Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Preserving the Open Internet	)	GN Docket No. 09-191
	)	
Broadband Industry Practices	)	WC Docket No. 07-52

To: The Commission

COMMENTS OF T-MOBILE USA, INC.

Ari Q. Fitzgerald
Michele C. Farquhar
David L. Martin
Mark W. Brennan

HOGAN LOVELLS US LLP
555 Thirteenth Street, NW
Washington, DC 20004
(202) 637-5600

Thomas J. Sugrue
Kathleen O'Brien Ham
Amy R. Wolverton

T-MOBILE USA, INC.
401 Ninth Street, NW Suite 550
Washington, DC 20005
(202) 654-5900

Attorneys for T-Mobile USA, Inc.

October 12, 2010

TABLE OF CONTENTS

Page

INTRODUCTION AND SUMMARY 1

I. WIRELESS CARRIERS PRESENTLY PROVIDE MEANINGFUL AND TRANSPARENT NOTICE OF THEIR NETWORK PRACTICES AND POLICES 3

A. Wireless Carriers Already Provide Information on Service Practices and Policies to Consumers 3

B. Technically Detailed Disclosure Requirements for Wireless Network Management Practices Would Do More Harm than Good 6

C. Mandating Specific Public Disclosure of a Provider's Device and Application Requirements and Certification Processes Is Unnecessary 10

II. THE COMMISSION SHOULD NOT REQUIRE WIRELESS BROADBAND PROVIDERS TO ALLOW ANY AND ALL DEVICES AND EVERY APPLICATION ON THEIR NETWORKS 11

A. In the Competitive Mobile Wireless Sector, Network Providers Have a Strong Incentive to Enable Consumers to Use as Many Devices and Applications as Possible 12

B. Wireless Broadband Providers Must Have the Flexibility to Address Network Security and Reliability Risks and Other Threats to the Consumer Experience 14

C. Usage-Based Data Pricing and Industry Standards Cannot Fully Protect Consumers, Wireless Providers, and Networks From the Harms That Would Result from Mandates to Permit All Devices and Applications on a Network 17

D. The Proposed "Reasonable Network Management" Qualification is Vague and Unworkable 19

E. The Commission Should Also Refrain From Regulating the Relationship Between Wireless Broadband Providers and Application Providers 20

III. CONCLUSION 22

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Preserving the Open Internet	)	GN Docket No. 09-191
	)	
Broadband Industry Practices	)	WC Docket No. 07-52

T-Mobile USA, Inc. ("T-Mobile") submits these comments in response to the *Public Notice* issued in the above-referenced proceeding.[1]

INTRODUCTION AND SUMMARY

The Federal Communications Commission ("Commission") is correct to recognize that the potential need for any net neutrality regulation should be considered separately for wireless broadband, given the unique constraints and challenges faced by wireless networks. As T-Mobile and others have demonstrated in previous comments, the wireless broadband marketplace is highly competitive, and there is no current need for net neutrality regulation of wireless broadband services.

Transparency. T-Mobile makes every effort to disclose pertinent information about its services and practices to consumers so they can make informed purchasing decisions. In fact, all of the major wireless providers, in addition to many regional providers, have committed to CTIA's Consumer Code for Wireless Service, which requires providers to inform consumers of

[1] *Further Notice of Inquiry into Two Under-Developed Issues in the Open Internet Proceeding*, GN Docket No. 09-191, Public Notice, DA 10-1667 (rel. Sept. 1, 2010) ("*Public Notice*"). While submitting these comments in response to the questions raised in the *Public Notice*, T-Mobile recognizes that some parties have raised the issue of the Commission's authority to impose new regulations in this area. *See, e.g.*, CTIA Open Internet Reply Comments at 52-61.

all material terms and conditions of their service plans. Moreover, an updated version of the Code, which becomes effective in January, will specifically require relevant disclosures of providers' network management practices. T-Mobile and many other providers already comply with these new provisions by informing customers of limitations on permissible uses of their service, bandwidth or data caps, and measures that could affect their use of the service.

Content, application, and device developers are likewise well-informed and already have enough information to produce hundreds of thousands of services and products that consumers can use on wireless broadband networks. Wireless providers also continue to work closely with handset manufacturers to ensure that devices are optimized to provide the best user experience and make efficient use of the network. Moreover, competition among wireless broadband providers will ensure that, without compromising network security, developers continue to receive the information they need to satisfy consumers' increasing desire to use the applications and devices of their choice.

Imposition of the technically detailed, advance-notice disclosures advocated by Free Press and a few others[2] would hamstring providers from responding quickly to new and unanticipated network congestion problems, provide a road map for engineering around network security and integrity mechanisms for nefarious purposes, and force providers to reveal competitively sensitive network information. Moreover, disclosures of this type could lead to consumer confusion.

