FEDERAL COMMUNICATIONS COMMISSION

----------X

In re Verizon Wireless

FCC Complaint #:

Complainant,

-against-

Verizon Wireless

----------X

STATE OF NEW YORK)

)ss:

COUNTY OF SUFFOLK)

FEDERAL COMMUNICATIONS SUPPLEMENTAL COMPLAINT AGAINST VERIZON WIRELESS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Regulations

Reports

INTRODUCTION

This supplemental complaint is in response to Verizon Wireless's ("Verizon") initial response to the original complaint filed with the FCC, number 11-C00342645-1.

PRELIMINARY STATEMENT

The instant supplemental complaint is a response to Verizon's answer, received November 16, 2011, to the original complaint filed with the FCC. To my knowledge and belief, there has been no further action taken by any party.

STATEMENT OF FACTS

The initial complaint was filed because of Verizon's potential breach of the requirements of Block C of the wireless spectrum also known as Verizon's fourth generation ("4G") Long Term Evolution network ("LTE"). Verizon has selectively chosen to lock the bootloaders of certain phones under guise of "reasonable network management." The Motorola Droid X, Motorola Droid Bionic and the Motorola Droid Razr, which all run Google's Android OS open-source platform, all share a locked bootloader. The locked state of said bootloader has been demanded by Verizon as overseas models are due to have their bootloaders unlocked in future updates. Confirmed through Motorola, the locked bootloader is a requirement of Verizon and not of Motorola. The locked bootloader prohibits lawful owners of cellular devices to

choose how to customize their devices as well as unduly limits the applications able to be loaded and used on the device. Verizon, through their policy, has crippled these costly devices and has deprived the owners of the devices the full user experience they have paid for and rightly deserve.

ARGUMENT

I. VERIZON'S POLICIES HAVE VIOLATED BLOCK C REQUIREMENTS

"Licensees offering service on spectrum subject to this section shall not deny, limit, or restrict the ability of their customers to use the devices and applications of their choice on the licensee's C Block network…" 47 C.F.R. §27.16(b). The Code of Federal Regulations lists two exceptions to section (b), the applicable of which states "[i]nsofar as such use would not be compliant with published technical standards reasonably necessary for the management or protection of the licensee's network…." 47 C.F.R. §27.16(b)(1). Further, section (e) states "[h]andset locking prohibited. No licensee may disable features on handsets it provides to customers, to the extent such features are compliant with the licensee's standards pursuant to paragraph (b) of this section…." 47 C.F.R. §27.16(e).

A. *An open bootloader is not precluded by the reasonable network management exception to 47 C.F.R. §27.16*

In the FCC's Report and Order of September 23, 2011, the Commission outlines several factors defining reasonable network management: (1) Reduce or mitigate the effects of congestion on its network or to address quality-of-service concerns; (2) address traffic that is unwanted by users or harmful; (3) prevent the transfer of unlawful content; or (4) prevent the unlawful transfer of content." 76 FR 59192-01. However, the Commission goes on to adopt the following definition for reasonable network management: "A network management practice is reasonable if it is appropriate and tailored to achieving a legitimate network management purpose, taking into account the particular network architecture and technology of the broadband Internet access service" allowing for an ad hoc determination. *Id*. Because the Commission has adopted an approach that is wholly governed by a case by case determination, the only effective way to outline a complaint will be to address relevant factors as delineated above.

"A bootloader is usually locked on an Android device because although it's an open source OS, still the manufacturers want you to stick to their Android OS version specifically designed for the device. In order to apply this concept, manufacturers lock the bootloader. With a locked bootloader on Android devices, it is virtually impossible to flash a Custom ROM and forced attempts void warranty as well as usually end up in bricks."[1] Locking a bootloader does not provide any type network management advantage to Verizon. The locking of a bootloader prevents developers having full access to a device to fully customize the kernel of the device in order to provide the end user the best experience. In Verizon's response to this initial complaint, they cite NO specific reasons as to why the bootloader should remain locked or how it will

[1] Obtained from: http://www.addictivetips.com/mobile/what-is-bootloader-and-how-to-unlock-bootloader-on-android-phones-complete-guide/

impact their network. Instead, they choose to recite the language of §27.16 and state "it would allow users to change the phone or otherwise modify the software and, potentially, negatively impact how the phone connects with the network. The addition of unapproved software could also negatively impact the wireless experience for other customers." Verizon does not indicate how any negative impact would occur. Verizon has chosen to take advantage of the vague language of §27.16 to manipulate its customers.

i. Verizon has stripped out features native to Android OS that do not impact their network

