

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Gary

Last Name: Starkweather

Mailing Address: 1377 Tatlo Rd.

City: Crofton

Country: Canada

State or Province: British Columbia

ZIP/Postal Code: V0R 1R0

Email Address: GStark@rustycat.com

Organization Name: RustyCat

Comment: This seems like shooting yourself (or the rest of us anyway) in the foot.

How will we fix security holes or bugs in the firmware of our WiFi devices?

Why would you disallow security updates?

It makes no sense.

I am an American but living in my wife's hometown in BC Canada for now.

This seems like shooting yourself (or the rest of us anyway) in the foot.

How will we fix security holes or bugs in the firmware of our WiFi devices?

Why would you disallow security updates?

It makes no sense.

I am an American but living in my wife's hometown in BC Canada for now.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Christine

Last Name: Wilinsky

Mailing Address: P.O. Box 3612

City: Laguna Hills

Country: United States

State or Province: CA

ZIP/Postal Code: 92654

Email Address: asksqn@gmail.com

Organization Name: self

Comment: Please see attached

Please see attached

To Whom It May Concern:

Although I believe that the Federal Communications Commission (Hereinafter referred to as "commission") has the best of intentions, I also believe that the NPRM is a dangerous intrusion upon the rights of computing users and substantially interferes with innovation in the wireless space.

I am are concerned about three changes in the NPRM:

- § 2.1033 Application for grant of certification. Paragraph 4(i),
- § 2.935 Electronic labeling of radiofrequency devices. Clause (d) and
- § 2.1042 Certified modular transmitters. Section 8(e)

The NPRM removes the ability of computing users to control and modify their devices in both Paragraph 4(i). In Paragraph 4(i), the manufacturer is required to describe how the software of the device is secured against modification. Additionally, Clause (d) implies that the device must be secured against modification due to the requirement to prevent label information from being modified. Finally, Section 8(e) requires manufacturers to only allow "approved" software to be installed on a device. These requirements combined prevent most modifications to the device even when the user wants to improve on the security of the device or even to correct problems with the wireless radio software itself.

Infringing upon computing users rights

Until now, users of computing devices have had the ability to install the software of their choice. In particular, users have had the ability to install free and open source operating systems and software which most appropriately fits their needs. Whether the user wants to install OpenWrt on a router or a distribution based upon the Linux kernel on their laptop computer or smartphone, users have been able to control the devices they own. Through this control, users can explore how their computing devices work, educate themselves on the design of hardware, protect themselves from invasive spying by competitors and foreign governments and enrich their own lives and the lives of others through improved software.

Interfering with innovation in the wireless space

Innovation in network and wireless technology depends on the ability of users and resellers to experiment with software and hardware at the deepest levels. CeroWrt, an open source router firmware, developed a fix for an important form of network congestion called Bufferbloat. This fix is was added to the Linux kernel to be used by the billions of users of Linux.

Mesh networking technologies for developing stable distributed internet access are regularly implemented using various versions of Linux installed by an end-user and much research and implementation on mesh networking has occurred outside of manufacturers. Nearly 7,200 scholarly articles on wireless networking technologies reference a particular brand of open and modifiable hardware which would be banned under these rules. Mesh networking is used for data communication by amateur radio operators responding to natural disasters. Without the ability to change the software on the device, these innovations would not have occurred.

User-access to source code is another innovation in and of itself. It has led to bug fixes, security enhancements, and features that were not part of the original code base. In one instance a user was able to fix a critical bug impacting all wifi adapters based on a particular set of Qualcomm Atheros wireless chipset(s). As users were frequently being disconnected under certain conditions one user took it upon

themselves to track down and fix the bug [1]. This would not have been possible had the source code for the firmware been unavailable, or had these devices otherwise been locked.

Finally, numerous companies modify the software on off-the-shelf wireless devices for custom uses. Companies who sell hardware to retailers for WiFi hotspots often install software customized to that task. Additionally many commercial VPN providers sell wireless routers as part of their product offerings. Denying companies and users the option to purchase more secure routers with support for VPN services will put a variety of users at risk.

Recommendations

I respectfully recommend the following changes:

The regulations on software defined radios should not restrict the ability to replace software on computing devices

As written, the regulations require that manufacturers prevent modification of all software computing devices which use software defined radios. The Commission should amend the regulations in a manner which protects the traditional right of law abiding users to understand and improve the software on their devices.

The regulations on e-labels should not restrict the ability to replace software on computing devices

I appreciate the need for proper labeling of wireless devices and the requirements set by Congress in the E-Label Act. The Commission should amend the regulations to guarantee electronic labels do not interfere with the ability of downstream parties to install any software they so choose.

Conclusion

I share the commission's interest in protecting the wireless spectrum. As the Commission deliberates on the NPRM, we invite the Commission to meet with signers, the computing industry, users, free and open source software advocates and all interested parties. Through a collaboration we believe the wireless spectrum can be protected while enabling the innovation and freedom key to American competitiveness in the 21st century.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Brendan

Last Name: White

Mailing Address: 2121 Spaulding Ave

City: Berkeley

Country: United States

State or Province: CA

ZIP/Postal Code: 94703

Email Address:

Organization Name:

Comment: Please do not implement rules that will take away my ability to install the software of my choice on my wireless routers. Specifically:

- i depend on this ability to debug, test, and fix wireless hardware
- i need a way to modify the system for security patches once the vendor has stopped supporting
- i have many times in the past needed to update wifi drivers to get around buggy manufacturers versions
- i have designed and deployed local mesh networks for community building, that are not possible without modified firmwares

As a software and network engineer, the proposed changes would be disastrous for the open source networking community. Projects like openWRT are the public's only way to fully utilize the hardware they've paid for.

Please do not implement rules that will take away my ability to install the software of my choice on my wireless routers. Specifically:

- i depend on this ability to debug, test, and fix wireless hardware
- i need a way to modify the system for security patches once the vendor has stopped supporting
- i have many times in the past needed to update wifi drivers to get around buggy manufacturers versions
- i have designed and deployed local mesh networks for community building, that are not possible without modified firmwares

As a software and network engineer, the proposed changes would be disastrous for the open source networking community. Projects like openWRT are the public's only way to fully utilize the hardware they've paid for.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: John

Last Name: Kinsella

Mailing Address: 400 Beale St, #1401

City: San Francisco

Country: United States

State or Province: CA

ZIP/Postal Code: 94105

Email Address: jlkinsel@gmail.com

Organization Name:

Comment: Please do not implement rules that removes my ability to install software of my choosing on my wifi devices.

As a computer security professional, being able to install and configure custom software on my wifi devices allows me to test and ensure the wifi security of my customers. Wireless networking research depends on the ability of researchers to investigate and modify their devices.

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.

Please do not implement rules that removes my ability to install software of my choosing on my wifi devices.

