

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: Neel

Last Name: Kshetramade

Mailing Address: 1600 Amphitheater Parkway

City: Mountain View

Country: United States

State or Province: CA

ZIP/Postal Code: 94043

Email Address: swapneelakb@yahoo.com

Organization Name:

Comment: To the FCC,

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.

To the FCC,

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: Kareem

Last Name: Dado

Mailing Address: 450 J st.

City: San Diego

Country: United States

State or Province: CA

ZIP/Postal Code: 92101

Email Address:

Organization Name:

Comment: Respectfully requesting the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Additional points of emphasis you should consider adding:

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.

Respectfully requesting the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Additional points of emphasis you should consider adding:

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: Jack

Last Name: Enneking

Mailing Address: 3722 Alabama St. #125

City: San Diego

Country: United States

State or Province: CA

ZIP/Postal Code: 92104

Email Address: jackenneking@gmail.com

Organization Name:

Comment: Please don't make any changes that prevent consumers from maintaining control of their own devices. That would damage security of many devices, chill research and development, and even destroy some businesses who provide customized WiFi solutions. Plus, on principle, why should you or I be unable to do what we want with the devices we purchase?

Please don't make any changes that prevent consumers from maintaining control of their own devices. That would damage security of many devices, chill research and development, and even destroy some businesses who provide customized WiFi solutions. Plus, on principle, why should you or I be unable to do what we want with the devices we purchase?

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: James

Last Name: Jacocks

Mailing Address: 7121 Main Street

City: Queenstown

Country: United States

State or Province: MD

ZIP/Postal Code: 21658

Email Address: jjacocks@gmail.com

Organization Name:

Comment: To whom it may concern,

It is critically important that you not implement rules that take away the ability of users to install the software of their choosing on their computing devices. This seems like a very simple issue, simply involving the restriction of possibly non-compliant changes to software-defined radio devices, but it has much larger implications for the entire industry. Any device bought by a consumer should be truly owned by that consumer; i.e. any changes that the consumer sees fit to make should not be actively prevented. It is the consumer's responsibility, of course, to make sure that such changes don't fall afoul of the law.

Other points to consider are: that wireless networking research depends on the ability of researchers to investigate and modify their devices; that Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so; that users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM; and that billions of dollars of commerce, involving such markets as secure wifi vendors, retail hotspot vendors, and others, depend on the ability of users and companies to install the software of their choosing on network devices.

Thank you for your consideration,

James Alexander Jacocks

To whom it may concern,

It is critically important that you not implement rules that take away the ability of users to install the software of their choosing on their computing devices. This seems like a very simple issue, simply involving the restriction of possibly non-compliant changes to software-defined radio devices, but it has much larger implications for the entire industry. Any device bought by a consumer should be truly owned by that consumer; i.e. any changes that the consumer sees fit to make should not be actively prevented. It is the consumer's responsibility, of course, to make sure that such changes don't fall afoul of the law.

Other points to consider are: that wireless networking research depends on the ability of researchers to investigate and modify their devices; that Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so; that users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM; and that billions of dollars of commerce, involving such markets as secure wifi vendors, retail hotspot vendors, and others, depend on the ability of users and companies to install the software of their choosing on network devices.

Thank you for your consideration,  
James Alexander Jacocks

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: Robert

Last Name: Miller

Mailing Address: 1093D Summit Trail Circle

City: West Palm Beach

Country: United States

State or Province: FL

ZIP/Postal Code: 33415

Email Address: humagotchy@yahoo.com

Organization Name:

Comment: Please do not implement rules that take away the ability of users to install the software of their choosing on our computing devices, such as home wireless routers.

I also strongly agree with the following as well:

- 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.

Thank you for taking the above into consideration!

Please do not implement rules that take away the ability of users to install the software of their choosing on our computing devices, such as home wireless routers.

I also strongly agree with the following as well:

- 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.

Thank you for taking the above into consideration!

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: Zephaniah

Last Name: Loss-Cutler-Hull

Mailing Address: 12432 21st Ave SE

City: Everett

Country: United States

State or Province: WA

ZIP/Postal Code: 98208

Email Address: warp-spam\_federalregister@aehallh.com

Organization Name:

Comment: Hello,

My name is Zephaniah Loss-Cutler-Hull, and I am writing you in regards to the proposed rules for mandating locked firmware on wifi devices.

In my personal use, I very rarely encounter affordable wifi access points that offer the functionality that I desire, and very often find that hardware is rapidly abandoned by the manufacturer.