Connection of Devices and Access to Applications. Requiring wireless service providers to allow all devices to be connected to their networks, or requiring providers to allow every

[2] *See* Free Press Open Internet Comments at 113-116; Open Internet Coalition Open Internet Comments at 88-91; Public Knowledge Open Internet Comments at 65-66; Center for Democracy and Technology Open Internet Comments at 33-35.

application, would harm both consumers and the networks. In the highly competitive wireless marketplace, any provider that arbitrarily restricts the use of devices or access to applications does so at its peril. However, providers must have the network management tools necessary to ensure a high-quality consumer experience and the safety and integrity of their networks. Usage-based pricing and industry standards can be useful tools for addressing network integrity and congestion issues, but providers need the flexibility to use and experiment with a broader set of tools, including throttling, traffic shaping, and other network management methods. In addition, the Commission's proposed "reasonable network management" qualifier is too ambiguous and cannot replace wireless providers' need for flexibility.[3]

I. WIRELESS CARRIERS PRESENTLY PROVIDE MEANINGFUL AND TRANSPARENT NOTICE OF THEIR NETWORK PRACTICES AND POLICES

A. Wireless Carriers Already Provide Information on Service Practices and Policies to Consumers

T-Mobile has long been a proponent of providing consumers with the information they need to make informed decisions about their service. For example, T-Mobile was the first wireless provider to offer Personal Coverage Check ("PCC"), a tool on its website and in retail stores providing highly granular street-level signal coverage quality information for any U.S. address or location, which consumers can use to determine if T-Mobile's service is appropriate

[3] In an effort to resolve outstanding net neutrality and broadband reclassification issues raised in FCC proceedings, Representatives Waxman and Boucher have been working with industry, public interest, and other groups to negotiate draft legislation on the issues. *See* Representative Waxman Statement on Net Neutrality Proposal (Sept. 29, 2010), *available at* http://energycommerce.house.gov/index.php?option=com_content&view=article&id=2133:waxman-statement-on-net-neutrality-proposal&catid=155:statements&Itemid=55. While T-Mobile has not been a party to the discussions, we understand that the proposals to date have included some reasonable transparency requirements, along with a prohibition on the blocking of websites and competing applications. T-Mobile supports such efforts to forge a legislative solution to the issues, and would be happy to contribute to those efforts.

for them *in advance* of purchasing service.[4] With regard to broadband Internet access services, PCC includes a comparative description of network speeds that a customer might expect in a particular area.[5] T-Mobile's PCC has been praised as an "honest" approach to wireless service,[6] and its innovation was subsequently imitated by others,[7] demonstrating how a competitive industry responds to disclosures that consumers find valuable. In fact, wireless broadband providers generally want to provide consumers with relevant information about their products and services, as surprised or disappointed consumers are more likely to drop their service and provide negative word-of-mouth "advertising" to friends, family, and colleagues about that provider's service.

Similarly, T-Mobile was also among the first wireless providers to sign onto CTIA's Consumer Code for Wireless Service (the "Code"), which has been adopted by all major wireless carriers and many regional carriers.[8] The Code requires signatories to disclose all material terms and conditions of service, with the goal of providing consumers "with information to help them make informed choices when selecting wireless service, [and] to help

---

[4] *See* Personal Coverage Check, http://www.t-mobile.com/coverage/pcc.aspx (last accessed Oct. 4, 2010).

[5] The application categorizes potential network speeds as "very fast mobile web," "fast mobile web," or "mobile web," and informs consumers that their service can be affected by their equipment, specific location and obstructions, traffic volume, outages, technical limitations, signal strength, weather and other conditions.

[6] Sacha Sagan, *T-Mobile Personal Coverage Check Get "A" for Honesty*, PCMag.com (Mar. 9, 2005), *available at* http://www.pcmag.com/article2/0,2817,1774481,00.asp (last accessed Oct. 4, 2010) ("T-Mobile unabashedly unveils both their strong and weak spots, block by block, across the USA for all to see.").

[7] *See, e.g.*, Sprint Coverage Tool, http://coverage.sprint.com/IMPACT.jsp (last accessed Oct. 4, 2010); AT&T Coverage Viewer, http://www.wireless.att.com/coverageviewer/#?type=voice (last accessed Oct. 4, 2010).

[8] *See, e.g.*, Wireless Industry Unveils 10-Point Consumer Code, CTIA News Release (Sept. 9, 2003) (last accessed Oct. 11, 2010).

ensure that consumers understand their wireless service and rate plans…."[9] Recent updates to the Code, due to go into effect in January 2011, will specifically require signatory companies to disclose whether there are "network management practices that will have a material impact on the customer's wireless data experience."[10] Signatory providers will also be required to disclose any data allowances offered in a service plan and whether there are any prohibitions on data service usage.[11]

Signatories are required to submit materials and certify annually that they are in compliance with all aspects of the Code. As CTIA notes, "one of the benefits of competition is that each carrier's competitors will be watching other companies' compliance and will respond accordingly."[12] Any signatories found to be non-compliant will no longer be allowed to display the Code's Seal of Wireless Quality/Consumer Information.[13] With wide-spread industry adoption of the Code and competitive pressure in the wireless industry to provide consumers with greater transparency, there are significant measures already in force in the market to meet consumer needs.[14]

---

[9] CTIA, Consumer Code for Wireless Service, *available at* http://files.ctia.org/pdf/The_Code.pdf (last accessed Oct. 10, 2010) (currently effective version of the Code).

[10] *See* CTIA, Consumer Code For Wireless Service, *available at* http://files.ctia.org/pdf/ConsumerCode.pdf (last accessed Oct. 4, 2010) (effective January 1, 2011).

[11] *Id.*

[12] *See* CTIA, "Consumer Code: Questions & Answers," *available at* http://www.ctia.org/content/index.cfm/AID/10549 (last accessed Oct. 4, 2010).