As a computer security professional, being able to install and configure custom software on my wifi devices allows me to test and ensure the wifi security of my customers. Wireless networking research depends on the ability of researchers to investigate and modify their devices.

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Andrew

Last Name: Bezella

Mailing Address: 160 BEULAH ST APT A

City: SAN FRANCISCO

Country: United States

State or Province: CA

ZIP/Postal Code: 94117

Email Address: dovienea@yahoo.com

Organization Name: null

Comment: Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

- \* Wireless networking research depends on the ability of researchers to investigate and modify their devices.
- \* Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
- \* Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
- \* Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

- \* Wireless networking research depends on the ability of researchers to investigate and modify their devices.
- \* Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
- \* Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
- \* Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Christine

Last Name: Wilinsky

Mailing Address: P.O. Box 3612

City: Laguna Hills

Country: United States

State or Province: CA

ZIP/Postal Code: 92654

Email Address: asksqn@gmail.com

Organization Name: [Self]

Comment: Please see attached comment.

Please see attached comment.

To Whom It May Concern:

Although I believe that the Federal Communications Commission (Hereinafter referred to as "commission") has the best of intentions, I also believe that the NPRM is a dangerous intrusion upon the rights of computing users and substantially interferes with innovation in the wireless space.

I am are concerned about three changes in the NPRM:

- § 2.1033 Application for grant of certification. Paragraph 4(i),
- § 2.935 Electronic labeling of radiofrequency devices. Clause (d) and
- § 2.1042 Certified modular transmitters. Section 8(e)

The NPRM removes the ability of computing users to control and modify their devices in both Paragraph 4(i). In Paragraph 4(i), the manufacturer is required to describe how the software of the device is secured against modification. Additionally, Clause (d) implies that the device must be secured against modification due to the requirement to prevent label information from being modified. Finally, Section 8(e) requires manufacturers to only allow "approved" software to be installed on a device. These requirements combined prevent most modifications to the device even when the user wants to improve on the security of the device or even to correct problems with the wireless radio software itself.

Infringing upon computing users rights

Until now, users of computing devices have had the ability to install the software of their choice. In particular, users have had the ability to install free and open source operating systems and software which most appropriately fits their needs. Whether the user wants to install OpenWrt on a router or a distribution based upon the Linux kernel on their laptop computer or smartphone, users have been able to control the devices they own. Through this control, users can explore how their computing devices work, educate themselves on the design of hardware, protect themselves from invasive spying by competitors and foreign governments and enrich their own lives and the lives of others through improved software.

Interfering with innovation in the wireless space

Innovation in network and wireless technology depends on the ability of users and resellers to experiment with software and hardware at the deepest levels. CeroWrt, an open source router firmware, developed a fix for an important form of network congestion called Bufferbloat. This fix is was added to the Linux kernel to be used by the billions of users of Linux.

Mesh networking technologies for developing stable distributed internet access are regularly implemented using various versions of Linux installed by an end-user and much research and implementation on mesh networking has occurred outside of manufacturers. Nearly 7,200 scholarly articles on wireless networking technologies reference a particular brand of open and modifiable hardware which would be banned under these rules. Mesh networking is used for data communication by amateur radio operators responding to natural disasters. Without the ability to change the software on the device, these innovations would not have occurred.

User-access to source code is another innovation in and of itself. It has led to bug fixes, security enhancements, and features that were not part of the original code base. In one instance a user was able to fix a critical bug impacting all wifi adapters based on a particular set of Qualcomm Atheros wireless chipset(s). As users were frequently being disconnected under certain conditions one user took it upon

themselves to track down and fix the bug [1]. This would not have been possible had the source code for the firmware been unavailable, or had these devices otherwise been locked.

Finally, numerous companies modify the software on off-the-shelf wireless devices for custom uses. Companies who sell hardware to retailers for WiFi hotspots often install software customized to that task. Additionally many commercial VPN providers sell wireless routers as part of their product offerings. Denying companies and users the option to purchase more secure routers with support for VPN services will put a variety of users at risk.

Recommendations

I respectfully recommend the following changes:

The regulations on software defined radios should not restrict the ability to replace software on computing devices

As written, the regulations require that manufacturers prevent modification of all software computing devices which use software defined radios. The Commission should amend the regulations in a manner which protects the traditional right of law abiding users to understand and improve the software on their devices.

The regulations on e-labels should not restrict the ability to replace software on computing devices

I appreciate the need for proper labeling of wireless devices and the requirements set by Congress in the E-Label Act. The Commission should amend the regulations to guarantee electronic labels do not interfere with the ability of downstream parties to install any software they so choose.

Conclusion

I share the commission's interest in protecting the wireless spectrum. As the Commission deliberates on the NPRM, we invite the Commission to meet with signers, the computing industry, users, free and open source software advocates and all interested parties. Through a collaboration we believe the wireless spectrum can be protected while enabling the innovation and freedom key to American competitiveness in the 21st century.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Kyle

Last Name: Jones

Mailing Address: 900 SW St Clair Street

City: Portland

Country: United States

State or Province: OR

ZIP/Postal Code: 97205

Email Address:

Organization Name:

Comment: I believe it is foolish to put a software limitation, firmware or otherwise, on an electronic device purchased by a consumer. Investigating and prosecuting those who utilize said act to commit a crime is one thing, but completely outlawing code creates walled gardens unfair to the owners of said devices and will encourage manufacturers to lock out features for a price. Promote firmware and tinkering! We will find more problems in our foundations that way.

I believe it is foolish to put a software limitation, firmware or otherwise, on an electronic device purchased by a consumer. Investigating and prosecuting those who utilize said act to commit a crime is one thing, but completely outlawing code creates walled gardens unfair to the owners of said devices and will encourage manufacturers to lock out features for a price. Promote firmware and tinkering! We will find more problems in our foundations that way.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Simone

Last Name: Sold

Mailing Address: Via Morandi 8/A

City: Uboldo

Country: Italy

State or Province: VA

ZIP/Postal Code: 21040

Email Address: simone.solda@gmail.com

Organization Name:

Comment: I ask the FCC to refrain from implementing such measures on restricting the modification of U-NII devices. It will hamper security, commerce, and innovation.

\* Manufacturers are known for their terrible record in providing security fixes, most of the devices involved are \*never\* updated during their lifetime, instead preferring to just ignore current devices and iterate on a new product. This has come to its ultimate consequences recently, when a software bug affecting a \*billion\* of smartphones has been discovered and wont be fixed for almost all of the affected devices. 3rd-party firmwares are the only safeguard against this kind of situations: manufactures are not and cannot be forced to provide security fixes.

\* Without the ability to modify the software running on these devices, nothing more than the very limited, more lucrative use cases addressed by the manufacturer would be implemented. This leaves behind advanced and/or custom scenarios which businesses could integrate on their services/products with very small costs by replacing the software.