Native to Android is the ability to tether[2] as well as initiate SIP[3] data voice calls. Verizon has stripped out these features in the name of requiring users to pay Verizon for access to these features. This is a clear violation of §27.16(e). In the Commission's Report and Order of September 23, 2011 the Commission states that mobile broadband provides may not "block applications that compete with their voice or video telephony services." 76 FR 59192-01. If Verizon were to allow these features, they would compete directly with Verizon's services. SIP allows customers to place voice calls over their data line and bypass Verizon's wireless minutes. Moreover, Android's native ability to tether competes directly with Verizon's "wifi hotspot" feature, which is an additional $30.00 per month on top of the $30.00 per month minimum data package required for all smartphones. Verizon may argue that to allow Android users to freely

[2] Tether: A cellular device may act as a router and allow other wireless devices to connect to the cellular device over an ad hoc wifi network using the cellular device's cellular data to provide internet access.
[3] SIP: The **Session Initiation Protocol** (**SIP**) is an IETF-defined signaling protocol widely used for controlling communication sessions such as voice and video calls over Internet Protocol (IP). The protocol can be used for creating, modifying and terminating two-party (unicast) or multiparty (multicast) sessions. Sessions may consist of one or several media streams. http://en.wikipedia.org/wiki/Session_Initiation_Protocol

tether their devices could unduly burden Verizon's network to the extent that it interferes with reasonable network management. This argument must fail because Verizon ALLOWS this feature to those who are willing to pay for it. In order to provide a simple analogy, the idea of requiring users to pay for tethering is the same as if a fixed broadband provider required additional fees for a user to have multiple computers hooked up to a home router. It is well settled that internet service providers ("ISP") do not charge by the computer, nor do they limit the number of devices that can be connected to a local area network.

Verizon may also argue that they do not block SIP applications from being installed on devices. While this is true, the consequence of having to install third party applications, instead of that which is natively a part of the Android OS, is the user sacrifices ease of use, stability, security due to potential malicious programs being installed and battery life by having to use multiple programs to accomplish a singular task. Even if the commission were to find Verizon's argument sufficient, the bottom line is Verizon is violating the Report and Order of September 23, 2011 and C.F.R. §27.16 by stripping this feature out of Android because it is blocking features that directly compete with its provided services.

ii. Open bootloaders and root access do not interfere with Verizon's network management.

By denying consumers root access[4] to their devices, Verizon has disabled features of the device that may be integral to many users as well as disallowed consumers to fully access the

[4] In Unix-style computer operating systems, **root** is the conventional name of the user who has all rights or permissions (to all files and programs) in all modes (single- or multi-user). http://en.wikipedia.org/wiki/Superuser

device for which they paid. Verizon, through its original equipment manufacturer ("OEM") partners, has by default disabled root access leaving consumers with, what would be considered "guest" access if referring to a personal computer. Through root access a user is allowed to change aspects of the file system of the devices as well as allow programs to access certain features of the phone Verizon deems unnecessary for consumers to access, a benign example is an application used to sync the device's clock with the atomic clock. While this seems to be an innocuous usage of the capabilities of the phone, without root access it is not possible to do accurately and automatically.

Moreover, Verizon has installed programs into its devices that users are unable to remove. These programs are applications such as VZ Navigator, V CAST Tones, Verizon Video and many more. Each of these programs is installed on the device before the consumer purchases the device and through Verizon's policies, these programs (of which there are myriad free counterparts made by third party developers such as Google Maps) are unable to be removed as root access is required to remove these programs. Other than having programs on a device that the end user does not want and is unable to remove, these programs use system resources which causes the device to slow down or act in other undesirable ways and the user is left no viable alternative to solve this problem. This is tantamount to purchasing a personal computer from a company such as Dell, Sony, HP or the like and being unable to remove software that comes preloaded on the computer.

Further, by blocking root access users are unable to make system backups which allow a user to completely reflash a device with a known working backup in case there is some type of

software malfunction. These backups are known as nandroids and contain images of the radios, kernel, system, data and cache of the device that can be restored to the device should a user "brick" their device due to any number of issues that can occur.