[13] *Id.*

[14] Indeed, consumer complaints have dropped since the introduction of the Code. *See* Comments of CTIA, CG Docket No. 09-158 (filed Oct. 13, 2009) at 18-19 (noting that complaints dropped from an annualized rate of 80 per one million subscribers in 2004, to just 40 per one million subscribers in 2008). Moreover, other government bodies have recognized the advantages of self-regulatory programs relating to consumer disclosures. *See, e.g.,* European Commission, Health & Consumer Protection Directorate General, "Labeling: competitiveness, consumer information and better regulation for the EU" (Feb. 2006), *available at* http://ec.europa.eu/food/food/labellingnutrition/betterregulation/competitiveness_consumer_info.pdf (last accessed Oct. 4, 2010) ("*EU Food Labeling Report*") (finding a "need to

We would caution the Commission to ensure that if it does introduce regulation here, it should limit any new rule to a flexible disclosure obligation like that contained in the revised Code. As the *NPRM* in this proceeding suggested, the goal of any transparency requirement should be to ensure that consumers have access to information that they "would consider relevant in choosing a service provider or a particular service option."[15] T-Mobile and many other providers have already achieved this goal by ensuring that consumers are informed of limitations on permissible uses of their service, bandwidth or data caps, and measures such as throttling that could affect their use of the service.[16] Providing more than this – such as the exact technical mechanisms the provider will use in managing network use – would confuse the average consumer and add little value to their understanding of their service. Most consumers want a practical and simple understanding of their service offering, which is what T-Mobile and other operators are motivated to provide.

B. Technically Detailed Disclosure Requirements for Wireless Network Management Practices Would Do More Harm than Good

The Commission should reject the sweeping, technically detailed disclosure mandates called for by Free Press and a few other net neutrality advocates.[17] Not satisfied with the *NPRM*'s proposal to require disclosure of information that is "reasonably required for users … to

---

consider alternatives to legislation, *e.g.*, self-regulation or codes of best practice" regarding food-related labeling).

[15] *Preserving the Open Internet, Broadband Industry Practices*, Notice of Proposed Rulemaking, 24 FCC Rcd 13064 ¶¶ 121, 123 (2009) ("*Open Internet NPRM*").

[16] *See, e.g.*, T-Mobile Terms & Conditions at sections 10 and 17, *available at* http://www.t-mobile.com/Templates/Popup.aspx?WT.z_unav=ftr__TC&PAsset=Ftr_Ftr_TermsAndConditions&print=true (effective July 18, 2010).

[17] *See, e.g.*, Open Internet Coalition ("OIC") Open Internet Comments at 88-89; Public Knowledge Open Internet Comments at 65; Center for Democracy and Technology Open Internet Comments at 33-35.

enjoy the protections" specified in the proposed rules, Free Press suggests that providers be forced to overwhelm consumers with hyper-technical information relating to:

- the "technology used for network control"
- "evidence to demonstrate the existence of congestion or other problems"
- "any and all" changes made to upstream or downstream traffic
- "technical details of the methods used"
- "exact details of all thresholds, such as time of day or exact levels of congestion or bandwidth consumption, that trigger network interference"
- the percentage of users that will be impacted based on chosen thresholds and the duration of such impact
- "exact details of thresholds that trigger a cessation" of network management[18]

In addition, Free Press proposes that providers give "sufficient advance notice [of network management changes] to enable users to seek alternate Internet access services providers, should they choose not to accept the changes."[19] Such an onerous approach is simply unworkable, not friendly to the average consumer, and would undoubtedly prevent real-time fixes and fail to adequately protect consumers and networks. Mobile networks are extremely dynamic, and network congestion or problems can develop very quickly and at unpredictable times and locations.[20] Providers must be able to respond immediately to unpredictable situations, such as that experienced by T-Mobile when a new Android-based instant messaging application caused an overload of T-Mobile's facilities for an entire city.[21] Under Free Press's

---

[18] Free Press Open Internet Comments at 113-116 and n. 232.

[19] *Id.* at 117. Similarly, Public Knowledge and OIC suggested 30 days prior notice for any change to network management practices. *See* Public Knowledge Open Internet Comments at 65-66; OIC Open Internet Comments at 90-91.

[20] *See* Comments of T-Mobile USA, Inc., GN Docket No. 10-127 (filed July 15, 2010) ("T-Mobile Framework Comments") at 5-7; *Open Internet NPRM* at ¶ 172 ("users in a cell share the spectrum at any given time and the demands on capacity can vary widely depending on such factors as the number of users within that cell at any given time and the applications they are using"); *id*. at ¶ 159 ("wireless networks must deal with particularly dynamic changes in the communications path due to radio interference and propagation effects such as signal loss with increasing distance of the wireless phone to the base station, fading, multipath, and shadowing").

[21] *See* T-Mobile Open Internet Comments at 21-22.

proposal, however, mobile broadband providers would be helpless to confront new problems that had not already been anticipated in their network management policies, and consumers would suffer as a result of the likely network degradation.

Setting aside the fact that compliance with the list of Free Press requirements is not technically feasible[22] and would be cost prohibitive,[23] flooding consumers with volumes of information can actually be counterproductive to consumer protection goals, as the Commission acknowledged in the *NPRM*.[24] Too much information can lead to confusion and make it harder for the consumer to discern what is actually relevant.[25] As one government official explained:

> [T]he disclosure-focused model for consumer protection only works if disclosures are understandable and convey the information consumers want and most need to know. … Disclosures often are … overly complex and detailed; and fail to effectively focus the consumer on information key to the consumer's decisions.[26]

---

[22] For example, on a mobile network, it is impossible to predict how many subscribers would be impacted by any given change, because the number of users accessing a particular site changes constantly, as do the types of applications they are using on the network.