The first half of this means that my options are currently: Have a configuration that lacks the features that I rely on, flash a custom firmware, or pay several times as much for a device that offers most, but often not all, of what I desire feature wise.

The second half means that there is a very high chance that when a security vulnerability such as shellshock, heartbleed, testing backdoors accidentally left on in the firmware, or the like, my only recourse is to replace the device.

With the options for custom firmware removed, my options are bleak, financially prohibitive, and in all cases less functional than I can legally get today on a reasonably wide range of commodity devices.

Some of the features that I use that are not always common, especially in more affordable hardware, are easy display of connection data(what devices are associated, when they last re-associated, signal strength, mac address), complex firewall rules, bridging, remote administration via ssh, the ability to use a valid SSL certificate for the administrative web interface, sometimes even the ability to use HTTPS for the administrative web interface.

In short, I strongly disagree with the proposal as written.

Regards,  
Zephaniah E. Loss-Cutler-Hull.

Hello,

My name is Zephaniah Loss-Cutler-Hull, and I am writing you in regards to the proposed rules for mandating locked firmware on wifi devices.

In my personal use, I very rarely encounter affordable wifi access points that offer the functionality that I desire, and

very often find that hardware is rapidly abandoned by the manufacturer.

The first half of this means that my options are currently: Have a configuration that lacks the features that I rely on, flash a custom firmware, or pay several times as much for a device that offers most, but often not all, of what I desire feature wise.

The second half means that there is a very high chance that when a security vulnerability such as shellshock, heartbleed, testing backdoors accidentally left on in the firmware, or the like, my only recourse is to replace the device.

With the options for custom firmware removed, my options are bleak, financially prohibitive, and in all cases less functional than I can legally get today on a reasonably wide range of commodity devices.

Some of the features that I use that are not always common, especially in more affordable hardware, are easy display of connection data(what devices are associated, when they last re-associated, signal strength, mac address), complex firewall rules, bridging, remote administration via ssh, the ability to use a valid SSL certificate for the administrative web interface, sometimes even the ability to use HTTPS for the administrative web interface.

In short, I strongly disagree with the proposal as written.

Regards,  
Zephaniah E. Loss-Cutler-Hull.

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: Toby

Last Name: norton

Mailing Address: 714 "J" St.

City: Crescent City

Country: United States

State or Province: CA

ZIP/Postal Code: 95531

Email Address:

Organization Name:

Comment: This is \*CRAP\*!!!!

I don't want to loose the use of DD-WRT!  
They add features to Routers that the  
Router manufacturer should put in Routers  
in the first place!

This is \*CRAP\*!!!!

I don't want to loose the use of DD-WRT!  
They add features to Routers that the  
Router manufacturer should put in Routers  
in the first 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: Albert

Last Name: DeWitt Jr.

Mailing Address: 720 N. Farr Rd.

City: Spokane Valley

Country: United States

State or Province: WA

ZIP/Postal Code: 99206-3879

Email Address: will.dewitt+fcc@gmail.com

Organization Name:

Comment: I will be as brief as possible:

I think this proposed rule is a bad idea as it stifles innovation and would unfairly (and unreasonably) deter open source development of Wifi software (including software that controls the radio devices available in the hardware). Further, as hardware is abandoned by the manufacturer, this would make it illegal for end users to maintain the equipment if they have the technical prowess or means (and would, as noted earlier, be further reduced by the fact that nobody else will have done any work on firmware because the practice will have been illegal). Even if an exception were added to allow this kind of work if a product is abandoned, the concept would be difficult (if not impossible) to correctly define and enforce. And again, efforts would be harmed because no work would have begun until after the product had clearly been "abandoned".

For the reasons outlined above, I strongly discourage adoption of any rule that would curtail the development of wifi router firmware (or modifications to existing firmware).

I will be as brief as possible:

I think this proposed rule is a bad idea as it stifles innovation and would unfairly (and unreasonably) deter open source development of Wifi software (including software that controls the radio devices available in the hardware). Further, as hardware is abandoned by the manufacturer, this would make it illegal for end users to maintain the equipment if they have the technical prowess or means (and would, as noted earlier, be further reduced by the fact that nobody else will have done any work on firmware because the practice will have been illegal). Even if an exception were added to allow this kind of work if a product is abandoned, the concept would be difficult (if not impossible) to correctly define and enforce. And again, efforts would be harmed because no work would have begun until after the product had clearly been "abandoned".