\* Research and innovation in wireless communications, ranging from entirely new designs, models and protocols to software implementations, would basically come to an halt, severely harmed by the unavailability of low-cost, readily-available solutions upon which to experiment. Community Mesh Networks are entirely reliant on the ability to customize low-cost networking equipment.

\* These rules are overreaching and not even helping in ensuring compliance. Virtually none of the FCC rule breaches is due to 3rd-party software modification. It is however \*still\* possible to trivially enable non-compliant modes on unmodified devices on major wireless equipment manufactures.

Thanks for listening.

I ask the FCC to refrain from implementing such measures on restricting the modification of U-NII devices. It will hamper security, commerce, and innovation.

\* Manufacturers are known for their terrible record in providing security fixes, most of the devices involved are \*never\* updated during their lifetime, instead preferring to just ignore current devices and iterate on a new product. This has come to its ultimate consequences recently, when a software bug affecting a \*billion\* of smartphones has been discovered and wont be fixed for almost all of the affected devices. 3rd-party firmwares are the only safeguard against this kind of situations: manufactures are not and cannot be forced to provide security fixes.

\* Without the ability to modify the software running on these devices, nothing more than the very limited, more lucrative use cases addressed by the manufacturer would be implemented. This leaves behind advanced and/or custom scenarios which businesses could integrate on their services/products with very small costs by replacing the software.

\* Research and innovation in wireless communications, ranging from entirely new designs, models and protocols to software implementations, would basically come to an halt, severely harmed by the unavailability of low-cost, readily-available solutions upon which to experiment. Community Mesh Networks are entirely reliant on the ability to customize low-cost networking equipment.

\* These rules are overreaching and not even helping in ensuring compliance. Virtually none of the FCC rule breaches is due to 3rd-party software modification. It is however *\*still\** possible to trivially enable non-compliant modes on unmodified devices on major wireless equipment manufactures.

Thanks for listening.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Vic

Last Name: Simone

Mailing Address: PO Box 881

City: Lansdale

Country: United States

State or Province: PA

ZIP/Postal Code: 19446

Email Address:

Organization Name:

Comment:

I am writing to request the FCC not implement rules which would prevent end users from installing or updating firmware on their devices which contain a "modular wireless radio".

Preventing end users from upgrading or installing software of their choosing will decreasing security by preventing every day users from fixing security problems. Additionally, it will hinder software development, technological progress and even make it impossible for some business to continue operation.

In conclusion I am asking the FCC to not implement rules laid out in the proposed document labeled "Equipment Authorization and Electronic Labeling for Wireless Devices" on 08/16/2015.

I am writing to request the FCC not implement rules which would prevent end users from installing or updating firmware on their devices which contain a "modular wireless radio".

Preventing end users from upgrading or installing software of their choosing will decreasing security by preventing every day users from fixing security problems. Additionally, it will hinder software development, technological progress and even make it impossible for some business to continue operation.

In conclusion I am asking the FCC to not implement rules laid out in the proposed document labeled "Equipment Authorization and Electronic Labeling for Wireless Devices" on 08/16/2015.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Jason

Last Name: Gallegos

Mailing Address: 1523 Pleasant Ave

City: Los Angeles

Country: United States

State or Province: CA

ZIP/Postal Code: 90033

Email Address: abstrak@gmail.com

Organization Name:

Comment: What you are proposing makes no sense

What you are proposing makes no sense

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Kenneth

Last Name: Thieme

Mailing Address: 8207 Olde Village Dr.

City: San Antonio

Country: United States

State or Province: TX

ZIP/Postal Code: 78250

Email Address: ken@goobsoft.com

Organization Name:

Comment: Due to the how wireless routers/access points operate this proposed rule will make illegal the modification of a wireless device's firmware. I currently operate two older wireless access points that run OpenWRT firmware. If this rule passes, I will have to throw these devices away or be branded a criminal. Beside the ridiculous fact of potentially turning thousands of currently law-abiding U.S. citizens into criminals overnight, the ability to choose the firmware/code that operates my devices (so long as they do not violate current rules concerning radio transmissions) should be a basic right. While you may be able to reduce incidents of illegal modifications to wireless device radio transmissions by making firmware modifications illegal, in the process you will be drastically reducing the functionality of these devices, increasing costs to manufacturers, taking away our ability as consumers to legally modify devices we own and, as mentioned previously, making many of us criminals.

For these reasons I implore you to not implement this rule that would make firmware modification of wireless devices illegal.

Thank you,  
Kenneth Thieme

Due to the how wireless routers/access points operate this proposed rule will make illegal the modification of a wireless device's firmware. I currently operate two older wireless access points that run OpenWRT firmware. If this rule passes, I will have to throw these devices away or be branded a criminal. Beside the ridiculous fact of potentially turning thousands of currently law-abiding U.S. citizens into criminals overnight, the ability to choose the firmware/code that operates my devices (so long as they do not violate current rules concerning radio transmissions) should be a basic right. While you may be able to reduce incidents of illegal modifications to wireless device radio transmissions by making firmware modifications illegal, in the process you will be drastically reducing the functionality of these devices, increasing costs to manufacturers, taking away our ability as consumers to legally modify devices we own and, as mentioned previously, making many of us criminals.

For these reasons I implore you to not implement this rule that would make firmware modification of wireless devices illegal.

Thank you,  
Kenneth Thieme

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Steve

Last Name: Willson

Mailing Address: 100 Yeager Ave Apt B

City: Fort Benning

Country: United States

State or Province: GA

ZIP/Postal Code: 31905

Email Address: steve@colorado.edu

Organization Name:

Comment: I am a Electronic Hobbyist and would like the FCC to allow modification of hardware for private use.

I am a Electronic Hobbyist and would like the FCC to allow modification of hardware for private use.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: John

Last Name: Medema

Mailing Address: 11842 N 32nd Pl

City: Phoenix

Country: United States

State or Province: AZ

ZIP/Postal Code: 85028

Email Address: jmedema@gmail.com

Organization Name:

Comment: As a personal computer/wifi user, I am against this proposal. Specifically 2.1042 section (8)(e) and and 2.935 section (d). While I can understand the FCC's desire to stop people from misusing the spectrum, this DRM solution is far too restrictive and usually ineffective.

I often need the ability to diagnose my wifi signal by using various apps on my android phone. This would not be possible with future phones that are locked down by my phone manufacturer. In addition, I also have rooted & flashed my phone in order to fully utilized the hardware I had legally purchased. I often want my phone to be on the most current kernel possible for security purposes, and phone manufacturers have only just recently started pushing out OS security updates on a regular basis - far too infrequent to truly be considered secure. These proposed restrictions will cost me significantly for no practical gain.

As a personal computer/wifi user, I am against this proposal. Specifically 2.1042 section (8)(e) and and 2.935 section (d). While I can understand the FCC's desire to stop people from misusing the spectrum, this DRM solution is far too restrictive and usually ineffective.