[23] Given the dynamic nature of mobile networks and the need for frequent changes in network management techniques, significant resources would have to be devoted to constantly revising the network management practice disclosures and compiling the kind of detailed data that network neutrality advocates suggest is needed.

[24] *Open Internet NPRM* at ¶ 126 ("too much detail may be counterproductive if users ignore or find it difficult to understand those details").

[25] *See, e.g.* T. Miller and W. Sage, "Disclosing Physician Financial Incentives," 281 *Journal of the American Medical Association* 1424, 1425 (Apr. 21, 1999) (article on disclosing physician financial incentives concluding that "disclosed information must not be so detailed that it confuses readers or obscures essential points"); s*ee also* M. Hincha-Ownby, *Consumers confused by proposed EPA car labels*, Mother Nature Network (Sept. 28, 2010) *available at* http://www.mnn.com/transportation/cars/stories/consumers-confused-by-proposed-epa-car-labels (describing a consumer survey of the EPA's proposed new vehicle fuel efficiency labels, which concluded that the labels "may send buyers into information overload") (last accessed Oct. 4, 2010).

[26] Remarks by Julie L. Williams, Chief Counsel, Office of the Comptroller of the Currency, before the Joint Center for Housing Studies, Harvard University (Nov. 28, 2007), *available at* http://www.occ.treas.gov/ftp/release/2007-128a.pdf, at 2-3 (last accessed Oct. 4, 2010).

The Commission should therefore avoid adopting any rule that would bury consumers with information that is not comprehensible or relevant to the vast majority of users, and should instead allow providers the flexibility to present the type of information that will enable consumers to make informed choices about their service.[27]

Moreover, any detailed, hyper-technical disclosures of network management techniques would endanger network and consumer security by providing a "road map" for hackers, criminals, and other persons seeking to engineer around network security and integrity mechanisms to introduce harmful content, or to otherwise unfairly exploit the network, such as by "hogging" bandwidth to the detriment of other users.[28] Detailed disclosures about how a provider combats network congestion or other problems would facilitate "denial of service" attacks, a common form of network attack in which the perpetrator seeks to overwhelm the network's resources.[29] Meticulous disclosures of the type advocated by Free Press and others would also force providers to reveal competitively sensitive network information, a significant concern in the competitive wireless market. As AT&T notes, "a provider's ability to offer customers a highly secure and well-functioning network is a marketplace advantage, and providers should not be forced to disclose the often proprietary techniques they use to accomplish this."[30]

---

[27] *See EU Food Labeling Report* at ¶¶ 6, 10 (finding that food labels often "contain too much information, much of which is not understood," and concluded that any new regulations should "be based on whether a given piece of information is necessary to enable consumers to make their choice").

[28] *See also* AT&T Open Internet Comments at 193-94 ("There is no surer way to compromise the integrity of a network than by broadcasting the technical details of how that network will be managed.").

[29] Verizon and Verizon Wireless Open Internet Reply Comments at 20-21.

[30] AT&T Open Internet Comments at 195.

C. Mandating Specific Public Disclosure of a Provider's Device and Application Requirements and Certification Processes Is Unnecessary

Wireless network providers already have strong, market-based incentives (and demanding consumers) to ensure that application and device developers have all the information they need to create applications and devices that consumers can use on their networks, so rules requiring disclosure to such developers are not needed.[31] Moreover, new content, applications, and services are already developed and deployed every day based on the information currently available.[32] Given the exponential growth in applications (and even in devices) developers and manufacturers plainly are getting all the information they need to develop successful applications, devices, and other products.[33] Indeed, as AT&T noted, network operators, not developers, are more often at an information disadvantage: "They must contend with any applications that their end users access over the network, and they must scramble to understand new applications that may be damaging the network, that consume large and unanticipated amounts of bandwidth, or that otherwise pose network-management or consumer privacy challenges."[34]

Two of the reasons for not publicly disclosing highly technical details of a network operator's practices are the same with regard to developers as they are for consumers: such

---

[31] The *Public Notice* seeks comment on what disclosure requirements would be appropriate to ensure that "content, application, service and device providers can make informed choices regarding use of mobile broadband networks." *Public Notice* at 5.

[32] Increasingly, application developers can take advantage of open Application Programming Interfaces ("API") published by industry coalitions. *See* Alcatel Lucent Open Internet Reply Comments at 21-23 (describing current industry open API initiatives, including "OneAPI" supported by the GSM Alliance, and the Wholesale Applications Community, composed of 24 operators along with LG Electronics, Samsung, and Sony Electronics).

[33] For example, there are already many tens of thousands of applications for the Android platform and even more for the iPhone.

[34] AT&T Open Internet Comments at 193.

disclosures would endanger network and consumer security and reveal competitively sensitive network details. And, with regard to devices, wireless providers already work closely with handset manufacturers and share sufficient information to ensure that devices are efficiently optimized for network use.

Because consumers have an insatiable desire to use the newest and most cutting-edge applications and devices of their choice, competitive market forces will continue to ensure that wireless network operators provide the information necessary for application and device developers to produce services and products that consumers can use on wireless networks. Because the marketplace is working, there is no need for new rules regarding the disclosure of wireless broadband provider application and device requirements and certification procedures.