iii. Allowing custom ROMs cannot impact Verizon's network

Custom ROMs are a standalone version of Android OS that have been customized by developers to include additional user interface features. Through an open bootloader custom ROMs can easily be flashed to a device with little risk of permanently "bricking" a device. Developers have created methods to hijack the boot process in order to flash custom ROMs but this method can be risky because it relies on the OEM to release system boot files ("SBF") or fast XML zips ("FXZ") in order to completely restore the device should the user unintentionally "brick" their device. Such files are typically not released by the companies and are usually obtained via leaked information and may not be reliable, providing no safety net that would otherwise be available but for Verizon's policies. Verizon's only statement regarding custom ROMS are they may lead to network connection problems. Verizon's argument fails for several reasons. Those who install a custom ROM do so with the understanding, or the implied understanding as it is expressly outlined when downloading and installing the ROM, that there may be issues with connectivity and operational problems as these are not official releases sanctioned by the OEM, Google or Verizon. Verizon would be in no way responsible for problems post-installation of a custom ROM as these are done with a certain risk to the end user. This risk is limited to the specific user and can in no way affect Verizon's customers as Verizon

has led this Commission to believe when it stated "unapproved software could also negatively impact the wireless experience for other customers."

Custom ROMs allow users to customize their device as they see fit. The user accepts the responsibility of the outcome of customization through a third party developer. However, as discussed in romanette ii above, were Verizon to unlock the bootloader, users can easily create backup images of their device should a custom ROM cause the device to malfunction. Therefore, Verizon does not have to accept responsibility should a user "brick" their device as a backup can easily be restored.

Lastly, Verizon's policy of disallowing a consumer to load a custom ROM is the equivalent of disallowing a consumer who purchases a personal computer to load the operating system of their choosing. This is an untenable position and cannot be tolerated by this Commission. ISPs do not require any specific programs to be installed or any specific operating systems to be used in order to maintain network access. As this Commission has adopted rules for mobile broadband providers that largely mirror fixed broadband providers, the Commission must disallow Verizon's monopolistic views of what ROM may be used to access their network.

iv. Open bootloaders have not negatively impacted or affected Verizon's network or network management

Verizon has had several devices which have had open bootloaders, these devices include the original Motorola Droid, the Motorola Xoom and every variant of the Samsung Galaxy series including the upcoming Samsung Galaxy Nexus. With the exception of the Galaxy Nexus,

which has yet to be released, all the above listed devices have open bootloaders and have not negatively impacted Verizon's network. While it cannot be conclusively proven this is the case, it can be inferred from the fact that if the open bootloaders were interfering with Verizon's network management they can easily create an over-the-air update that could lock the bootloaders. The fact that Verizon has not done this since the release of the original Motorola Droid, October 17, 2009, shows beyond a doubt that open bootloaders do not impact, nor negatively affect, Verizon's network or its ability to manage its network.

II. VERIZON HAS FAILED TO CARRY ITS BURDEN WHEN CONFRONTED WITH ALLEGATIONS OF C BLOCK VIOLATIONS

"Once a complainant sets forth a *prima facie* case that the C Block licensee has refused to attach a device or application in violation of the requirements adopted in this section, the licensee shall have the burden of proof to demonstrate that it has adopted reasonable network standards and reasonably applied those standards in the complainant's case. Where the licensee bases its network restrictions on industry-wide consensus standards, such restrictions would be presumed reasonable." 47 C.F.R. §27.16(f). After countless complaints against it, Verizon has yet to demonstrate it has adopted and applied reasonable network standards. Verizon instead, chooses to insult its customers and this Commission by stating vague generalities such as "an open bootloader could prevent Verizon Wireless from providing the same level of customer experience and support because it would allow users to change the phone or otherwise modify the software and, potentially, negatively impact how the phone connects to the network." Verizon fails to cite

ONE specific example of how an open bootloader or root access would negatively impact the wireless experience of other customers or impact network connectivity. Even if Verizon were to offer reasons, the solutions presented above more than resolve the potential issues Verizon may cite.

Finally, Verizon may try to rely on the last clause of §27.16(f) in defense that it has adopted and applied reasonable network standards that have an industry wide consensus. Yet this exculpatory clause remains suspiciously absent from Verizon's response. This is because it is evident that the policy of locked bootloaders does NOT have an industry wide consensus. One only has to look at T-Mobile and see the fact that Google has release two Nexus devices, the Nexus One and the Nexus S, on T-Mobile's network. These devices are specifically referred to because they are known to have open bootloaders.

CONCLUSION

WHEREFORE, based on the foregoing it is respectfully requested that this Commission find Verizon Wireless to have violated the requirements of Block C as codified in the Code Federal Regulations at §27.16. Further, the Commission is respectfully requested to require Verizon Wireless to allow its bootloaders to be unlocked, allow root access to its devices and any other remedy this Commission deems necessary and proper.

Respectfully submitted,

Complainant

To: Federal Communications Commission

Consumer Inquires and Complaints Division

Consumer & Governmental Affairs Bureau

445 12th Street, SW

Washington, DC 20554

Fax: 1-866-418-0232