# ATTACHMENT E

**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 |

**JOINT DECLARATION OF MICHAEL D. POLING AND THOMAS K. SAWANOBORI**

## I. INTRODUCTION

1. The purpose of this declaration is to describe the reasons that Internet access providers engage in network management, review some of the types of network management practices providers commonly deploy today, and explain why providers need flexibility to engage in network management going forward.

2. As an initial matter, network management is not new or unique to the provision of Internet access services. Telecommunications carriers have long managed traffic on their networks to better serve their customers, and the need to manage Internet access service is similar, although the nature of the challenges to the network and to users is different and even greater. This need to engage actively in network management is widely accepted, and both network providers and other participants in the Internet ecosystem (e.g., content providers, search engines, and caching providers) have long engaged in various forms of network management.

3. In the normal course of business, Verizon and Verizon Wireless do not block or degrade Internet traffic. Verizon and Verizon Wireless engage in network management practices for legitimate purposes that stem from security needs, capacity or congestion management, and service optimization. The flexibility to apply network management practices

is critical to providing our customers with a reliable, safe, and quality on-line experience. Flexibility is essential because of the wide range of issues that warrant network management. Some network management practices are carried out in the regular course of business, such as augmenting capacity in response to particular utilization levels, while others (such as responding to specific security threats) are invoked in real time in response to events as they occur.

4. This declaration covers the following: (1) identification of declarants; (2) description of commonly deployed network management practices to safeguard users, protect network integrity, address network capacity, and optimize services for subscribers; (3) discussion of the extent to which network management is interwoven in all parts of the Internet ecosystem; and (4) explanation of the importance of allowing providers the flexibility to manage their networks and, conversely, how uncertainty created by net neutrality rules – even ones permitting "reasonable" network management practices – would undermine providers' ability to respond quickly and adequately to emerging threats and risks.

## II. DECLARANTS

*Michael D. Poling*

5. I, Michael D. Poling, serve as Senior Vice President – Network Operations for Verizon Services Operations ("VSO"), with overall responsibility for VSO's global network operations including network creation, network management, surveillance/maintenance, and network security. Prior to my appointment to Network Operations in 2009, I held a number of positions within the company, including Senior Vice President – National Network Services, Vice President – Surveillance, Maintenance and Tier II Support, Vice President – Broadband Operations and Processes, and Vice President of Portal Management. I hold a Bachelor's Degree in Civil Engineering from West Virginia University and a Master of Science in

Information Systems Engineering from Polytechnic University. I am jointly responsible for all of this declaration, with the exception of the paragraphs relating only to wireless matters (paragraphs 13(g), 17, 19-29, and 39-40), which are covered by my co-declarant Mr. Sawanobori.

*Thomas K. Sawanobori*

6. I, Thomas K. Sawanobori, serve as Vice President of Network and Technology Strategy for Verizon, with overall responsibility for technology strategy and planning, focusing on wireless networks. In my previous role as Vice President, Network Planning for Verizon Wireless, I led technology direction, planning, and evolution of the radio and core network. My operational experience includes leading the Northern California team to expand coverage, improve performance, and deploy the EV-DO wireless broadband network. I hold a Bachelor's Degree in Mechanical Engineering from Duke University and a Master of Science Degree in Engineering from California State University, Fullerton. I am jointly or individually responsible for all of this declaration.

## III. NETWORK MANAGEMENT PRACTICES – TODAY AND TOMORROW

7. Internet access providers, including Verizon and Verizon Wireless, engage in network management to prevent and defend against harms to users, their networks, and the Internet at large; manage capacity or congestion; and optimize the network or services for users' benefit. We discuss below a sampling of the network management practices that providers employ today – and will need to employ going forward – to address these three important purposes.

8. ***Protecting Users and Network Integrity***. By its open nature, the Internet provides opportunities for those who seek to cause harm to users or the network. With the rapid

growth of the Internet and broadband communications more generally, hackers and other attackers are aggressively engaged in launching increasingly challenging threats against consumers and enterprise users, networks, and the Internet itself. These pernicious attacks are often major news events, such as the Melissa and Nimba viruses and the Code Red worm, but less-publicized attacks occur regularly. As described below, these attacks come in many forms, and the sources and methods of attack are constantly changing. Indeed, attackers often alter the way they hide their identity and the techniques they use to engage users and the network. Some threats originate in the U.S., but a large proportion are launched offshore. As a result, all members of the ecosystem – not just network providers – engage in a constant battle against Internet-borne threats in an attempt to block or limit the risk of these harms. The actions taken by Internet security professionals must evolve and change dynamically as the threats themselves evolve. Preventing and defending against attacks requires flexible, agile network management practices and quick responses to emerging threats if harm is to be limited and to ensure continuity of critical services. It also requires modifying equipment, architecture, design, and techniques in order to identify and defend against new forms of attacks.