II. THE COMMISSION SHOULD NOT REQUIRE WIRELESS BROADBAND PROVIDERS TO ALLOW ANY AND ALL DEVICES AND EVERY APPLICATION ON THEIR NETWORKS

Mandates requiring wireless providers to allow all devices[35] or every application on their networks, as contemplated by the *Public Notice*, would harm both consumers and networks.[36] Wireless providers compete vigorously for consumers by offering a broad selection of cutting-edge mobile devices and access to thousands of applications.[37] But, some devices and applications can pose network security, reliability, congestion, and efficiency problems that, if left unaddressed, can degrade the consumer experience or ultimately harm the network. While

[35] While the *Public Notice* suggests that any new rule would only require providers to allow all "non-harmful" devices to attach to their networks, *see Public Notice* at 5, in reality it is often impossible to know with certainty, prior to allowing an attachment, that a device will not cause harm to the network.

[36] The Commission seeks comment on how mobile broadband provider conduct would have to change if the Commission were to require mobile providers to allow any non-harmful device to connect to their networks, subject to reasonable network management. *Public Notice at 5.*

[37] *See, e.g.*, T-Mobile Open Internet Reply Comments at 6, 12; *see also* CTIA Open Internet Comments at 14.

industry standards and usage-based data pricing can be helpful tools for addressing these issues, wireless providers should not be limited to these network management techniques alone. Some wireless providers might opt for these techniques, but others might find them insufficient or incompatible with their operations and favor other techniques such as throttling or traffic shaping. A "one-size-fits-all" approach, moreover, could advantage some wireless providers over others, thereby harming competition. And, even a "reasonable network management" qualifier is insufficient to provide wireless operators the certainty they need to address the issues that arise.

A. In the Competitive Mobile Wireless Sector, Network Providers Have a Strong Incentive to Enable Consumers to Use as Many Devices and Applications as Possible

Consumers hold appreciable leverage over wireless service providers,[38] and those providers that have not kept pace with evolving customer demands have been quickly driven from the market. Thus, no provider can afford to risk alienating current or potential future customers by needlessly or arbitrarily denying access to mobile devices or applications.

Devices. One critical way in which providers vie for customers is by offering the latest mobile devices to suit various tastes and market segments.[39] A wide range of devices operate on T-Mobile's network, including some of the most advanced smartphones and other devices currently available in the market.[40] To ensure that its network remains open to an expansive

[38] *See* Reply Comments of T-Mobile USA, Inc., GN Docket No. 10-127 (filed Aug. 12, 2010) at 13-14.

[39] *See* CTIA Open Internet Comments at 14. To illustrate, CTIA has reported that there are 33 different companies manufacturing more than 630 unique wireless devices for the U.S. market, more than in any other country in the world.

[40] For example, T-Mobile offers the myTouch 3G, the G2 with Google, the HTC HD2, the BlackBerry Bold and Curve, and the Garmin-Asus Garminfone with integrated GPS navigation. T-Mobile, Choose a Phone, http://www.t-mobile.com/shop/phones/?shape=smp&WT.z_unav=mst_shop_phones_smart (last accessed Oct. 12, 2010).

selection of handsets and devices and continues to meet consumer demand, T-Mobile also allows consumers to "bring their own device" so long as it is compatible with T-Mobile's network. T-Mobile also does not lock unsubsidized devices and allows subscribers to unlock subsidized handsets after only 40-60 days, depending on the customer's service plan.[41] These are just a few of the pro-consumer policies adopted by T-Mobile that allow customers a broad range of choices with respect to their devices.[42]

Applications. In addition, new apps from wireless network providers and non-network providers alike abound because of the market-driven needs of network operators and app developers to continuously update their broadband product lines and service offerings to satisfy growing demand.[43] Consumers have shown an immense appetite for these apps, which span a variety of genres such as education, health and fitness, entertainment, productivity, social networking, sports, business, and safety.[44] In the face of this enthusiasm, it is extremely unlikely that any individual wireless broadband provider could succeed by limiting access in any arbitrary

---

[41] *See* T-Mobile Support: SIM Unlock Code, http://support.t-mobile.com/doc/tm51885.xml (last accessed Oct. 4, 2010).

[42] Other major wireless providers have adopted similar policies.

[43] The mobile applications, or "apps" market continues to skyrocket, with hundreds of thousands of apps now offered to consumers – more than double the number available at the end of 2009. *See* CTIA Open Internet Comments at 22 (reporting 150,000 apps at the end of 2009). For example, there are more than 250,000 iPhone apps currently available, along with more than 80,000 Android apps. *See* Apple, Learn about apps available on the App Store, http://www.apple.com/iphone/apps-for-iphone/ (last visited Oct. 4, 2010). *See Android Market Has More than 80,000 Apps, Android's Rubin Says*, Android Central (Sept. 9, 2010) *at* http://www.androidcentral.com/googles-andy-rubin-says-over-80k-apps-now-android-market (last accessed Oct. 4, 2010). Network operators are even innovating at the edge by upgrading their networks, such as T-Mobile has done with its HSPA+ deployment. *See* "T-Mobile HSPA+ Network now delivers broadest reach" (July 21, 2010), *available at* http://press.t-mobile.com/articles/t-mobile-HSPA-4G.