I often need the ability to diagnose my wifi signal by using various apps on my android phone. This would not be possible with future phones that are locked down by my phone manufacturer. In addition, I also have rooted & flashed my phone in order to fully utilized the hardware I had legally purchased. I often want my phone to be on the most current kernel possible for security purposes, and phone manufacturers have only just recently started pushing out OS security updates on a regular basis - far too infrequent to truly be considered secure. These proposed restrictions will cost me significantly for no practical gain.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: John

Last Name: Medema

Mailing Address: 11842 N 32nd Pl

City: Phoenix

Country: United States

State or Province: AZ

ZIP/Postal Code: 85028

Email Address: jmedema@gmail.com

Organization Name:

Comment: As a personal computer/wifi user, I am against this proposal. Specifically 2.1042 section (8)(e) and and 2.935 section (d). While I can understand the FCC's desire to stop people from misusing the spectrum, this DRM solution is far too restrictive and usually ineffective.

I often need the ability to diagnose my wifi signal by using various apps on my android phone. This would not be possible with future phones that are locked down by my phone manufacturer. In addition, I also have rooted & flashed my phone in order to fully utilized the hardware I had legally purchased. I often want my phone to be on the most current kernel possible for security purposes, and phone manufacturers have only just recently started pushing out OS security updates on a regular basis - far too infrequent to truly be considered secure. These proposed restrictions will cost me significantly for no practical gain.

As a personal computer/wifi user, I am against this proposal. Specifically 2.1042 section (8)(e) and and 2.935 section (d). While I can understand the FCC's desire to stop people from misusing the spectrum, this DRM solution is far too restrictive and usually ineffective.

I often need the ability to diagnose my wifi signal by using various apps on my android phone. This would not be possible with future phones that are locked down by my phone manufacturer. In addition, I also have rooted & flashed my phone in order to fully utilized the hardware I had legally purchased. I often want my phone to be on the most current kernel possible for security purposes, and phone manufacturers have only just recently started pushing out OS security updates on a regular basis - far too infrequent to truly be considered secure. These proposed restrictions will cost me significantly for no practical gain.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Glenn

Last Name: Wallace

Mailing Address: 24854 Woodmont Way

City: Athens

Country: United States

State or Province: AL

ZIP/Postal Code: 35613-7208

Email Address:

Organization Name:

Comment: There should be no rules promulgated which preclude the ability of wifi router owners to modify the firmware in their own equipment. The use of open source software by consumers to modify and enhance manufacturer-installed firmware in routers is a common practice and the ability to do so should not be limited.

There should be no rules promulgated which preclude the ability of wifi router owners to modify the firmware in their own equipment. The use of open source software by consumers to modify and enhance manufacturer-installed firmware in routers is a common practice and the ability to do so should not be limited.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Michael

Last Name: Henshaw

Mailing Address: 2302 Lakeshore Dr.

City: Sheboygan

Country: United States

State or Province: WI

ZIP/Postal Code: 53081

Email Address:

Organization Name:

Comment: Fair Use and innovation will be denied to the public if this policy is enacted.

I personally use a WIFI device that is running customized open sourced firmware not being supplied or supported by the original manufactor. My reasoning is simple. The firmware deployed by the manufactor lacks a number of features and is dramatically of poorer quality with user interface design, packet processing, utilization of resources, and possibility of usable features.

These are just some of the custom features the custom open source firmware allows for. 1) Custom firmware allow allowing the dual radio device as being a WIFI WAN connection while also allowing the other radio as a WIFI LAN connection. 2) State-Full packet inspection firewall. 3) Built in anti-virus packet scanning at WAN level connection. 4) Responsive and fluid user interface 5) Configuration backups are applicable between different brands of devices with the standardization of the open source firmware. 6) Improved CPU processing of packets allowing for more throughput.

This would hinder technology by; 1) Prevent improving abandoned products or products from defunct companies. 2) Fixing security issues that companies do not deem risky based on cost benefit analysis; back-doors, embedded passwords, buffer-over or buffer-under flows, individual personal marks (privacy). 3) Prevent creation of new solutions using off-the-self products. 4) Turn public domain frequencies into a commercially licensed frequencies. 5) Turn hobbyists, such as myself, and inventors into criminals.

Ones own the hardware, why can't they choose which software it runs? The policy would be equivalent of not allowing the choice of Operating System on a Desktop PC, Notebook, Tablet, or Smart Phone. Public should have the right of choose not the force of use.

In the end, the only difference between a SoC with a 5GHz WIFI radio and a USB or PCI connected 5GHz WIFI radio with a non-SoC processor or a fully embedded solution is physical connection and style of BUS connector. Fair Use should not depended on the style of BUS connector and PCB traces.

Fair Use and innovation will be denied to the public if this policy is enacted.

I personally use a WIFI device that is running customized open sourced firmware not being supplied or supported by the original manufactor. My reasoning is simple. The firmware deployed by the manufactor lacks a number of features and is dramatically of poorer quality with user interface design, packet processing, utilization of resources, and possibility of usable features.

These are just some of the custom features the custom open source firmware allows for. 1) Custom firmware allow allowing the dual radio device as being a WIFI WAN connection while also allowing the other radio as a WIFI LAN connection. 2) State-Full packet inspection firewall. 3) Built in anti-virus packet scanning at WAN level connection. 4) Responsive and fluid user interface 5) Configuration backups are applicable between different brands of devices with the standardization of the open source firmware. 6) Improved CPU processing of packets allowing for more throughput.

This would hinder technology by; 1) Prevent improving abandoned products or products from defunct companies. 2) Fixing security issues that companies do not deem risky based on cost benefit analysis; back-doors, embedded passwords, buffer-over or buffer-under flows, individual personal marks (privacy). 3) Prevent creation of new solutions using off-the-self products. 4) Turn public domain frequencies into a commercially licensed frequencies. 5) Turn hobbyists, such as myself, and inventors into criminals.

Ones own the hardware, why can't they choose which software it runs? The policy would be equivalent of not allowing the choice of Operating System on a Desktop PC, Notebook, Tablet, or Smart Phone. Public should have the right of choose not the force of use.

In the end, the only difference between a SoC with a 5GHz WIFI radio and a USB or PCI connected 5GHz WIFI radio with a non-SoC processor or a fully embedded solution is physical connection and style of BUS connector. Fair Use should not depended on the style of BUS connector and PCB traces.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Jm

Last Name: Casler

Mailing Address: 495 HARKNESS AVE

City: SAN FRANCISCO

Country: United States

State or Province: CA

ZIP/Postal Code: 94134

Email Address: jm@casler.org

Organization Name:

Comment: To whom this may concern,

My name is Jm Casler and as an artist who works in the 5ghz band to coordinate my art, this proposed rule will immediately stop much of the capabilities I now enjoy.

