Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

DECLARATION OF GRANT CASTLE

1. My name is Grant Castle. My business address is 12920 SE 38th Street, Bellevue, Washington 98006. I am the Director, National Planning & Performance Engineering at T-Mobile USA, Inc., a position that I have held since October 2008. My team is responsible for the all aspects of network capacity planning as well as all aspects of network performance and optimization. I have been in the engineering department at T-Mobile and its predecessor-companies since June 1994 and have a degree in Engineering from the University of Washington.

2. The purpose of my declaration is to discuss the potential impact of the rules proposed by the Federal Communications Commission ("FCC") in its October 22, 2009, Notice

of Proposed Rulemaking (FCC 09-93) ("NPRM") on the unique technology and network management needs of wireless broadband services.

3. Wireless network technology makes application of the proposed net neutrality rules both risky and unnecessary in the wireless broadband context. Wireless network operators must contend with increasingly scarce spectrum, rapidly expanding yet highly unpredictable demand, interference hurdles, challenging topologies, handset and device coordination requirements, and ongoing and fast-paced technological evolution. To respond to these challenges in a timely and effective manner, wireless network managers must be free to rely on their expert judgment and employ the full range of network management techniques available. The proposed rules contained in the Commission's Notice of Proposed Rulemaking (the "NPRM") raise a host of questions that could complicate T-Mobile's network management. By depriving wireless network managers of the freedom and flexibility they depend upon to develop and employ network management tools, the proposed rules could undermine T-Mobile's ability to deliver high-quality voice services and next-generation applications in a bandwidth-constrained environment.

4. Without regulation, T-Mobile is already responding to consumer demands for open, flexible platforms. Because of the variety of devices and the increases in open Internet access via wireless networks, however, wireless broadband providers are now facing even greater technological challenges and require new tools to manage complex and unpredictable network demands. Neither the NPRM's "reasonable network management" exception—even interpreted liberally—nor the "managed" or "specialized" services exemptions can alone address the technical challenges faced by T-Mobile and other wireless providers.

The Wireless Industry Grapples with Unique Technology Challenges

5. **Limited Spectrum.** The amount of spectrum available to a wireless provider sets a concrete, upper limit on the last-mile capacity of the network. Wireless carriers, including T-Mobile, must do the best they can with the spectrum they have to deliver broadband access services that consumers want. T-Mobile has worked intensively to increase spectral efficiency, and will continue to do so. This has included building thousands of sites to provide infill capacity; rolling out HSPA technology across our network; continued innovation on antenna systems; the introduction of low-rate codecs to make voice more efficient; and the deployment of numerous other tools designed to maximize our spectrum usage. But efficiency improvements alone cannot keep pace with the increasing pace of wireless broadband adoption and use. The bottom line is that wireless network providers need more spectrum to keep up with demand.

6. **Insatiable Demand Driven by Device and Service Innovation.** T-Mobile has first-hand experience with ballooning demand for wireless broadband access, and in our experience, demand increases whenever new devices and new capabilities emerge. Customers with devices that lack full web browsing capabilities consume minimal amounts of data and require lower throughput. But that has changed as T-Mobile has introduced new devices with capabilities to make use of T-Mobile's 3G network for all sorts of web-based applications. Eighty percent of T-Mobile's myTouch users now browse the web at least once per day, and two-thirds do so several times per day. Thirty percent of T-Mobile's data traffic today consists of bandwidth-intensive video streaming—most of which is done by Android users. In other words, network capabilities, new devices, and new applications exacerbate rather than relieve spectrum constraints, and make network management even more critical.

7. **Shared Bandwidth.** More than with other forms of broadband access, wireless users can have profound impacts on the experience of other users. For example, T-Mobile network service was temporarily degraded recently when an independent application developer released an Android-based instant messaging application that was designed to refresh its network connection with substantial frequency. The frequent refresh feature did not create problems during the testing the developer did via the WiFi to wireline broadband environment, but in the wireless environment, it caused severe overload in certain densely populated network nodes, because it massively increased signaling—especially once it became more popular and more T-Mobile users began downloading it to their smartphones. One study showed that network utilization of one device increased by 1,200% from this one application alone. These signaling problems not only caused network overload problems that affected all T-Mobile broadband users in the area; it also ended up forcing T-Mobile's UMTS radio vendors to reevaluate the architecture of their Radio Network Controllers to address this never-before-seen signaling issue. Ultimately, this was solved in the short term by reaching out to the developer directly to work out a means of better coding the application.