9. Internet viruses and other malicious acts pose a threat not only to network providers. They also threaten national security, and they are growing. This fact is reflected in the Cybersecurity Act of 2009, S.773, as introduced by Senators John D. Rockefeller IV and Olympia Snowe on April 1, 2009. The Cybersecurity Act highlights the enormous size and complexity of the issues network providers and others in the Internet ecosystem face in defending against cyber threats:

a. *Scope of the Threat*. The Internet, telecommunications networks, and computer systems are increasingly being targeted by state and non-state actors, and these trends are likely to continue. Cyber-espionage and cybercrime is on the rise.

b. *Evolving Nature*. Cyber threats are evolving and growing as attackers are constantly responding to defenses put in place.

c. *Magnitude*. The protection of cyberspace is a major national security problem for the United States. Losing the struggle will wreak serious harm on the Nation's economic health and national security.

10. President Obama emphasized the importance of cybersecurity in his May 29, 2009 speech "Securing Our Nation's Cyber Infrastructure." These remarks underscore that cyber threats pose some of the most serious challenges facing our Nation's economy and national security and put at risk our global competitiveness. As President Obama's comments make clear, America's prosperity in the 21st century depends on effective cybersecurity, and America's network providers are at the frontline of the battle to safeguard consumers, businesses, and governments from these threats.

11. Additional information regarding the scope and depth of the current cyber threat, and its impact on the Nation's economy, security, infrastructure, and other key resources, is available from a variety of government sources, including: the White House (see http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf and http://www.whitehouse.gov/cyberreview/documents); the U.S. Department of Justice, Computer Crime & Intellectual Property Section (see http://www.cybercrime.gov/); the Director of National Intelligence (see http://www.dni.gov/testimonies/20090212_testimony.pdf); the National Institute of Standards and Technology, Information Technology Laboratory (see

http://www.nist.gov/testimony/2009/cyber%20sec-smart%20grid%20house%20hs%20hearing%20furlani%20final.pdf); and the Internet Crime Complaint Center (see http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf), as well as other non-government sources.

12. In responding to certain threats, network providers must first determine whether a threat exists, and then proceed to assess risks, identify responses and, in some cases, act quickly to counter the threat. Sources of information include the provider's own internal resources and experience in identifying and understanding the key characteristics of cyber attacks; the Computer Emergency Response Team/Coordination Center ("CERT/CC") located at Carnegie Mellon University's Software Engineering Center, which analyzes Internet security, monitors vulnerabilities, and conveys that information to the Internet community; the Department of Homeland Security's Computer Emergency Readiness Team ("U.S.-CERT"), which is a particularly valuable information source for disseminating threat information known to the Federal government to industry; other third party sources, including vendors that learn of vulnerabilities in their products and other Internet access providers that experience attacks; and organizations like CERT/CC and U.S.-CERT in other countries. The variety and sources of intelligence change as the scope and nature of threats evolve.

13. Based on the information they gather, network and other providers may need to respond in real time to limit threats, safeguard users, or protect the network and the Internet. Attacks that threaten network integrity or connected devices come in myriad forms, including Distributed Denial-of-Service ("DDOS") attacks and propagation of computer viruses, worms, and other forms of malware, as well as botnets. Harms to consumers can result from these threats, as well as from other forms of malicious activity, including phishing (fraud and identity

theft), spam (which is used as a delivery vehicle for phishing sites, malware, and worms), and delivery of illegal material (such as child pornography). Network providers act to protect the network and their customers, and they offer security services to their customers ranging from anti-virus, anti-spyware, and firewall software for consumers, to sophisticated managed security services for enterprise and government customers. Below is a fuller description of some threats to networks or individual customers, as well as several well-accepted and non-controversial measures that have been widely deployed to combat these threats:

*DDOS Attack*

a. A DDOS attack is an attempt to make a computer or network resource unavailable to its intended users. These attacks are sometimes launched from zombie computers, which are computers connected to the Internet that have been compromised and can be commanded by a third party (often located outside the U.S.) through a botnet. While many DDOS attacks are intentional, some can be unintentional, as where customer equipment (routers, modems, etc.) has been misconfigured.

b. Techniques used to combat DDOS attacks include IP address null routing, or "black-hole" routing, in which routers drop traffic to specific Internet Protocol ("IP") addresses (such as a computer that is being used as a botnet controller or a computer that is the target of a DDOS attack) to disrupt IP communications to those addresses. By dropping all packets intended to go to a specific IP address, network providers may be able to (1) prevent zombie machines from communicating with a controller machine, thus interfering with the hacker's control over a botnot, or (2) remove unwanted DDOS attack traffic from the

network generally, thereby reducing congestion at various points in the network. We note that the use of black-hole routing and some other threat mitigation techniques described below carry the downside risk that some amount of benign traffic will be adversely affected, as discussed further in Section V.

c. Another DDOS mitigation technique is traffic "scrubbing," whereby all traffic to the victim IP address is re-routed through a series of systems that attempt to identify – and drop – malicious packets (packets that are part of the attack) while allowing benign packets to proceed to their destination.