Please take this as a conscious objection toward this rule.

Thank you.

- Jm Casler

To whom this may concern,

My name is Jm Casler and as an artist who works in the 5ghz band to coordinate my art, this proposed rule will immediately stop much of the capabilities I now enjoy.

Please take this as a conscious objection toward this rule.

Thank you.

- Jm Casler

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Jonathan

Last Name: Conley

Mailing Address: 3700 kristi lake drive apt d 2

City: Jonesboro

Country: United States

State or Province: AR

ZIP/Postal Code: 72404

Email Address: cscodemaster@gmail.com

Organization Name:

Comment: Respectfully,

It has come to my attention there is a proposed rule in this that would make it illegal to change the Operating system on my Pc, the Operating system on my Smartphone or the firmware of my wireless router and/or wireless access point.

Many times the software running on these pieces of hardware (PC, Smartphone, Router, and/or Wireless Access point) needs to be changed out over time for reasons of usability, security, and or personal choice.

Here is an example;

WPA2 wireless encryption has become broken and is no longer suitable to secure wireless communications. The certified manufacturer of my router will not release a firmware patch that has an updated encryption protocol as the device is old and they do not wish to support it. And updated build of OpenWRT (third party firmware) does but it is illegal to fix the issue because of this FCC rule.

Respectfully,

It has come to my attention there is a proposed rule in this that would make it illegal to change the Operating system on my Pc, the Operating system on my Smartphone or the firmware of my wireless router and/or wireless access point.

Many times the software running on these pieces of hardware (PC, Smartphone, Router, and/or Wireless Access point) needs to be changed out over time for reasons of usability, security, and or personal choice.

Here is an example;

WPA2 wireless encryption has become broken and is no longer suitable to secure wireless communications. The certified manufacturer of my router will not release a firmware patch that has an updated encryption protocol as the device is old and they do not wish to support it. And updated build of OpenWRT (third party firmware) does but it is illegal to fix the issue because of this FCC rule.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Matthew

Last Name: von Arx

Mailing Address: 111 Wilderness Trail

City: Candler

Country: United States

State or Province: NC

ZIP/Postal Code: 28715

Email Address:

Organization Name:

Comment: Please do not implement rules taking away the ability for users to install custom software on computing devices whose related hardware is owned by the user. I personally install custom software/firmware on many of my devices in order to extend functionality and/or fix issues. If there is concern for out of band transmission, the onus should be on lower level transmission components utilized in these devices, and not on the software. Also, if the concern is for out of band, or unregulated transmission from these devices, I can assure you that 99+% of users who modify such hardware continue to use it (at least in regards to the transmission capability) precisely as the manufacturer intended. Please take time to carefully consider these points, and others from this comment submission.

Thank you

Please do not implement rules taking away the ability for users to install custom software on computing devices whose related hardware is owned by the user. I personally install custom software/firmware on many of my devices in order to extend functionality and/or fix issues. If there is concern for out of band transmission, the onus should be on lower level transmission components utilized in these devices, and not on the software. Also, if the concern is for out of band, or unregulated transmission from these devices, I can assure you that 99+% of users who modify such hardware continue to use it (at least in regards to the transmission capability) precisely as the manufacturer intended. Please take time to carefully consider these points, and others from this comment submission.

Thank you

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Richard

Last Name: Burgan

Mailing Address: 3946 Ravenwood Dr

City: Hilliard

Country: United States

State or Province: OH

ZIP/Postal Code: 43026

Email Address: rdburgan@gmail.com

Organization Name:

Comment: Commissioners:

I am specifically concerned about the proposed changes in this docket that will effectively prohibit firmware changes to 5GHz WiFi radios. These devices are low power short range devices. It is not likely that any changes to firmware would affect very many others. There is great benefit in allowing changes to firmware after manufacture. Problems can be fixed post manufacture and upgrades can add features and correct for unforeseen circumstances. It is especially important that security related patches be allowed.

Rather than prohibiting changes to prevent a device from exceeding limits or behaviors as described prior to manufacture. Why not clearly describe the limits and behaviors and require changes to stay within those limits.

Thank you.

Commissioners:

I am specifically concerned about the proposed changes in this docket that will effectively prohibit firmware changes to 5GHz WiFi radios. These devices are low power short range devices. It is not likely that any changes to firmware would affect very many others. There is great benefit in allowing changes to firmware after manufacture. Problems can be fixed post manufacture and upgrades can add features and correct for unforeseen circumstances. It is especially important that security related patches be allowed.

Rather than prohibiting changes to prevent a device from exceeding limits or behaviors as described prior to manufacture. Why not clearly describe the limits and behaviors and require changes to stay within those limits.

Thank you.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Blaise

Last Name: Friery

Mailing Address: 27463 Gateway Dr N apt 208

City: Farmington Hills

Country: United States

State or Province: MI

ZIP/Postal Code: 48334

Email Address:

Organization Name:

Comment: To whom it may concern:

I respectfully request that the FCC Not implement the rules put forth in this document. As a consumer, a user, and a developer, the ability to install software and firmware on devices that I own is important. Below is a list of 4 reasons why:

1. Wireless networking research depends on the ability of researchers to investigate and modify their devices.
2. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
3. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
4. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

Thank you for listening,

Blaise Friery

To whom it may concern:

I respectfully request that the FCC Not implement the rules put forth in this document. As a consumer, a user, and a developer, the ability to install software and firmware on devices that I own is important. Below is a list of 4 reasons why:

1. Wireless networking research depends on the ability of researchers to investigate and modify their devices.
2. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
3. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
4. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

Thank you for listening,

Blaise Friery

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Gaby

Last Name: Schilders

Mailing Address: toon hermanslaan 27

City: beverwijk

Country: Netherlands

State or Province: Noord-Holland

ZIP/Postal Code: 1948 ac

Email Address: Gaby.schilders@gmail

Organization Name:

Comment: You will take my OpenWRT from my cold, dead hands.

More formally: I will disregard any artificial limitations you choose to set on my liberty to run code on equipment I hold in ownership. I will however, respect all rules and regulations set forth to ensure the usability of the radio spectrum, as long as it does not contravene my stated rights.

You will take my OpenWRT from my cold, dead hands.

More formally: I will disregard any artificial limitations you choose to set on my liberty to run code on equipment I hold in ownership. I will however, respect all rules and regulations set forth to ensure the usability of the radio spectrum, as long as it does not contravene my stated rights.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Lonny

Last Name: Eachus

Mailing Address: 1602 E Sprague Ave

City: Spokane

Country: United States

State or Province: WA

ZIP/Postal Code: 99220

Email Address:

Organization Name:

Comment: This is a very bad idea, and will stifle innovation in the United States.

Current technology allows firmware to be updated for many reasons: to fix bugs, to add features, and even to add capabilities that were not there when the device was manufactured.