[44] As one example of the demand, wireless consumers downloaded more than 1.1 billion apps in 2009. *See* Comments of CTIA – The Wireless Association, GN Docket No. 10-127, 13 (filed July 15, 2010) ("CTIA Framework Comments") (internal citations omitted).

or anticompetitive manner and standing as a "gatekeeper" between a consumer and content or app providers.

As part of its efforts to satisfy consumer demand for apps, T-Mobile allows its customers to select and use devices based on the open Android platform or other operating systems,[45] each with their own apps and app stores, and use any smartphone to access web-based apps and content. T-Mobile also does not block or prohibit apps or technologies such as VoIP that arguably compete against T-Mobile core services. In fact, none of the major wireless broadband providers block VoIP over their networks, indicating that the networks of wireless providers like T-Mobile are apparently more open (and potentially subject to more competition) than some of the application providers or Internet service companies themselves.[46]

B. Wireless Broadband Providers Must Have the Flexibility to Address Network Security and Reliability Risks and Other Threats to the Consumer Experience

Despite carriers' efforts to provide consumers with the most device and application choices possible, mandating that wireless operators permit all devices or every application on their networks would limit operators' flexibility to address emerging risks, service degradations, or other unforeseen events – all of which could result in network security and reliability degradation.

---

[45] For example, T-Mobile offers the Android-based G2 with Google and myTouch 3G, Motorola CLIQ XT, Samsung Vibrant and Behold II, the Garmin-Asus Garminfone, and others. T-Mobile, Choose a Phone, http://www.t-mobile.com/shop/phones/Default.aspx?features=48CC3997-D234-4683-8B5A-F026B9DB5528&WT.z_unav=mst_shop_phones_android (last accessed Oct. 12, 2010). T-Mobile will also soon be offering the HTC HD7, which uses the Windows Phone operating system. T-Mobile, http://htc.t-mobile.com/hd7/?WT.z_unav=mst_disc_innovate_hd7 (last accessed Oct. 12, 2010).

[46] *See Skype-Fring Connection Unravels Over TOS Dispute*, PCMag.com (July 12, 2010), *available at* http://www.pcmag.com/article2/0,2817,2366354,00.asp (last accessed Oct. 4, 2010) (messaging aggregator Fring alleged that Skype was using threat of legal action to force Fring to halt its compatibility with Skype).

Security Risks. Wireless broadband providers must be able to address the security risks and other vulnerabilities, many of which are unforeseen, presented by devices and apps. Hackers and third parties can use devices and apps as conduits to introduce viruses or other malware, potentially causing harm not only to the networks and network operators, but also to other network users.[47] As mobile broadband usage expands and consumers transmit an increasing amount of personal information over wireless networks, the potential for such security threats will likely increase (including when consumers bring their own devices under wireless providers' openness policies). Even in the increasingly open wireless ecosystem, therefore, wireless broadband providers, as well as device manufacturers themselves,[48] need flexibility to protect consumers and networks against these threats. Consequently, to ensure customer privacy and network security, providers may need to conduct certain testing or certification activities (both before and after devices are connected to their networks and apps are initially authorized for use), to ensure that devices and apps operating on the network utilize evolving encryption technology, and to provide after-the-fact remediation on an expedited basis as needed.[49]

Efficiency and Reliability. Devices and apps operating on wireless networks can drain the limited resources available and impact both network integrity and the consumer experience, depending on how efficiently or inefficiently they operate and the usage patterns they create. Acknowledging these concerns, the Commission in 2007 affirmed the legitimate need of network

---

[47] *See, e.g.*, *See Service Rules for the 698-46, 747-762 and 777-792 MHz Bands*, Second Report and Order, 22 FCC Rcd 15289 ¶ 223 (2007) ("*700 MHz Second Report and Order*") (stating when adopting the Upper 700 MHz C Block open platform requirements that "we are mindful of the risks network operators face in protecting against harmful devices and malicious software").

[48] Device manufacturers, for example, play a principal role in developing handset operating systems with robust security mechanisms. *See* T-Mobile Statement, "Code Level Modifications to the G2" (Oct. 7, 2010), *available at* http://press.t-mobile.com/articles/t-mobile-G2-code-level-modifications.

[49] *See, e.g.*, Comments of AT&T Inc. at 149, 172 (discussing some of AT&T's application testing and remediation procedures).

providers to address issues regarding the attachment of devices and use of apps on their networks when it imposed the open platform requirements on the Upper 700 MHz C Block, stating:

> [W]ireless providers have legitimate technical reasons to restrict particular non-carrier devices and applications on their networks, specifically to ensure the safety and integrity of their networks. In particular, we believe that it is reasonable for wireless service providers to maintain network control features that permit dynamic management of network operations, including the management of devices operating on the network, and to restrict use of the network to devices compatible with these network control features. Standards to ensure that network performance will not be significantly degraded would also be appropriate.[50]

The substantial increase in data traffic caused by new devices and apps is of particular concern for spectrum-strapped wireless providers. For example, subscribers using certain smartphones consume 100 times more data than typical T-Mobile customers.[51] Data traffic has already begun to exceed voice traffic, and by 2014, three-quarters of all global broadband subscribers are expected to be using mobile devices.[52] In addition, data traffic has jumped 50% from the end of 2009 to the end of the first half of 2010.[53] Recognizing these trends, the Commission's National Broadband Plan ("NBP") recommended the release of an additional 500 MHz of spectrum for wireless broadband over the next ten years.[54]

Forcing providers to permit all devices and every app with network access would severely hinder providers' ability to ensure efficient and safe use of their networks and would be

---

[50] *See 700 MHz Second Report and Order* at ¶ 223.