*Malware*

d. Malware, including computer viruses and worms, consists of types of computer programs designed to damage or compromise the integrity of a device or a network or other system that relies on the device. Among the types of malware behind many data breaches are keyloggers and spyware, which collect, monitor, and log the actions of a system user to collect personal information, including usernames, passwords, and like information. Other types of malware are designed to provide a remote user with control over the machine on which the malware is installed, enabling that remote user to install and use his or her own software on that machine for his or her own purposes.

e. Historically, malware distribution methods have often been thought of as involving self-replicating viruses and worms that spread themselves through email or by network-based scanning activity or other means. Such methods may result in rapid and widespread propagation, which can result in availability losses and extensive clean-up for infected end users. Malware may also be distributed

through malicious code embedded in websites, through social engineering, phishing attacks (described below), and other means. Because malware is an increasingly useful tool for organized crime in the U.S. and around the world, it is becoming more directed, innovative, and stealthy as criminals seek to minimize detection and maximize their capabilities. Newer, more elaborate varieties of malware are able to bypass existing controls and encryption and gain access to applications and databases in a more covert and effective manner. Some of the new means by which malware is distributed include social networking sites and popular Internet websites that have been compromised. Visitors to those sites may not even know that they have been infected during the course of their visit.

f. One defense against the propagation of malware over the network is port filtering. Once traffic is determined to pose a threat, the provider may filter and drop traffic based on the logical Transmission Control Protocol ("TCP") or User Diagram Protocol ("UDP") port associated with that traffic, in order to slow or stop the spread of specific worm or virus traffic. Another network-based defense to the distribution of malware through websites or phishing attacks is null-routing the IP addresses of those websites to limit the number of users inadvertently infected through such sites until the site owner or operator or web hosting company can take remedial action.

g. Although malware is less common within the wireless environment, it can manifest itself on pieces of software that reside on users' handsets, which can then migrate onto the shared network infrastructure and impact many thousands of users. Strategies for dealing with these threats include prevention and effective

detection and removal and, if these efforts fail, steps to minimize impacts. For example, device-based controls can be used, including code signing to certify software authenticity; and access controls to limit access to particular application programmable interfaces containing sensitive information (like address books). Network-based anti-virus solutions, designed to prevent the introduction of viruses from external sources, are other possible defenses. But, for such network-based defenses to be effective, there would need to be a broader set of harmonized controls between user devices, the applications that ride on these devices, and the network elements that control their interaction with others.

*Phishing*

h. Phishing is a social engineering technique in which an attacker uses fraudulent electronic communication (usually an email) to lure the recipient to a website that closely resembles a legitimate website and then to divulge personal information. Most such fraudulent communications appear to come from a legitimate entity (like a bank or even the user's Internet access provider) and contain authentic-looking content. Some phishing attacks request that information be sent via reply while others contain a link to the fraudulent website.

i. Phishing techniques have improved over the years to the point where it is very difficult for a typical end user to determine the authenticity of these harmful email messages. The information collected from phishing schemes varies from identity theft and financial fraud to the use of stolen email account credentials to send more phishing and spam email. Many protective measures used to stop phishing mirror those used to stop spam while others are more targeted.

j. Black-hole routing, discussed above, is one technique network operators use to prevent customers from reaching phishing sites (and being phished). In addition, several techniques are available using the Domain Name System ("DNS"). These techniques, when used by third-party hackers and spammers, can severely disrupt traffic flow on the Internet. When used by Internet access providers, however, these same methods can minimize negative impact to customers. For example, DNS "poisoning" is a technique used to prevent customers from being victimized by preventing their web browser from successfully navigating to the malicious website. That is, to find websites by domain names, a user's computer must contact a DNS server to look up the IP address associated with that domain name. Network providers as well as third-party DNS providers such as Google and OpenDNS can protect users from exposure to those malicious sites by rendering those sites unreachable to the customer through domain-name based navigation.

k. Other techniques for combating phishing include configuring email clients to render html emails as text and email filtering to filter out spam.

*Spam*

l. Spam has moved from merely being an annoyance cluttering a user's inbox to a primary delivery device for propagating viruses, worms, and other malware and phishing scams directed at email and wireless Short Message Services ("SMS"). Although spam can be defined as the abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately, there is no universally-accepted definition. According to the Messaging Anti-Abuse Working Group ("MAAWG"), an industry working group focused on best practices to mitigate

against abusive emails, the percentage of email identified as abusive was as high as 89% to 92% for all of 2008 (http://www.maawg.org/about/MAAWG_2008-Q3Q4_Metrics_Report.pdf) and as high as 89% to 91% for the twelve-month period ending in June 2009 (http://www.maawg.org/about/MAAWG_2009-Q1Q2_Metrics_Report_11.pdf). (MAAWG measures "abusive email" rather than spam because the latter lacks a universally-accepted definition. MAAWG defines abusive email as "communications that seek to exploit the end user.")