An old example comes to mind: modems built around draft standards that could be firmware-upgraded once the standard was finalized.

That kind of technology is a great boon to consumers. Your proposal, on the other hand, would slow adoption of new technology even if for no other reason that an "upgrade" would require a completely new purchase.

Granted, router manufacturers are obligated to place a greater emphasis on security than they have in the past, but that doesn't justify this huge overreach on the part of the FCC.

You would also "lock in" firmware bugs, forcing consumers to purchase a replacement or cause the manufacturer a great deal by means of a recall, when the problem could have been fixed with a firmware update.

It's just a bad idea all around. Costly for consumers and industry, with little real benefit to anybody.

Rather than making the practice illegal, I suggest putting in place a formal complaint process so that people can notify of abuses, much as you do with other kinds of radio today.

This is a very bad idea, and will stifle innovation in the United States.

Current technology allows firmware to be updated for many reasons: to fix bugs, to add features, and even to add capabilities that were not there when the device was manufactured.

An old example comes to mind: modems built around draft standards that could be firmware-upgraded once the standard was finalized.

That kind of technology is a great boon to consumers. Your proposal, on the other hand, would slow adoption of new technology even if for no other reason that an "upgrade" would require a completely new purchase.

Granted, router manufacturers are obligated to place a greater emphasis on security than they have in the past, but that doesn't justify this huge overreach on the part of the FCC.

You would also "lock in" firmware bugs, forcing consumers to purchase a replacement or cause the manufacturer a great deal by means of a recall, when the problem could have been fixed with a firmware update.

It's just a bad idea all around. Costly for consumers and industry, with little real benefit to anybody.

Rather than making the practice illegal, I suggest putting in place a formal complaint process so that people can notify of abuses, much as you do with other kinds of radio today.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Joshua

Last Name: McKinley

Mailing Address: 2622 Commerce Drive

City: Jonesboro

Country: United States

State or Province: AR

ZIP/Postal Code: 72401

Email Address: jmckinley@techfriends.com

Organization Name: Tech Friends, Inc.

Comment: Respectfully,

I manage the tech support department at Tech Friends, Inc. We provide services to correctional institutions around the nation. Security in these institutions is of paramount concern. For that reason, we utilize a custom firmware for routers based on OpenWRT. The proposed rule would prohibit our ability to install customized security firmware on commercial router hardware. This would be catastrophic for our business interests and for the security of correctional facilities around the nation.

It is essential that businesses and individuals have the freedom to install custom firmware on routers.

We urgently ask you to reconsider this portion of the rule to ensure that innovation, security, and flexibility remain an integral part of the network ecosystem.

Respectfully,

I manage the tech support department at Tech Friends, Inc. We provide services to correctional institutions around the nation. Security in these institutions is of paramount concern. For that reason, we utilize a custom firmware for routers based on OpenWRT. The proposed rule would prohibit our ability to install customized security firmware on commercial router hardware. This would be catastrophic for our business interests and for the security of correctional facilities around the nation.

It is essential that businesses and individuals have the freedom to install custom firmware on routers.

We urgently ask you to reconsider this portion of the rule to ensure that innovation, security, and flexibility remain an integral part of the network ecosystem.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Mike

Last Name: Brown

Mailing Address: P.O. Box 1401

City: Campbell

Country: United States

State or Province: CA

ZIP/Postal Code: 95009

Email Address: politics@torvosoft.com

Organization Name:

Comment: To whom it may concern,

Please do not implement rules that prevent users from installing software of their choice on computing devices, including those which include a WiFi radio. Wireless networking research depends on the ability of researchers to investigate and modify their devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

To whom it may concern,

Please do not implement rules that prevent users from installing software of their choice on computing devices, including those which include a WiFi radio. Wireless networking research depends on the ability of researchers to investigate and modify their devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Michael

Last Name: Driscoll

Mailing Address: 10235 S Spaulding

City: Evergreen Park

Country: United States

State or Province: IL

ZIP/Postal Code: 60805

Email Address:

Organization Name:

Comment: I respectfully request the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. In this particular case:

Wireless networking research depends on the ability of researchers to investigate and modify their devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

I respectfully request the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. In this particular case:

Wireless networking research depends on the ability of researchers to investigate and modify their devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Jeffrey

Last Name: Henry

Mailing Address: 14573 Brown Lane

City: Trumann

Country: United States

State or Province: AR

ZIP/Postal Code: 72472

Email Address: yeratel08@gmail.com

Organization Name: Tech Friends, Inc.

Comment: Respectfully,

Our company, Tech Friends, Inc., provides services to correctional institutions around the nation. Obviously, security in these institutions is of paramount concern. For that reason, we utilize a custom firmware for routers based on OpenWRT. The proposed rule would prohibit our ability to install customized security firmware on commercial router hardware. This would be catastrophic for our business interests and for the security of correctional facilities around the nation.

It is essential that businesses and individuals have the freedom to install custom firmware on routers.

We urgently ask you to reconsider this portion of the rule to ensure that innovation, security, and flexibility remain an integral part of the network ecosystem.

Respectfully,

Our company, Tech Friends, Inc., provides services to correctional institutions around the nation. Obviously, security in these institutions is of paramount concern. For that reason, we utilize a custom firmware for routers based on OpenWRT. The proposed rule would prohibit our ability to install customized security firmware on commercial router hardware. This would be catastrophic for our business interests and for the security of correctional facilities around the nation.

It is essential that businesses and individuals have the freedom to install custom firmware on routers.

We urgently ask you to reconsider this portion of the rule to ensure that innovation, security, and flexibility remain an integral part of the network ecosystem.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Jacob

Last Name: Boline

Mailing Address: 1922 Natchez Trace

City: Allen

Country: United States

State or Province: TX

ZIP/Postal Code: 75013

Email Address:

Organization Name:

Comment: I am vehemently against any idea of controlling software installed on computing devices. As an amateur radio operator I find great importance in having control of the software running on my electronic device. For years DDWRT, OpenWRT, Tomato of any other open source firmware for routers has enabled consumers to extend the capability of their routers and close security holes increasing the security of the device and the Internet as a whole. In addition open source firmware has allowed amateur radio wireless meshes to flourish. If consumers were no longer allowed to install their own router firmware, meshes would no longer be possible in their current form. In addition, this could extended to the hackerspace and interfere with those who are experimenting with Arduinos, Raspberry Pis, and any other embedded devices. Rules that restrict consumers hurt not only the consumers, but also creators and tinkers.