8. **Threats to Sensitive Applications in Shared Environment.** Another unique problem in the wireless environment is that wireless broadband capacity is shared between voice and other applications, including bandwidth heavy applications like gaming, streaming video, or always-on social networking. No amount of planning can guarantee that every user's application needs will be met: wireless users are mobile and providers cannot anticipate how many users will be sharing the wireless network in a particular location at any particular time. Without careful network management, however, the risk is significantly increased that one customer's online video game frenzy could interfere with and even block another customer's critical life-saving telephone call.

9. **Interference**. Interference from other users and devices can also dramatically reduce available capacity in a given area at any given moment in time. Interference can be caused by unlicensed devices, by malfunctioning or noncompliant devices in or out-of-band, by buildings and topography, or by weather or atmospheric conditions.

10. **Constant Network Change**. Wireless network managers are faced with constant evolution of network technology. T-Mobile's deployment of HSPA 7.2, HSPA+, and eventually, 4G service will create new usage patterns, new possibilities for congestion, and new potential vulnerabilities and security risks. Even with the best of planning, we are likely to confront a number of unanticipated challenges.

11. **Balancing the Complex Interaction Between the Network and Different Devices and Applications.** In contrast to the wireline network, wireless networks are affected by the types of devices on the network and how they operate, because as devices communicate

with the network, they consume network resources in ways that can be more or less efficient and that can affect other users more or less radically. In order to ensure that there are sufficient network resources for all users, carriers try to work closely with their handset partners to ensure that devices are optimized to provide service over the network using the least possible network bandwidth. For example, a carrier and device manufacturer might work to limit unnecessary communication from the handset to the network nodes when the handset is not in active use. This is one reason that carriers face challenges in supporting unlocked third party devices, which are not optimized for the network. Older-generation devices also may place inefficient loads on the network, but must still be supported on the network. All of this makes for complex network management challenges.

12. Similar challenges are created by applications that are not optimized for a particular wireless network, as illustrated by the example I provided above, when a third party application caused massive network congestion. When T-Mobile works directly with a wireless application developer, it will seek to optimize the use of the radio network by following certain guidelines, like minimizing the number of connections that are opened and closed by the application, because establishing and terminating a connection consumes a substantial amount of network resources. Thus, even an application that is not inherently bandwidth "hungry" can cause substantial network loading and congestion on a wireless network simply because it is not well-engineered to avoid establishing multiple connections. This is a risk carriers face because the network is open to applications from third party, non-partner developers.

The NPRM Would Create Significant Uncertainty for Network Managers

13. The proposed rules could interfere with measures carriers use today to manage the challenges posed by wireless technology, and could deter the development of creative, forward-looking solutions in the future. The concerns described below illustrate the range of unintended and problematic consequences that concern T-Mobile's network managers, but are by no means an exhaustive list of uncertainties embodied in the proposed rules.

14. **Differentiation of IP voice packets**. Today, 3G network providers preserve voice quality by, for example, prioritizing voice calls over packet switched data calls. Where there is any clash between voice and other network uses, the network serves voice needs first, and then moves to fulfill demand for data requests. Notwithstanding the carve out for voice prioritization, from my reading of the NPRM, this might violate the proposed "nondiscrimination" rule, at least in the context of voice services provided in an all IP-format in LTE-based 4G networks.

15. **Nondiscrimination and Network Performance.** The proposed nondiscrimination rule could interfere with other useful network management techniques. Today, for example, T-Mobile's network has the ability to optimize network performance and customers' experience through techniques such as compression of website or video content. This compression can increase transmission speeds and improve the client-server interactions between the customer and the website and improve the customer's experience by, for example, compressing a streaming video so that it is "resized" for viewing over the small phone. This type of management could be undermined by the proposed rules.