For the reasons outlined above, I strongly discourage adoption of any rule that would curtail the development of wifi router firmware (or modifications to existing firmware).

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: Damiano

Last Name: Guerrini

Mailing Address: via Asiago 56/4

City: Quarrata

Country: Italy

State or Province: Pistoia

ZIP/Postal Code: 51039

Email Address: damiano.guerrini@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: Kahn

Last Name: Knight

Mailing Address: 1201 E Park #1718

City: Plano

Country: United States

State or Province: TX

ZIP/Postal Code: 75074

Email Address: nemisor@protonmail.com

Organization Name:

Comment: Our hardware. Our firmware. Keep your hands off it. Period.

Our hardware. Our firmware. Keep your hands off it. Period.

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: Bonham

Mailing Address: 7675 Reed St

City: Arvada

Country: United States

State or Province: CO

ZIP/Postal Code: 80003

Email Address: bonham@gmail.com

Organization Name:

Comment: Hello FCC,

I'm copying part of my response from others who write better than I: "As written, the rules and recommendations of the commission will prevent the installation of traditional free and open source wireless firmware such as OpenWrt. End-users often use such firmware because it better fits the users needs. Each user is better able to tailor the device to their needs. Users often set up a guest wireless network for their home or business, set up a web server at their home, create IoT hubs and other uses. The changes proposed will make such changes difficult and, in some cases, impossible."

I have used opensource (Tomato) router software for a decade; it is more reliable, more customizable, and more secure and audited than software provided by router manufacturers. It is an unwise overreach to shut down this ability.

Thank you.

Hello FCC,

I'm copying part of my response from others who write better than I: "As written, the rules and recommendations of the commission will prevent the installation of traditional free and open source wireless firmware such as OpenWrt. End-users often use such firmware because it better fits the users needs. Each user is better able to tailor the device to their needs. Users often set up a guest wireless network for their home or business, set up a web server at their home, create IoT hubs and other uses. The changes proposed will make such changes difficult and, in some cases, impossible."

I have used opensource (Tomato) router software for a decade; it is more reliable, more customizable, and more secure and audited than software provided by router manufacturers. It is an unwise overreach to shut down this ability.

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: Stephen

Last Name: Delear

Mailing Address: 414 Aurora Ct

City: College Station

Country: United States

State or Province: TX

ZIP/Postal Code: 77840

Email Address: sdelear@tamu.edu

Organization Name:

Comment: These proposed regulations would increase both threats to data security as well as the chance of radio frequency interference. A router should be thought of as three modules. An always on, wired, connection to a network (generally the internet), a computer to handle tasks (the router) and an rf transmitter/receiver.

Wireless routers are one of the key vulnerabilities in many networks. Unlike other equipment, they are rarely turned off. They, along with high speed modems, exists outside of the security programs/applications that consumers may run on their computers or devices.

Long experience has shown that proprietary software often lags behind its open source counterparts when it comes to addressing security concerns. These can be of a fairly serious nature. Unless substantial fines were imposed on manufacturers selling compromised products, prompt security updates are unlikely.

Flashing in open source firmware allows for all routers on a commercial network, regardless of maker, to run the same basic software -- allowing for ease of update, maintenance and security. Further, foreign customers may be unwilling or face regulatory requirements rendering them unwilling to utilize any network equipment that has not had its firmware installed within the jurisdiction from an audited and locally compiled source code.

The black box nature of the proposed regulations increases the probability of rf interference. If a security vulnerability were to exist, a third party might be able to utilize it to cause the device to blanket the area with interference. The more locked down the firmware is, the harder it is to fix if something unfortunate were to happen. What happens when a North Korean hacker finds a vulnerability that can turn 100,000 consumer routers into jamming devices, and those devices can only be fixed by physically interacting with them?

A better regulation would be to require manufacturers to release opensource drivers for the rf components of their devices that cause the device to act in the desired manner. The opensource community is unlikely to spend the effort to rewrite an open driver into something that might not work as intended.

These proposed regulations would increase both threats to data security as well as the chance of radio frequency interference. A router should be thought of as three modules. An always on, wired, connection to a network (generally the internet), a computer to handle tasks (the router) and an rf transmitter/receiver.

Wireless routers are one of the key vulnerabilities in many networks. Unlike other equipment, they are rarely turned off. They, along with high speed modems, exists outside of the security programs/applications that consumers may run on their computers or devices.