I am vehemently against any idea of controlling software installed on computing devices. As an amateur radio operator I find great importance in having control of the software running on my electronic device. For years DDWRT, OpenWRT, Tomato of any other open source firmware for routers has enabled consumers to extend the capability of their routers and close security holes increasing the security of the device and the Internet as a whole. In addition open source firmware has allowed amateur radio wireless meshes to flourish. If consumers were no longer allowed to install their own router firmware, meshes would no longer be possible in their current form. In addition, this could extended to the hackerspace and interfere with those who are experimenting with Arduinos, Raspberry Pis, and any other embedded devices. Rules that restrict consumers hurt not only the consumers, but also creators and tinkers.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: B Spencer

Last Name: Zawasky

Mailing Address: 487 S Main St

City: Andover

Country: United States

State or Province: MA

ZIP/Postal Code: 01810

Email Address:

Organization Name:

Comment: Please do not implement rules that take from us the ability to install the software of our choosing on our computing devices.

Companies generally are limited to fixing issues by selling new devices and software, leaving those of us who have already given them our money to suffer with flawed or dangerous firmware/software.

Further, I say to you that we Americans deserve the ability to fix security holes in our devices when the manufacturer chooses to not do so.

Additionally we as a computer using community generally depend on wireless networking research performed by individuals independent of the manufacturers. That work depends on the ability of such researchers to investigate and modify their devices.

There are many examples of users the past who have fixed serious bugs in their wifi drivers, which would be banned under the NPRM.

Meanwhile billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to trust the security of such devices and as such the ability to install the software of their choosing.

Please do not implement rules that take from us the ability to install the software of our choosing on our computing devices.

Companies generally are limited to fixing issues by selling new devices and software, leaving those of us who have already given them our money to suffer with flawed or dangerous firmware/software.

Further, I say to you that we Americans deserve the ability to fix security holes in our devices when the manufacturer chooses to not do so.

Additionally we as a computer using community generally depend on wireless networking research performed by individuals independent of the manufacturers. That work depends on the ability of such researchers to investigate and modify their devices.

There are many examples of users the past who have fixed serious bugs in their wifi drivers, which would be banned

under the NPRM.

Meanwhile billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to trust the security of such devices and as such the ability to install the software of their choosing.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Eric

Last Name: Harmon

Mailing Address: 44007 Lords Valley Terrace

City: Ashburn

Country: United States

State or Province: VA

ZIP/Postal Code: 20147

Email Address: eric@eharmon.org

Organization Name: None

Comment: The rule to inhibit or ban the modification of firmware of my personally owned router is a mistake.

This would unintentionally inhibit innovation and limit functionality that has been available to the general public for at least a decade. Cutting edge features and more obscure, but useful, abilities added by new software developers would be curtailed.

Many of the features in current routers are developed by open software developers to greatly enhance routers supplied by original equipment manufacturers (OEM).

OEMs rarely display innovation in firmware features until they see popular features added by independent developers.

Any new future enhancements would be moved out of the United States. New innovation would move off shore and open source projects available for decades (ex. DD-WRT) would die.

The only thing this rule would accomplish is a new underground movement to circumvent the restrictions put in place.

The rule to inhibit or ban the modification of firmware of my personally owned router is a mistake.

This would unintentionally inhibit innovation and limit functionality that has been available to the general public for at least a decade. Cutting edge features and more obscure, but useful, abilities added by new software developers would be curtailed.

Many of the features in current routers are developed by open software developers to greatly enhance routers supplied by original equipment manufacturers (OEM).

OEMs rarely display innovation in firmware features until they see popular features added by independent developers.

Any new future enhancements would be moved out of the United States. New innovation would move off shore and open source projects available for decades (ex. DD-WRT) would die.

The only thing this rule would accomplish is a new underground movement to circumvent the restrictions put in place.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Ken

Last Name: Purcell

Mailing Address: 1602 Waterford Dr

City: Lewisville

Country: United States

State or Province: TX

ZIP/Postal Code: 75077

Email Address: ken@kenpurcell.com

Organization Name:

Comment: Really, you feel the need to regulate the firmware controlling WiFi and it associated frequencies? This has all sorts of unintended consequences, most of which I cannot control what I own.

This is an overstep of regulation. What you propose it not even needed.

Really, you feel the need to regulate the firmware controlling WiFi and it associated frequencies? This has all sorts of unintended consequences, most of which I cannot control what I own.

This is an overstep of regulation. What you propose it not even needed.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Tod

Last Name: Stetson

Mailing Address: PO Box 631

City: Copperopolis

Country: United States

State or Province: CA

ZIP/Postal Code: 95228

Email Address: teedeus@gmail.com

Organization Name:

Comment: Please do not take away the ability for consumers to install the software of their choosing on their computing devices. It is an important right for consumers to be able to control the devices that they purchase. Almost every computing device made nowadays contains a wireless radio that operates in the 2.4GHz and 5.8GHz bands. It is imperative for innovation that everyone has the right to be able to change the software on their devices for any reason. Some of those reasons include:

Wireless networking research depends on the ability of researchers to investigate and modify their devices.

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.

Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.

Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

This bill is anti-consumer and anti-innovation. Please reject it.

Please do not take away the ability for consumers to install the software of their choosing on their computing devices. It is an important right for consumers to be able to control the devices that they purchase. Almost every computing device made nowadays contains a wireless radio that operates in the 2.4GHz and 5.8GHz bands. It is imperative for innovation that everyone has the right to be able to change the software on their devices for any reason. Some of those reasons include:

Wireless networking research depends on the ability of researchers to investigate and modify their devices.

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.

Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.

Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

This bill is anti-consumer and anti-innovation. Please reject it.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Krishna

Last Name: Raman

Mailing Address: 2592 Royal Ann Dr

City: Union City

Country: United States

State or Province: CA

ZIP/Postal Code: 94587

Email Address: kraman@gmail.com

Organization Name:

Comment: In the past few years a lot of OSS work has been done to make home routers more secure, easier to manage, feature rich, and much much more stable than the original versions shipped out by manufacturers. This has only been possible because it is currently possible to update the software running on these routers with open-source replacements. I myself use DD-WRT to secure all communications at home.

Most routers nowadays include RF, CPU and memory on the same integrated chip. The proposed rule would forbid flashing that one chip with new software and would seriously degrade performance and security of equipment that I bought and own. Please consider rejection or changing that portion of this regulation.

In the past few years a lot of OSS work has been done to make home routers more secure, easier to manage, feature rich, and much much more stable than the original versions shipped out by manufacturers. This has only been possible because it is currently possible to update the software running on these routers with open-source replacements. I myself use DD-WRT to secure all communications at home.

Most routers nowadays include RF, CPU and memory on the same integrated chip. The proposed rule would forbid flashing that one chip with new software and would seriously degrade performance and security of equipment that I bought and own. Please consider rejection or changing that portion of this regulation.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: John

Last Name: Prince

Mailing Address: PO Box 82768

City: Kenmore

Country: United States

State or Province: WA

ZIP/Postal Code: 98028

Email Address:

Organization Name:

Comment: I would respectfully ask the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

While I understand the need to manage the spectrum assets shared, this type of regulation does not contribute open development and alternative choices for the consumer.

