that valued privacy could choose to use that company.


Relieved from common-carrier regulation and empowered by deep-packet inspection that allows ISP computers to scrutinize the packets of Internet traffic passing through their network, Comcast’s actions invigorated the debate about whether ISPs should be required to treat Internet traffic in a neutral manner. Professor Rob Frieden pointed out that “the ability to ‘sniff’ packets makes it possible for ISPs to deviate from ‘best efforts’ routing by discriminating on the basis of price paid for service and as a function of what kind of traffic a bitstream represents.” These practices highlight the clash between the open Internet standards of TCP/IP protocol that made it easy for anyone to develop an application to run on the Internet when ISPs were subject to common-carrier regulation, and the closed network management standards, technologies, and contractual provisions that restrict use of certain applications in the absence of common-carrier laws.

Professor Paul Ohm argues that “ISPs have the opportunity, means, and motive to engage in new forms of customer surveillance.” The opportunity, Ohm writes, stems from “the design of the network, as ISPs operate network chokepoints giving them the ability to access every bit leaving from and returning to a customer’s computer.” Improvement in computer processing power and new software enable inspection of every packet. Professor Ohm also points out that “economic pressures and the lack of ethical counterweights motivate them [ISPs] to sniff more packets.”

I argue that the removal of explicit legal prohibitions against Internet traffic discrimination, not just economic incentives and the lack of ethical norms, made deep-packet inspection proliferate. Computer power and software technologically enabled inspection of every packet, but the removal of common-carrier nondiscrimination requirements created the legal space for ISPs to take action based on that information. The Internet’s architecture cannot heal this problem through self-regulation because the Internet’s designers assumed that the physical layer that provided access to and carried Internet data would be neutral and simply transport data across the network. The Internet’s design presumed common carriage.
Net Neutrality is Not Open Internet

competition and destroy privacy. We and others told them about the consequences, so they knew exactly what they were doing.\textsuperscript{16}

After it became clear that the government was going to kill competition and destroy privacy we decided to develop the Golden Frog products users employ today in order to fight back against provider and government surveillance. VyperVPN and Chameleon encrypt user traffic, and defeat the duopoly providers’ Deep Packet Inspection. Yes, they see the bits, and yes they store them, but neither they nor the government can make any sense of it without extraordinary effort. It defeats the degradation the incumbents consistently do, but also persistently deny. We and our users noticed, for example, that VyperVPN users consistently get faster speeds for NetFlix when they employ the VPN, which indicates that this traffic is being identified and separately treated when it is “in the clear.” Dump Truck lets you encrypt your stored data too. And, we have committed to you that we will never voluntarily turn over your content to anyone without your consent. When they come to us we tell them to get a warrant. AT&T, Verizon, Comcast and Time Warner or any of the other duopoly incumbents will never, ever, make the same unequivocal promise.

So, please understand. Data Foundry, Golden Frog and GigaNews believe in Open Internet and our entire purpose is to preserve it. But Net Neutrality is not Open Internet. Indeed, it is the opposite. Don’t be fooled by politicians, bureaucrats and their plutocrat cronies that have conspired to destroy freedom and liberty by hiding behind words that sound good but justify action wholly antithetical to what the Internet is all about. Net Neutrality is a complete sham because it prevents competition, allows (and sometimes requires) discrimination and it destroys privacy.

We will have Open Internet only when the U.S. re-embraces Open Access. Net Neutrality is not Open Internet. This is why we applaud the D.C. Circuit’s decision. Our promise to you is that we will once again do all we can to tell D.C. policy makers that they must discard return to the Open Access rules that prevailed before the FCC got rid of them in 2002. The FCC must admit its error and once again require Open Access by mandating that telcos and cable companies have to unbundle their transmission, offer it on a common carrier basis, and reasonably facilitate competitors’ ability to interconnect with the transmission so they can in turn offer unregulated Internet Access.

Quit praising Net Neutrality, and instead work with us to actually once again have Open Access. Long live the Open Internet.

\textsuperscript{16} The FCC said this in paragraph 57 of the “Net Neutrality” Notice of Proposed Rulemaking, \textit{In re Preserving the Open Internet}, 24 FCC Rcd 13064, 13087 (2009) (notes omitted):

With deep packet inspection, a broadband Internet access service provider can determine which packets to favor by examining in detail the content of an email, or web page, or downloaded file. It is possible to distinguish music files from text from pictures, or to search for key words within any text.


We seek comment on how the Commission should treat issues such as deep packet inspection and behavioral advertising in developing a national broadband plan and whether there are issues related to other types of information connected with the provision of broadband services that the Commission should consider. Do these practices discourage consumers from “access[ing] the lawful Internet content of their choice” for fear of having that access tracked or revealed?