Long experience has shown that proprietary software often lags behind its open source counterparts when it comes to addressing security concerns. These can be of a fairly serious nature. Unless substantial fines were imposed on manufacturers selling compromised products, prompt security updates are unlikely.

Flashing in open source firmware allows for all routers on a commercial network, regardless of maker, to run the same basic software -- allowing for ease of update, maintenance and security. Further, foreign customers may be unwilling or face regulatory requirements rendering them unwilling to utilize any network equipment that has not had its firmware installed within the jurisdiction from an audited and locally compiled source code.

The black box nature of the proposed regulations increases the probability of rf interference. If a security vulnerability were to exist, a third party might be able to utilize it to cause the device to blanket the area with interference. The more locked down the firmware is, the harder it is to fix if something unfortunate were to happen. What happens when a North Korean hacker finds a vulnerability that can turn 100,000 consumer routers into jamming devices, and those devices can only be fixed by physically interacting with them?

A better regulation would be to require manufacturers to release opensource drivers for the rf components of their devices that cause the device to act in the desired manner. The opensource community is unlikely to spend the effort to rewrite an open driver into something that might not work as intended.

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: Peter

Last Name: Wutzke

Mailing Address: 213 N. 5th st.

City: Mount Vernon

Country: United States

State or Province: WA

ZIP/Postal Code: 98273

Email Address:

Organization Name:

Comment: I am concerned that as written, the rules and recommendations of the commission will prevent the installation of traditional free and open source wireless firmware such as OpenWrt. End-users often use such firmware because it better fits the users needs. Each user is better able to tailor the device to their needs. Users often set up a guest wireless network for their home or business, set up a web server at their home, create IoT hubs and other uses. The changes proposed will make such changes difficult and, in some cases, impossible.

This rule change also seems completely unnecessary, as no FCC complaints about improper usage of routers were related to flashing third-party firmware. Most were related to commercial wifi providers breaking the law. In some cases, the official router web administration for the routers used in the complaint had a UI for operating in an illegal fashion. For example, it was possible to turn off all DFS or allow test operation on all possible channels which are both wildly irresponsible to place in a standard router UI.

Innovation in network and wireless technology depends on the ability 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. HNCP, a proposed IETF proposed standard for managing home networks, is being developed using OpenWrt. Mesh networking technologies for developing stable distributed internet access are regularly implemented on OpenWrt 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. Without the ability to change the software on the device, these innovations would not have occurred. The innovations done by the community are later often picked up by the home router vendors and being integrated into their normal firmware versions for their next generations of devices.

I am also concerned that emergency preparedness could be hindered by restrictions on the modification of router hardware. Mesh networking is a key component of disaster response in our modern world. In disasters, amateur radio operators create mesh networks for disaster response. These operators use firmware like Broadband-Hamnet to create mesh networks on low-cost commodity routers operating at frequencies and power levels legally authorized for hams but not for other users. By modifying the device in such ways, wireless networks can be organized to cover much larger swaths of area to first-responders and emergency personnel. These restrictions would delay the exchange of emergency information and put lives at risk. The value of modified router hardware to assist in disaster response is recognized by emergency managers. In 2013, the International Association of Emergency Managers [6] designated Broadband-Hamnet as their US Technology and Innovation Award winner and Global Technology and Innovation Award winner.

Perhaps most troubling, is that restrictions on replacing router software will have a serious impact on security.

Manufacturers are notoriously lax about providing timely security updates where such updates are provided at all. Security experts routinely recommend users replace manufacturer shipped router firmware with alternative community driven versions as a solution to this problem. In a recent security review of commercial routers, every one had critical security vulnerabilities. In most security instances replacing router firmware with third party peer reviewed firmware is the only option to solving this type of problem. While the security dangers for home users are serious, for large companies security dangers are critical. Without the ability to replace this software, large companies purchasing routers are entirely at the whim of the router maker. If this software is insecure, whether accidentally or intentionally, large American companies will be put at risk of industrial espionage.

I am concerned that as written, the rules and recommendations of the commission will prevent the installation of traditional free and open source wireless firmware such as OpenWrt. End-users often use such firmware because it better fits the users needs. Each user is better able to tailor the device to their needs. Users often set up a guest wireless network for their home or business, set up a web server at their home, create IoT hubs and other uses. The changes proposed will make such changes difficult and, in some cases, impossible.