Wireless networking research depends on the ability of researchers to investigate and modify their devices. In addition, having the ability to fix security holes in wireless devices when the manufacturer chooses to not do so.

Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.

Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

I would strongly urge that this restriction not be enacted.

Thank you

John Prince

I would respectfully ask the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

While I understand the need to manage the spectrum assets shared, this type of regulation does not contribute open development and alternative choices for the consumer.

Wireless networking research depends on the ability of researchers to investigate and modify their devices. In addition, having the ability to fix security holes in wireless devices when the manufacturer chooses to not do so.

Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.

Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

I would strongly urge that this restriction not be enacted.

Thank you

John Prince

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: emil

Last Name: heitzler

Mailing Address: christophstr 18

City: Eislingen

Country: Germany

State or Province: Baden Wrttemberg

ZIP/Postal Code: 73241

Email Address: emilheitzler@yahoo.com

Organization Name:

Comment: The proposed rule changes infringes the freedom of a device owner to adopt the device to his personal needs and to develop new features or enhance functionality.

The proposed rule changes infringes the freedom of a device owner to adopt the device to his personal needs and to develop new features or enhance functionality.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: John

Last Name: Ferrini

Mailing Address: 1844 E. 12th Ave

City: Spokane

Country: United States

State or Province: WA

ZIP/Postal Code: 99202

Email Address: john.ferrini@outlook.com

Organization Name:

Comment: I use the opensouce software to control the inteface of my home router. The manufacturer of these pieces of hardware have shown lack of regard for security on these devices that I own one of. Stopping me and others from use of this software can cause irreparable harm to my network protection. The software does not in any way change the radio frequency or use there of. I own this device I do not rent, lease, or license this device from anyone making it my personal property. Your ruling violates this personal property use along with opening my personal devices to unwanted intrusion.

I use the opensouce software to control the inteface of my home router. The manufacturer of these pieces of hardware have shown lack of regard for security on these devices that I own one of. Stopping me and others from use of this software can cause irreparable harm to my network protection. The software does not in any way change the radio frequency or use there of. I own this device I do not rent, lease, or license this device from anyone making it my personal property. Your ruling violates this personal property use along with opening my personal devices to unwanted intrusion.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Marc

Last Name: Levine

Mailing Address: 2400 Deerwood Drive

City: Ukiah

Country: United States

State or Province: CA

ZIP/Postal Code: 95482

Email Address: marc@allearsaudio.com

Organization Name:

Comment: Perhaps the FCC is unaware that there is a substantial public interest in being able to control or modify the software or firmware on a device of one's own.

Just like I am able to purchase a PC and run the programs of my choice, not the programs the manufacturer demands that I run, I can also currently buy a router and replace the firmware with some excellent open source releases that give me extended features, more control, and better performance.

Often the manufacturer has no interest in providing these features, since most customers wouldn't know what to do with them and are not interested in finding out. And so the manufacturer has no incentive to invest in better firmware.

However, advanced users, hobbyists, and professionals all welcome the opportunity to configure their own devices, that they own and have fully paid for, in order to take full advantage of the device's capabilities.

Surely there are penalties in place even now for those who violate the FCC's restrictions on spectrum, power, etc. But there is a whole wealth of possibilities available for modifying a device's settings that do not violate FCC restrictions in any way, but simply provide the user with more functionality.

Perhaps equipment manufacturers would prefer to lock in their proprietary and inadequate firmware for marketing purposes, but it's definitely not in the public interest. There should be no FCC restrictions on what a consumer may do with his or her own device, as long as it still complies with the relevant spectrum and power rules.

Perhaps the FCC is unaware that there is a substantial public interest in being able to control or modify the software or firmware on a device of one's own.

Just like I am able to purchase a PC and run the programs of my choice, not the programs the manufacturer demands that I run, I can also currently buy a router and replace the firmware with some excellent open source releases that give me extended features, more control, and better performance.

Often the manufacturer has no interest in providing these features, since most customers wouldn't know what to do with them and are not interested in finding out. And so the manufacturer has no incentive to invest in better firmware.

However, advanced users, hobbyists, and professionals all welcome the opportunity to configure their own devices, that they own and have fully paid for, in order to take full advantage of the device's capabilities.

Surely there are penalties in place even now for those who violate the FCC's restrictions on spectrum, power, etc. But there is a whole wealth of possibilities available for modifying a device's settings that do not violate FCC restrictions in any way, but simply provide the user with more functionality.

Perhaps equipment manufacturers would prefer to lock in their proprietary and inadequate firmware for marketing purposes, but it's definitely not in the public interest. There should be no FCC restrictions on what a consumer may do with his or her own device, as long as it still complies with the relevant spectrum and power rules.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:=====

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:

First Name: Benjamin

Last Name: Stassart

Mailing Address: 6084 Monterey Hwy, Apt 101

City: San Jose

Country: United States

State or Province: CA

ZIP/Postal Code: 95138-1750

Email Address: ben-fcc@stassart.org

Organization Name: null

Comment: Dear FCC:

I respectfully request that the FCC not implement rules that take away the ability of users to install the software of their choosing on computing devices that they own. This takes away freedom, hurts innovation and competition, and drastically reduces the security of home routers.

With the emphasis the administration is placing on Cyber security, not allowing consumers to fix security issues in their home routers when the vendor chooses not to harms Americans security. Before my current router that I bought because I knew it could run DD-WRT firmware, I had a Cisco M20 wireless router. The Cisco M20 had a security issue that allowed anyone who runs a program downloadable off the Internet to obtain the wireless password and thus to connect to my wireless network. The vendor chose never to fix the issue after being informed about the security issue; it remains unfixed as I write this comment.

Researchers often use custom firmware to test new technologies. If computers had not allowed custom operating system software 25 years ago, we would never have the Linux operating system that is widely used and responsible for so much other innovation such as Android smartphones. If a similar rule had been in place for computers 25 years ago, we wouldn't have Android smartphones today. There are projects like DD-WRT and OpenWRT that provide wireless router firmware and get hardware manufacturers to jump on board; this benefits the manufacturers as they do not have to do the work and it benefits consumers by having options and software that can be used across vendors.

I am not opposed to requiring wireless router manufacturers to put hardware limits on power, frequency, and other items that may cause interference or other concerns for the FCC and ensuring that these limits cannot be overridden by firmware. One could also put regulations on the firmware such as what options are presented to the user; although this would have to be done carefully. However, do not accomplish this by limiting the ability to replace the firmware. In my opinion, limiting the replacement of firmware may cause great harm to American consumers long term.

Thank you very much for your time.

Sincerely,  
Benjamin Stassart

Dear FCC:

I respectfully request that the FCC not implement rules that take away the ability of users to install the software of their