16. There are even more important network management techniques that could be endangered by the NPRM's proposed rule. T-Mobile is evaluating techniques in UMTS networks that allow for the reprioritization of traffic based on application type with the goal of providing the best user experience for all users. For example, if there are users in a cell that are engaged in a "real-time" service (*e.g.* watching a streaming video), as well as users with devices that are engaged in applications that are less latency-sensitive (*e.g.,* downloading email), it is advantageous from the perspective of the network and users overall to depriortize (or minimally delay, by milliseconds or seconds) the email traffic in order to allow the "live" traffic to go through to the actively-engaged users. Doing this would mean that the email user might end up receiving the email a few seconds later, but this incremental delay might not even be perceptible. That is especially true where the small delay occurs in connection with "passive" email downloading—i.e., automatic downloads for email that a device like a Blackberry does proactively even when the user is not actively engaged in using the device. And this delay (in either case) would be far less disruptive and quality-affecting than a delay in the real-time viewing of a video stream (or a VoIP call).

17. These sorts of management techniques involve "scheduling" algorithms, "channel selection" (i.e., assigning lower power/lower throughput channels to certain applications), and could even be accomplished by dividing applications up by frequency—and by other complicated network algorithms. These techniques either exist today or are in the development or deployment stages, and they will ultimately become a key component of network management as more and more bandwidth-intensive and performance-sensitive applications are brought onto the shared network. They will need to be employed on a near-constant basis to manage the

network load and fairly serve the different needs of different users, devices, and applications. Without the flexibility to employ such measures, all users and all applications would suffer.

18. I understand that the NPRM may be intended to protect this type of activity as "reasonable network management," but relying on that exception raises many concerns for network engineers. Different providers may employ these algorithms based on different determinations about how different applications should be treated, and the right approach will turn on the mix of uses, devices and applications on any given provider's network at any given moment in time. There is no "rule book" defining what mix or treatment is "reasonable"—especially because these technologies and techniques are so new. I also note that over time, prioritization techniques and capabilities may be enhanced with forward-looking technological developments to allow even more enhanced and more dynamic quality of service assurances that could be valuable for certain applications and services offered by content and application providers or to address important social objectives. The NPRM could preclude T-Mobile from offering those capabilities for a fee, which makes no sense. That may make it impossible for us to develop those capabilities, and/or impossible for the applications and content that need that prioritization to develop at all.

19. For example, I can envision that content providers might want to work with carriers to develop the capability to better stream high quality video over 3G or 4G networks. Since video streaming is jitter and error sensitive, it is very difficult to offer high quality video service over wireless devices, particularly to a mobile user moving from cell tower to cell tower. And, because video is bandwidth-hungry, streaming video applications (especially high quality ones) could interfere with other sensitive applications such as voice. I understand that engineers

are exploring various techniques that might help address this problem, including prioritization techniques (and other techniques such as the use of distributed video-server nodes throughout the wireless network). One or more content providers might be willing to partner with T-Mobile (or with several wireless providers) to invest in such a solution. I am concerned that these types of developments, particularly if offered on a commercial basis, would be prohibited as "discriminatory" because they would be designed for specific types of applications.

20. **Responding to Threats or Suspicious Applications.** Providers need the flexibility to limit suspicious applications until they are tested and to constrain use of potentially disruptive applications at least temporarily to prevent collateral damage to other applications and services on the network. For example, it should be obvious that T-Mobile would have had the right to block the instant messaging application discussed above, which directly threatened scarce network resources. And it is not always responsible to wait until an application has harmed the network to act: From time to time, T-Mobile will restrict applications from a certain source that has been particularly problematic in the past—at least until the developer has certified (or T-Mobile has verified) that the applications meet network standards. T-Mobile may also take prudent preventative action when it encounters an application that is similar to others that have carried viruses, worms, or cybersecurity threats in the past. Under the proposed rules, however, a network manager faced with a previously unknown but potentially harmful application cannot be confident that any specific response to this threat will be deemed reasonable in hindsight, and in the face of such second-guessing may be extremely reluctant to take good faith steps to protect the security and quality of the network from new threats. Every time an engineer confronts a new situation, he or she will have to weigh prompt action against the threat of regulatory or

judicial sanction. This will consume critically valuable time and resources and could constrain network management decisions. It also could deter or at least seriously delay creative new network management techniques and technologies.

I, Grant Castle, declare under penalty of perjury that, to the best of my knowledge, the foregoing is true and correct.

Grant Castle

Date: January 12, 2010