This rule change also seems completely unnecessary, as no FCC complaints about improper usage of routers were related to flashing third-party firmware. Most were related to commercial wifi providers breaking the law. In some cases, the official router web administration for the routers used in the complaint had a UI for operating in an illegal fashion. For example, it was possible to turn off all DFS or allow test operation on all possible channels which are both wildly irresponsible to place in a standard router UI.

Innovation in network and wireless technology depends on the ability 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. HNCP, a proposed IETF proposed standard for managing home networks, is being developed using OpenWrt. Mesh networking technologies for developing stable distributed internet access are regularly implemented on OpenWrt 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. Without the ability to change the software on the device, these innovations would not have occurred. The innovations done by the community are later often picked up by the home router vendors and being integrated into their normal firmware versions for their next generations of devices.

I am also concerned that emergency preparedness could be hindered by restrictions on the modification of router hardware. Mesh networking is a key component of disaster response in our modern world. In disasters, amateur radio operators create mesh networks for disaster response. These operators use firmware like Broadband-Hamnet to create mesh networks on low-cost commodity routers operating at frequencies and power levels legally authorized for hams but not for other users. By modifying the device in such ways, wireless networks can be organized to cover much larger swaths of area to first-responders and emergency personnel. These restrictions would delay the exchange of emergency information and put lives at risk. The value of modified router hardware to assist in disaster response is recognized by emergency managers. In 2013, the International Association of Emergency Managers [6] designated Broadband-Hamnet as their US Technology and Innovation Award winner and Global Technology and Innovation Award winner.

Perhaps most troubling, is that restrictions on replacing router software will have a serious impact on security. Manufacturers are notoriously lax about providing timely security updates where such updates are provided at all. Security experts routinely recommend users replace manufacturer shipped router firmware with alternative community driven versions as a solution to this problem. In a recent security review of commercial routers, every one had critical security vulnerabilities. In most security instances replacing router firmware with third party peer reviewed firmware is the only option to solving this type of problem. While the security dangers for home users are serious, for large companies security dangers are critical. Without the ability to replace this software, large companies purchasing routers are entirely at the whim of the router maker. If this software is insecure, whether accidentally or intentionally, large American companies will be put at risk of industrial espionage.

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: Adam

Last Name: Dyess

Mailing Address: 101 Mill Village Place

City: Madison

Country: United States

State or Province: AL

ZIP/Postal Code: 35758

Email Address: adyess@gmail.com

Organization Name: ADTRAN

Comment: This is a pretty terrible plan:

- \* 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 is a pretty terrible plan:

- \* 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: William

Last Name: Wong

Mailing Address: 1333 Moon Drive

City: Yardley

Country: United States

State or Province: PA

ZIP/Postal Code: 19067

Email Address: bwong789@gmail.com

Organization Name:

Comment: I have worked in the computer and electronics industry for over 35 years and I think that the proposed rules are a very bad idea that will restrict suitable use of wireless hardware unnecessarily. The ability to update software in a device has major benefits from including providing better security, bug fixes and alternative functionality.

Preventing users from making firmware changes is an unnecessary limitation to meet the goals of preventing a wireless device from exceeding its design with respect to FCC rules. For example, power level limitations are something that is easily handled in hardware.

I know others have provided significantly more detailed examples and reasons so I will not repeat or enumerate them here. Suffice it to say that I disagree with the proposed rules for all those reasons.

I have worked in the computer and electronics industry for over 35 years and I think that the proposed rules are a very bad idea that will restrict suitable use of wireless hardware unnecessarily. The ability to update software in a device has major benefits from including providing better security, bug fixes and alternative functionality.

Preventing users from making firmware changes is an unnecessary limitation to meet the goals of preventing a wireless device from exceeding its design with respect to FCC rules. For example, power level limitations are something that is easily handled in hardware.

I know others have provided significantly more detailed examples and reasons so I will not repeat or enumerate them here. Suffice it to say that I disagree with the proposed rules for all those reasons.

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: Dave

Last Name: Mills

Mailing Address: P.O. Box 44070

City: Tucson

Country: United States

State or Province: AZ

ZIP/Postal Code: 85733

Email Address: dmills@noao.edu

Organization Name:

Comment: Preventing third party firmware updates will severely impact the security of future devices. Most manufacturers have an appalling record of patching security flaws in these products. Open Source third party projects on the other hand, have an excellent record in this area.

Preventing third party firmware updates will severely impact the security of future devices. Most manufacturers have an appalling record of patching security flaws in these products. Open Source third party projects on the other hand, have an excellent record in this area.