[51] T-Mobile Open Internet Reply Comments at n.56; T-Mobile Open Internet Comments at 18.

[52] *See, e.g.*, "Industry Urges Different Neutrality Treatment for Wireless Services," TR Daily (Sept. 15, 2010), statement by Paul Jacobs, Qualcomm, Inc. Chairman and CEO.

[53] *CTIA: Wireless data use increased by 50 percent*, The Hill (Oct. 6, 2010), *available at* http://thehill.com/blogs/hillicon-valley/technology/122991-ctia-wireless-data-use-increased-by-50-percent (last accessed Oct. 7, 2010).

[54] *See* Federal Communications Commission, *Connecting America: The National Broadband Plan*, Recommendation 5.8, 84-93 (rel. Mar. 16, 2010), *available at* www.broadband.gov.

contrary to the NBP. For example, wireless broadband providers need to be able to prevent and respond to unnecessary bandwidth drains and network congestion that could disrupt service (including emergency, public safety, law enforcement, and other high priority communications) to other network users.

C. Usage-Based Data Pricing and Industry Standards Cannot Fully Protect Consumers, Wireless Providers, and Networks From the Harms That Would Result from Mandates to Permit All Devices and Applications on a Network

Usage-Based Data Pricing. Although usage-based data pricing can help mitigate some concerns about wireless network congestion caused by apps and third-party devices, wireless providers need the ability to use other network management techniques in addressing wireless network congestion or other legitimate network-related concerns, including the security, reliability, and efficiency issues discussed above.[55]

Usage-based pricing may moderate average usage patterns, but even under a tiered-pricing framework, a small number of users operating inefficient (or, worse, malicious) devices or "bandwidth-hog" apps in the same cell could block other users in the area from accessing the network and cause harm to the network, consumers, or other devices. Because users often travel across multiple cells, a large number of other users could be affected by just a few inefficient or malicious devices or apps. In addition, operators offering usage-based pricing will still need to manage certain high priority traffic from lower-tier users (*e.g.*, emergency calls) and congestion spikes.[56]

Industry Standards. Similarly, adherence to industry standards or independent tests cannot ensure non-harmful technical interoperability between mobile broadband devices, apps,

---

[55] *See Public Notice* at 5.

[56] *See, e.g.*, AT&T Open Internet Reply Comments at 94-95.

and networks.[57] Industry standards bodies and working groups can discuss technical network management issues and may help facilitate non-harmful technical interoperability,[58] but they are only one tool in a broader set of tools that must be available to address the wide range of wireless network challenges. For example, industry standards bodies and working groups cannot account for the unique characteristics of each network, and cannot respond quickly enough to some of the unique day-to-day threats that providers must handle. And, although independent, authorized test laboratories could validate compliance of devices with a "one-size-fits-all" wireless network technical standard,[59] such uniform standards are not feasible given the myriad unique technical network characteristics and challenges faced by different wireless providers.[60] Thus, a mandate to support any and all devices or apps that meet certain industry standards should not be the basis for a general right of access for third-party devices or apps.

Network operator validation or certification of devices and apps seeking access to a mobile wireless network can, depending on network and other constraints, be a more effective

---

[57] *See Public Notice* at 5.

[58] T-Mobile actively participates in industry standards bodies and is an original member of the industry-driven Broadband Internet Technical Advisory Group ("BITAG"), overseen by Dale Hatfield, Adjunct Professor of the University of Colorado at Boulder. *See Initial Plans for Broadband Internet Technical Advisory Group Announced*, PR Newswire (June 9, 2010) *at* http://www.prnewswire.com/news-releases/initial-plans-for-broadband-internet-technical-advisory-group-announced-95950709.html (last accessed Oct. 9, 2010). Mr. Hatfield recently announced that BITAG is open to "any person or entity interested in furthering its mission and able to bring the requisite technical expertise." *Broad Consensus Achieved on BITAG's Structure*, BITAG Blog (Oct. 4, 2010), *at* http://blogs.bitag.org/ (last accessed Oct. 9, 2010).

[59] *See* NAF Open Internet Comments at 29-31, 34.

[60] Even assuming that a common standard could be developed, it could not ensure optimized performance on all networks because the differences are too great, nor could it incorporate all of the service features constantly introduced by different providers. *See, e.g.*, Verizon Wireless Open Internet Reply Comments at 56. As Verizon Wireless notes, "[e]ach carrier knows its own network better than any third party and is best situated to determine the technical standards to which a device must conform to minimize interference, maximize network performance, and otherwise provide the best possible customer experience." *Id.* at 55.

way to ensure that the use of such devices and apps will not harm the network or network users.[61] Through these processes, network operators may work directly with equipment manufacturers and app developers to address interoperability and technical issues, ideally before the devices and apps are made available to consumers. They can also optimize device efficiency and attempt to address security concerns pre-deployment (and on an on-going basis).[62]

D. The Proposed "Reasonable Network Management" Qualification is Vague and Unworkable

The proposed "reasonable network management" standard is too ambiguous to give wireless network operators the certainty they need to address threats to the consumer experience and their networks. Under an "any device" or "every app" rule subject to reasonable network management, every network management decision will be injected with legal risk and uncertainty, distorting the process of making those decisions to the detriment of wireless service providers, device manufacturers, and consumers.[63] Every time a provider encounters a new network challenge involving a device or app, it will have to weigh the need for prompt action against the regulatory prospect of legal sanctions.