m. Today, the vast majority of all spam traversing the Internet is generated from botnets. The techniques used by these botnets change frequently and require Internet access providers to adjust existing protective mechanisms as well as create new ones in order to continuously manage the threat. In recent years, botnets have begun using compromised user email credentials in order to send spam through otherwise legitimate sources which are unlikely to be caught by Internet access providers. Providers must be able to find new methods to detect compromised account activity and to stop the abuse while allowing email from their legitimate customers to be delivered.

n. There are many techniques that are or may be employed to defend against spam, including black-hole routing and email throttling (network- or server-based measures that rate-limit the volume of email that can be sent by individual end-user machines, thereby impairing the efficient delivery of thousands or millions of emails and serving as a deterrent to spam operators). Other techniques include IP address blocking/filtering, or IP address "blacklisting," in which email traffic

from IP addresses associated with known senders of spam is blocked at the point of ingress to the network.

o. Another technique is port filtering, discussed above, which is used to prevent "infected" users from sending unauthenticated email using their home machines as an email server. Port filtering is consistent with the anti-spam recommendations of the Federal Trade Commission, MAAWG and the London Action Plan ("LAP"). It is designed to reduce spam sent from virus-infected personal computers by preventing the virus-infected computer from acting as a mail server. These changes only impact the customer's outbound email settings, and reduce the chance of a customer's PC being used to send email without his or her knowledge.

p. Email filtering is also used in email servers to filter out spam. For example, an email service provider's mail servers may compare hashes of inbound email messages with known spam signatures or hashes, and take remedial action if there is a match, based either on the service provider's network management policies or options selected by the customer. On the outbound side, if a customer attempts to send a message determined to be spam, the mail servers may send the customer an error message or other response from the email service provider.

q. Email rate limiting is another technique used to combat spam. An email service provider may limit the number of recipients of a given message or the number of emails that a given end user may send within a defined period of time. For example, an email message being sent to an inordinately high number of email

addresses may be dropped by the email service provider's mail servers, or may be subject to quarantine or other action.

r. Another technique that may be used to combat spam is "tar pitting," in which inbound email from suspicious email servers may be delayed for some nominal period of time while mail from valid senders is processed without such a delay.

*Unlawful Traffic*

s. Illegal traffic can include the distribution of child pornography. Botnets can be used to surreptitiously disseminate this illegal material, but illegal content can reside on servers located on any network or housed at a user's location.

t. Where child pornography is discovered to reside on a network provider's own servers, the provider will immediately remove and secure the illegal material for law enforcement under most circumstances. In addition, any person engaged in providing an electronic communication service or a remote computing service who learns of any information that reflects an apparent violation of child pornography laws is legally obligated to report such facts and circumstances to the National Center for Missing and Exploited Children ("NCMEC"). Network providers, website hosting providers, and content and application providers may also be exploring other innovative forms of addressing the dissemination of child pornography, such as the use of image hashes to filter or block illegal content.

14. ***Addressing Capacity or Congestion Issues***. In addition to the types of management described above, exponential growth in Internet traffic volume and broadband usage also necessitates increased use of network management to ensure reliable passage of traffic over available bandwidth and to optimize the network and services for consumers – both

today and tomorrow. This growth is attributable to a number of factors, including a general increase in traffic volume; growing use of bandwidth-intensive applications (such as video, gaming and peer-to-peer traffic); the rise in latency- and jitter-sensitive traffic (such as streaming video, VoIP and multi-party gaming); the rise in upstream traffic (such as uploading videos); and the rise of non-Internet offerings sent over a shared "pipe" (such as voice and subscription video).

15. Further traffic growth is anticipated as the nation increasingly relies on broadband communications as an integral component of Health IT, Smart Grid, Education and Workforce Development, and many other welfare-enhancing advancements.

16. Because traffic growth has been increasing dramatically and is expected to continue, networks must combine managing existing capacity while augmenting capacity in support of the terms of service selected by customers. In order to provide an affordable service, Internet access providers cannot maintain dedicated bandwidth from each customer to the Internet handoff point or prices would be prohibitive for individual consumers (similar to prices for large businesses with dedicated links). Thus, active network management is required to efficiently manage the shared bandwidth and provide subscribers with an Internet experience that comports with or exceeds their expectations, as identified in their terms of service. In some circumstances, this may result in redirecting traffic or controlling the amount of resources that any one user can demand from the network in order to ensure fairness to all customers. In the case of Verizon and Verizon Wireless, our approach is to manage the available capacity to give the user a quality experience for the services he or she wants to use at any given time.

17. This goal is particularly complex for wireless services, because of the unique characteristics and requirements of wireless communications. Chief among them is user

mobility, which creates usage uncertainty and further complicates the need for wireless providers to address shared capacity, operate on limited bandwidth, and have interdependent networks, devices, and applications.

a. *Mobility*. The number and mix of subscribers in a given area constantly changes – sometimes in highly unpredictable ways. Moreover, mobile wireless networks enable customers to change locations and still communicate with the network while travelling. As a result, wireless networks need to accommodate a constantly changing mix and volume of voice and data users and traffic at individual cell site locations. The network must engage in real-time, dynamic management of the radio frequency ("RF") "last mile" connections. Resource availability and network performance in the mobile wireless environment are thus subject to significantly more variation in usage than a fixed network (although fixed wireless services frequently share bandwidth resources with mobile services and therefore can be subject to the same constraints). In addition, the need to follow individual users throughout the network also imposes bandwidth "overhead" on the system, because there must always be a small reserve of capacity at each cell site in order to prepare for either the next user to originate a session or for a current session to engage in the next handoff. This further limits the spectrum resource that can be allocated to any one user.

b. *Shared User Access in a Fluctuating Environment*. Mobile systems are shared bandwidth systems – meaning the "last mile" to the user is a shared RF link. The bandwidth is spread across all the active customers in the vicinity of the same cell site – as noted above, mobility results in the number of active customers

constantly changing. Available bandwidth is constrained by the RF signal strength and quality, which varies with geography, weather, traffic, speed, and the position of the people and objects near the device. A user nearer to the cell site with very good RF channel conditions will have access to higher throughput than one farther away, and the network must be able to recognize these differences in order to optimally allocate resources to all of the users in the cell area. As a result, heavy use by one or more wireless broadband customers can and will impact the ability to access the network and throughput at which individual users can communicate.

c. *Bandwidth Availability*. Wireless networks also face management challenges because they operate with comparatively limited bandwidth. First, the throughput of a wireless network is more constrained than a wired infrastructure. Because the RF link to the user must compensate for interference from other users and noise, the attainable throughput for wireless broadband is significantly less than fiber even on comparable bandwidths. In other words, fiber operates in an essentially noiseless environment, while wireless-based connections must account for interference from nearby users in adjacent bands as well as all users sharing the same spectrum in any one cell site. Further, adding more wireless capacity is limited not only by technological and financial resources but by spectrum availability as well. Given the bandwidth limits of spectrum-based services, a handful of customers, by choosing to upload or download data that require significant bandwidth, may degrade the wireless experience for all other customers in the vicinity of the cell site.

d. *Interdependence of the Network, Devices, and Applications*. While the FCC's wireline broadband principles envision an environment where the network and the computers that attach to it are essentially independent, a wireless device operates as an integral part of the provider's network. These wireless devices are deemed "mobile stations" under the FCC rules and are part of the provider's regulated ecosystem. Wireless providers therefore also must ensure that devices are coordinated and compliant with technical rules and public interest obligations such as E911 and CALEA, which requires additional oversight and network management.

18. ***Optimizing Services for Consumers***. Another goal of network management is to optimize services for consumers. In general, network operators provide Internet access services on a "best efforts" basis. Providers seek to maintain equitable access to network resources for the most users and ensure that they have access to the capacity expected at any given time.

19. Wireless operators in particular engage in a variety of practices to optimize network usage, address congestion, and increase efficiency. As a threshold matter, adding capacity to a wireless network generally requires adding cell sites and/or adding spectrum. Both of these can take months or years: cell sites may require various land use approvals before construction, while acquisition of spectrum depends on its availability at auction or through the secondary market and may require regulatory approval. Even when spectrum is available, the laws of physics limit how much capacity can be added at any given site. While wireless engineers can plan for typical peak loads, it is not practical or economical to build for much higher levels of capacity. Moreover, the limited spectrum resources are shared – so whether

there is congestion or not, it is important to be able to provide all users with fair access to the bandwidth available because other factors affect the end user radio link.

20. For instance, to operate the network efficiently and optimize data throughput, wireless operators may use sophisticated queuing and scheduling algorithms at each cell site that send more packets of data to and from users during times of good signal-to-noise conditions and fewer packets when signal-to-noise conditions are bad. As an example, EVDO networks use the "proportional fairness algorithm" which, when needed, delays some data packets until the radio channel conditions change. This increases the throughput per cell and increases the average throughput for the user.

21. Wireless operators may also approach low latency-tolerant, low bandwidth applications such as VoIP in other ways. For example, they may use quality of service marking at the cell site to instruct the scheduler to bypass the throughput performance improvements and send the data in real time but at reduced speed. This treatment can improve the quality of low bandwidth voice while still enabling high capacity data to simultaneously be served by the cell site. Network management practices like these help to optimize user experiences over wireless data networks. As network technology moves further toward all-IP, it is essential that the marketplace offer quality of service for latency-sensitive applications such as VoIP and certain video applications.

22. In addition, because congestion is difficult to predict on a cell site-specific, real-time basis given user mobility, wireless providers may utilize predictive modeling to assist in determining where congestion might occur. However, given the size, complexity, and growth of wireless data, it may not be practical or realistic to accurately predict congestion. Furthermore, if a customer in a congested cell site is utilizing a disproportionate share of the capacity of that

cell, it may be appropriate to temporarily adjust the throughput of that user so that others can fairly share the available bandwidth, subject to disclosure of such a practice to the customer. Wireless providers may also adjust throughput and network resources of certain users if those users are employing applications and devices that can degrade the service of other users, such as applications that keep an access connection alive for more than is needed for typical usage. The network, for example, can be adversely impacted by an application's behavior with respect to frequency and duration of "keep alive" and retry functions and, left unchecked, these features can overwhelm a cell site without achieving any benefit to the end user.