---

[61] *See, e.g.*, "Verizon Wireless to Introduce 'Any Apps, Any Device' Option for Customers in 2008: New Open Development Initiative Will Accelerate Innovation and Growth," Verizon Wireless Press Release (Nov. 27, 2007) *available at* http://news.vzw.com/news/2007/11/pr2007-11-27.html (last accessed Oct. 4, 2010) (noting Verizon Wireless's intent to "publish technical standards the development community will need to design products to interface with the Verizon Wireless network" and that "[a]ny device that meets the minimum technical standard will be activated on the network"). While the setting of minimum technical standards might be appropriate for some providers with respect to their own networks, it might not be appropriate (for technical and other reasons) for other providers. Thus, each provider must be afforded the flexibility to develop an approach that works best for its network.

[62] *See, e.g.*, *700 MHz Second Report and Order* at ¶ 223 (recognizing the need for wireless service providers to protect against harmful devices, malicious software, and other risks to the safety and integrity of their networks, and authorizing the Upper 700 MHz C Block licensees to use certification standards and processes to approve the use of devices and applications on their open platform networks).

[63] T-Mobile Open Internet Comments at 31.

To manage the day-to-day challenges of a wireless network, including spectrum constraints, expanding and highly unpredictable demand, interference sensitivity, security threats, and the effects of technological evolution, wireless broadband providers must have a full toolkit of network management techniques that enable them to respond quickly and dynamically. Many harms caused by devices and apps are not deliberate or foreseeable,[64] and as network congestion and security threats increase, so too will the pressure on providers to act quickly to manage their networks. Instead of mandating access for all devices and every app and then layering on a vague exception to that standard that will have a chilling impact and unintended consequences, the Commission should allow the wireless broadband marketplace to continue to thrive by preserving the autonomy carriers need.

E. The Commission Should Also Refrain From Regulating the Relationship Between Wireless Broadband Providers and Application Providers

In the *Public Notice*, the Commission seeks comment on the extent to which certain application distribution models may affect consumer choice, as well as whether mobile providers should have more discretion to restrict consumers' downloading or use of native applications than web-based applications.[65]

Consumer choice, innovation, freedom of expression, continued private investment and competition in the mobile wireless broadband market would best be achieved by refraining from regulating the relationship between mobile wireless broadband providers and application providers at this time. Just as a wireless provider cannot act as an unreasonable gatekeeper over apps or device selection, it also cannot remain competitive as an app store owner by utilizing

[64] *See, e.g.*, Leap Wireless Open Internet Reply Comments at 16 (noting that "even with appropriate planning and testing, a carrier may not be able to anticipate the precise network management tools it will need to employ to prevent service interruptions and harm to the network").

[65] *Public Notice* at 5-6.

restrictive policies; wireless consumers have consistently been willing to vote with their feet and switch providers. The competitive wireless marketplace will continue to discipline app store owners (whether or not they are also wireless service providers) that exclude third-party apps from their app stores entirely, eliminating the need for Commission action.[66] For example, likely due to market pressures, Apple recently relaxed restrictions on app developers and published App Store approval guidelines in an attempt to increase transparency and consumer access.[67]

In addition, nothing in the record supports restricting wireless broadband providers' ability to restrict downloading and/or use of web-based applications to a lesser degree than native applications. Both types of applications potentially raise network security, service quality and reliability, and consumer experience concerns, and in neither case is the subscriber prohibited from reacting to policies with which he or she disagrees by changing wireless broadband providers.

---

[66] T-Mobile notes that there is a clear difference between a wireless service provider acting as an app store owner that excludes third-party apps from its app store entirely (which could be problematic, depending on the circumstances) and one that allows third-party apps but showcases certain apps over others in the app store (which is entirely reasonable).

[67] *Apple Relaxes Restrictions on Apps, Opening Door to Flash: iPhone Maker Says Developer Feedback Fueled Change; Adobe Shares Jump*, MarketWatch (Sept. 9, 2010) *at* http://www.marketwatch.com/story/apple-relaxes-app-restrictions-adobe-shares-jump-2010-09-09 (last accessed Oct. 2, 2010) (stating that "[a]nalysts say Apple's move was likely prompted by increased competition from competing mobile platforms – most notably the Android operating system from Google Inc.").

III. CONCLUSION

For the reasons discussed above, any network management disclosure requirement should be carefully limited to prevent network security and competition harms, and the Commission should refrain from imposing any restrictions that limit the flexibility of wireless broadband providers with respect to the devices and applications running on their networks.

Respectfully submitted,

Tom Sugrue

Thomas J. Sugrue
Kathleen O'Brien Ham
Amy R. Wolverton

T-MOBILE USA, INC.
401 Ninth Street, NW Suite 550
Washington, DC 20005
(202) 654-5900

Ari Q. Fitzgerald
Michele C. Farquhar
David L. Martin
Mark W. Brennan

HOGAN LOVELLS US LLP
555 Thirteenth Street, NW
Washington, DC 20004
(202) 637-5600

Attorneys for T-Mobile USA, Inc.

October 12, 2010