23. Likewise, wireless network operators also manage Media Access Control ("MAC") address functions at the cell site level. MAC addresses are used to assign individual radio channels to each active user connected to a particular cell site. Although there is no limit to the number of mobile devices that can be in the coverage area of a single cell site, there is a hard limit to the number of mobile devices that can actively use the radio resources. In other words, the MAC is used like a token. If a user has a token, then it can transmit data. Once the user's data queue has emptied, the device returns the token so that it can be assigned to the next mobile device with data to transmit. Thus, if a cell site's inventory of MAC addresses is exhausted at a particular time, other users are unable to establish connections. Unfortunately, some applications and devices hold onto a MAC address, once assigned, even when the particular application or device is not actively being used to transmit data to the network. Other users are then blocked from obtaining a MAC address that they need to send and receive data. An effective network management practice is to drop the otherwise idle mobile application or device that is taking up a MAC address and assign it to another mobile device.

24. There are also special issues presented in managing wireless networks supporting third-party devices. While the FCC has adopted detailed rules in Part 68 governing the connection of equipment located at the customer's premises to the wireline network, there are no corresponding rules for wireless. As a result, to a much greater degree than with wireline networks, each wireless network is engineered differently, built to accommodate different air interfaces and frequencies, and contains varying network elements used to offer content and meet regulatory requirements. In other words, there is no "legal device" concept in the wireless world other than a device that a network operator has approved or certified for use in accordance with its technical requirements and regulatory obligations.

25. The devices and applications offered by a network are generally the result of an extensive development and testing process intended to ensure that they work well together and work well with the network. In Verizon Wireless's case, this includes testing to ensure that devices meet strict interference and general compliance guidelines, including "Safe for Network" testing, validation of operation with network infrastructure providers, and E911 capabilities, among others. It also includes testing to optimize performance with the functionalities and services available on the Verizon Wireless network. Wireless providers also design products and services to work efficiently together. Even parts used within the devices, e.g., the vocoder, influence the spectral efficiency of the end product. Further, as networks and services evolve over time, many wireless providers design products that can take advantage of new network capabilities. For example, smartphones can now record and send video.

26. Through the Open Development program, Verizon Wireless enables device manufacturers and developers to go through a streamlined certification process so that their devices can be optimized for the network. Open Development is the company's streamlined and

efficient device certification program designed to allow and encourage the development community to create new and non-traditional products, applications, and services, beyond what Verizon Wireless offers in its portfolio, and to bring these to the marketplace running on the Verizon Wireless network. To date, over 85 specialty devices have been certified by Open Development for use on the Verizon Wireless network, from Smart Grid and offender compliance monitors to senior citizen phones and an e-reader. Many more devices are in process, including fleet tracking systems, portable gaming devices, health status tracking meters, and vending machines.

27. It is important to note, however, that Verizon Wireless also allows a user to attach independent, technically compatible devices to its network, although the user may not be able to avail itself of all the capabilities that the device has to offer because it is not optimized for the network. Even among networks that rely on the same air interface technology, standards bodies' work covers some but not all of the network requirements, and each network is designed differently. Devices built to standards bodies' network access specifications, therefore, will not necessarily perform in the same way as those that are optimized for use on a particular network. Users may, however, submit a third party device to Verizon Wireless for possible optimization.

28. As the FCC points out, wireless carriers are developing devices that are able to connect to a network in different ways. The use of a Subscriber Identify Module ("SIM") card, or a preregistered chip inserted into a device, can in some situations facilitate this network-independent connection, but not in all cases. For example, in Europe where SIM cards were first deployed, regulators have mandated the radio technology choice in each wireless band. Because all network operators are required to have exactly the same technology, the swapping of SIM cards is an effective way of providing network access across different providers in

Europe. In the United States, however, the FCC does not mandate technology choices. While this has facilitated technology innovation, multiple technology networks create a barrier to absolute network interoperability. A SIM card is not universal. A SIM designed to work in a GSM network is different from a SIM designed to work in a CDMA network, and they are not interchangeable. Moreover, the device must be designed to work with the specific spectrum bands on the network with which the SIM is associated. Even if the FCC were to require carriers to provide SIM cards for all devices, there would still be incompatibility with respect to the device, the SIM card, and the network technology. SIM swapping could be possible between like-technology networks (such as AT&T and T-Mobile, or Verizon Wireless and Sprint), but it would not be possible between disparate technologies.

29. Another practice used to connect to the network is tethering, which allows the mobile device to act as a modem while the connected device, such as a computer, provides the operating system. For example, tethering essentially converts a smartphone into an aircard for a laptop. Tethering can thus increase the data usage of a device to accommodate the larger screen of the computer and differing usage patterns from the mobile device. Because it increases data usage, tethering can increase traffic and congestion, which could impact services or networks designed specifically for small screen data usage. A requirement that wireless providers offer tethering would force providers to adjust predicted usage patterns and network management planning, in effect compelling providers to modify business models to accommodate increased and differing data usage than what would be expected from the mobile device alone.

## IV. NETWORK MANAGEMENT THROUGHOUT THE INTERNET ECOSYSTEM

30. Notwithstanding the FCC's focus on Internet access providers and its proposal to impose rules only on such providers, network management is omnipresent throughout the

Internet ecosystem. Indeed, the need for Internet access providers to engage in network management is not inherently different from practices widely engaged in by others in the Internet ecosystem, such as content providers, search engines and caching providers. However, the proposed rules threaten to introduce specific inequities into the range and choice of network management practices available to broadband Internet access providers in a way that is not technology neutral and ignores the interconnected nature of the Internet ecosystem.

31. Combating spam is a good example. In addition to broadband Internet access providers, numerous other service providers, including Google, Yahoo, and Microsoft, offer email service. Such entities all engage in network practices to combat spam. As noted above, a broadband Internet access provider might engage in IP blacklisting to prevent the delivery of email from known spammers into the provider's network. While this management technique and its practice in individual circumstances would be subject to scrutiny for "reasonableness" under the proposed rules, a standalone email service provider engaged in the very same IP blacklisting practice would not be subject to any such review.

32. The same situation holds true for the provision of DNS, the look-up service used to translate words into IP addresses to reach a website on the Internet. While Internet access subscribers may use their network provider's DNS service, competing DNS services exist, such as OpenDNS and Google DNS. DNS is a critical element of Internet connectivity. For example, with regard to VoIP, when DNS is not functioning properly, phone calls may not work. Because voice and video rely on near real-time management to provide a seamless service to the subscriber, prompt reaction to fixing a problem is essential. Under the proposed rules, however, network management techniques or new features that broadband Internet access providers apply to their DNS services or to resolve any DNS service issues would be subject to

"reasonableness" review, while the activities of competing non-network DNS providers would not.

33. Other examples abound. Content providers have to manage traffic volumes and thus balance and distribute traffic as necessary across networks of servers to maintain well-functioning sites and efficient content delivery.

34. Likewise, third party caching providers like Akamai, which push content closer to end users by serving as wholesale content delivery enablers, also manage their servers to help the Internet withstand the crush of content requests. While this management encompasses detecting and avoiding Internet problem spots and vulnerabilities to ensure websites, downloads, ad networks, and applications perform well, it involves the manipulation of some – but not all – traffic. For example, some content servers cap how many streams they are concurrently serving to ensure stream quality. This may result in some new users being blocked, but preserves the quality for users already connected.

35. In addition, a search engine like Google maintains its own network and distributed databases and servers to address threats and manage traffic flow. In Google's case, it owns its own fiber backbone and can engage in active management as a network owner. Google can determine what traffic is routed over its network versus the public Internet, managing traffic volume according to its quality of service goals. Google can also engage in network management to respond to the threats to its network, e.g., responding to DDOS attacks, brute force attempts to compromise its servers, or other intrusions.

36. Indeed, Google's recent statement regarding a cyber attack on its corporate infrastructure originating from China underscores the importance of network management by all types of providers in the Internet ecosystem. Of particular note, Google observed

(http://googleblog.blogspot.com/2010/01/new-approach-to-china.html) that it has "already used information gained from this attack to make infrastructure and architectural improvements that enhance security for Google and for our users."

37. In sum, content providers, search engines, and caching providers all may engage in a wide range of network management for many of the same reasons as Internet access providers, i.e., prevention of harm, management of capacity, and optimization of service.

## V. THE NEED FOR FLEXIBILITY TO MANAGE THE NETWORK

38. Internet access providers need flexibility to adapt network management practices in real time to respond to emerging threats and address ever-changing capacity concerns, all while continually optimizing services for their subscribers in new and innovative ways. If the Commission adopts rules identified in or similar to those in the *Preserving the Open Internet Notice*, it will limit the flexibility providers need to manage their networks – even with an exception for "reasonable network management." Indeed, industry best practices, which can be updated and revised as needed, already provide sufficient guidelines for network operators without FCC regulation while providing needed flexibility.

39. Flexibility is critically important to the ability to respond to both active threats and seemingly benign developments on the network. For example, in 2001, Verizon implemented port filtering within its DSL network to protect devices in that network from the effects of the "Code Red" computer worm. In the absence of such filtering, there was concern that as the worm ramped up, Verizon's DSL network might have faced significant network degradation. To address that possibility, Verizon blocked inbound traffic on the affected port to protect routers in Verizon's DSL network, although legitimate traffic could still get through

using different ports. This was a widely-accepted solution, used by Internet service providers and other network managers.

40. In another case, Verizon Wireless discovered a situation where an FCC-certified repeater was improperly installed within a Manhattan office building. This particular installation was performed without the company's knowledge by a well-intentioned customer looking to enhance the coverage within the building. Although the customer was informed by the manufacturer that the FCC-certified device was thoroughly tested to operate effectively on a CDMA network, the implementation immediately proved that there is more to the integration of a device into a wireless network than simple certification.

41. Once the device was installed in the building, local RF engineers immediately began to see degradation in service on both the local and surrounding networks. In the final assessment, this single device negatively impacted about 200 surrounding cell sites within the New York metropolitan area, which resulted in tens of thousands of blocked voice and data sessions. This particular instance resulted in inconveniences to our customer base due to frustration over poor service, as well as lost revenue for Verizon Wireless. More importantly, if it had gone unchecked, it could have prevented the successful completion of 911 calls or similar critical communications – a scenario any provider always strives to avoid.

42. As these examples demonstrate, network engineers must react quickly and in real time to network challenges based on their experience and best judgment. To manage the network against potential harms, for example, providers first need to decide whether a source of information about a threat is sufficiently credible to act upon. Providers also need to determine whether the threat itself is sufficiently serious to warrant countermeasures.

43. In the regulated regime being proposed, network engineers' judgments throughout the decisionmaking chain will inevitably be viewed in the context of a vague legal standard of reasonableness – the violation of which could subject the company to fines or other enforcement action – resulting in uncertainty regarding what constitutes a "reasonable" network management practice. Indeed, if a mitigation technique results in benign traffic being interrupted or impaired, the deployment of that technique might be deemed unreasonable. Moreover, because the threats to networks and the challenges of congestion are constantly changing, the development of legal guidance for engineers on what might constitute reasonable responses would be impractical and continuously out of date. In addition, an Internet access provider needs to manage and coordinate a global response because the threats to U.S.-based assets can come from anywhere in the world and the networks are interconnected.

44. As a result, to protect the company in the face of potential liability, network managers likely would need to consult with legal counsel on a case-by-case basis to determine whether their proposed actions fall within the scope of what is viewed as "reasonable" network management practices. This need for legal clearance will hamper, delay or curtail the ability of providers like Verizon and Verizon Wireless to promptly respond to network challenges, making them slower and less effective. This threat of liability will inevitably result in fewer and less robust responses to threats and challenges, to the detriment of consumers and network integrity.

45. Indeed, the uncertainty created under a regulated regime is magnified because the risk of taking action that results in a "false positive" response increases the risk of liability. Many of the mitigation techniques discussed in Section III above, while widely accepted and effective in preventing harms to the network and users, also come with downside risks that some

amount of benign traffic will be adversely impacted by such action. For example, black-hole routing has the potential to drop some packets involving lawful applications or services intended for lawful recipients or that also happen to be sharing use of the IP address with a hacker; IP address blacklisting operates at the level of the IP address, which makes it difficult for a provider to ascertain in advance the scope and nature of any inadvertent, limited impact on lawful content, applications, and services; port filtering used to prevent the spread of malicious viruses or worms has the potential to block some lawful applications or services that may be using those same ports; traffic scrubbing may result in dropping too many packets, the wrong packets, or introduce delay into the routing process to a degree that certain lawful applications and services suffer degradation or impairment; and BGP route filtering (used to prevent malicious parties from hijacking traffic or routes on the Internet) has the potential to limit users' ability to access certain lawful content, applications and services provided via the routes that the network provider refused to accept. Ultimately, the goal of an Internet access provider is to keep the network and services up and running for as many subscribers as possible, while minimizing (though not always eliminating) any negative consequences to users.

46. In addition, network providers take steps everyday to plan for and manage capacity and congestion and optimize service. Congestion events can require flexibility to respond in real time to address capacity and maintain service. For example, certain events can trigger a spontaneous spike in traffic, such as a sporting event (e.g., the annual Ohio State-Michigan football game) or other limited-duration occurrence (e.g., the Consumer Electronics Show ("CES") or President Obama's inauguration). Moreover, unexpected interruptions, like a natural disaster (e.g., earthquakes in California) or an accident (e.g., a severed link) can likewise have a dramatic impact on network management. As a result, providers may need to make

routing changes, divert traffic over additional or diverse facilities, tunnel traffic through specific network segments, push traffic to cache providers, or otherwise act in near-real time to address congestion or hot-spots in the network.

47. In sum, the proposed FCC framework for determining the lawfulness of network management activities will detract from today's decisionmaking process, where network engineers react quickly based on their experience and best judgment. Instead, the proposed regime would create a serious jeopardy for providers caught between the twin horns of near-term harm to the network or end users and long-term regulatory sanctions for "getting it wrong." Ultimately, it would be consumers – those the proposed rules seek to protect – who would be harmed by such rules, as they become subjected to more attacks and service issues for longer durations while network engineers seek the legal clearances they need to implement recommended technical responses to the attacks. The Commission should thus leave to engineers and network managers – not lawyers and regulators – the flexibility to determine the network management practices that best protect and serve consumers' interests.

**[Remainder of the page intentionally left blank]**

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

Michael D. Poling

Michael D. Poling

January 12, 2010

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

Thomas K. Sawanobori

Executed on January 12, 2010