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: Todd

Last Name: Markley

Mailing Address: 3776 Headleys Mill RD

City: Pataskala

Country: United States

State or Province: OH

ZIP/Postal Code: 43062

Email Address:

Organization Name:

Comment: I strongly disagree with the plan to have the manufacturers of new wifi routers lock the firmware to prevent the customer from installing software on the equipment they own. The manufacturers have a very bad track record of fixing security problems of models that are not currently what they are marketing, and this would prevent owners from selecting more secure firmware. This could also hinder and/or prevent researchers from exposing security problems which would result in helping the criminals take advantage of these routers. Existing rules protect against any unlawful use of the router radio equipment and provide for enforcement, so this additional restriction on firmware changes is unnecessary.

I strongly disagree with the plan to have the manufacturers of new wifi routers lock the firmware to prevent the customer from installing software on the equipment they own. The manufacturers have a very bad track record of fixing security problems of models that are not currently what they are marketing, and this would prevent owners from selecting more secure firmware. This could also hinder and/or prevent researchers from exposing security problems which would result in helping the criminals take advantage of these routers. Existing rules protect against any unlawful use of the router radio equipment and provide for enforcement, so this additional restriction on firmware changes is unnecessary.

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: Jeremy

Last Name: Brandt

Mailing Address: 1595 Woodbine Ct

City: Bryan

Country: United States

State or Province: TX

ZIP/Postal Code: 77802

Email Address: jeremyabrandt@gmail.com

Organization Name:

Comment: While the FCC feels it needs to update its rules concerning RF radios, this broadly worded proposed rule making may in fact do much harm to end users/consumers. Without precise wording, history has shown us that certain entities will twist the rule's verbiage to artificially limit a consumers ability to use or interact with their own devices by threatening legal action. This has the potential to leave consumers with devices that are essentially crippled by poor or outdated software that could be corrected if not for that threat. Innovation and research in fields relating to wireless technologies will also be stifled if this rule making is passed "as-is".

A few points to consider:

- 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.

Respectfully, the FCC should take care not to implement any rule with even a slight chance of taking away the ability of users to install software of their choosing on their own computing devices.

While the FCC feels it needs to update its rules concerning RF radios, this broadly worded proposed rule making may in fact do much harm to end users/consumers. Without precise wording, history has shown us that certain entities will twist the rule's verbiage to artificially limit a consumers ability to use or interact with their own devices by threatening legal action. This has the potential to leave consumers with devices that are essentially crippled by poor or outdated software that could be corrected if not for that threat. Innovation and research in fields relating to wireless technologies will also be stifled if this rule making is passed "as-is".

A few points to consider:

- 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.

Respectfully, the FCC should take care not to implement any rule with even a slight chance of taking away the ability of users to install software of their choosing on their own computing devices.

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: Tom

Last Name: Spindler

Mailing Address: 1355 Market St, STE 900

City: San Francisco

Country: United States

State or Province: CA

ZIP/Postal Code: 94103

Email Address: dogcow@twitter.com

Organization Name: Twitter, Inc

Comment: As an IT professional, I must strongly object to this proposed rule change. With the move towards single SoC systems, the WiFi radio is the router; it's all-or-nothing. Bad actors will not care one whit about injecting bogus or malevolent data onto the WiFi spectrum - and if this change takes effect, I will have no legal option to mitigate security vulnerabilities except for "turn off all my equipment, and tell my users 'too bad'."

As an IT professional, I must strongly object to this proposed rule change. With the move towards single SoC systems, the WiFi radio is the router; it's all-or-nothing. Bad actors will not care one whit about injecting bogus or malevolent data onto the WiFi spectrum - and if this change takes effect, I will have no legal option to mitigate security vulnerabilities except for "turn off all my equipment, and tell my users 'too bad'."

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: Mitchel

Last Name: Humpherys

Mailing Address: 12940 Cree Dr

City: Poway

Country: United States

State or Province: CA

ZIP/Postal Code: 92064

Email Address: mitch.special@gmail.com

Organization Name:

Comment: No.

No.

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: Brandon

Last Name: Mitchell

Mailing Address: 3020 Hickory Grove Ct

City: Fairfax

Country: United States

State or Province: VA

ZIP/Postal Code: 22031-1141

Email Address:

Organization Name:

Comment: As a user of open source firmware on my home router, I ask that the proposed change be rejected by the FCC. Full details of the problems this policy will cause, and the need for open source firmware that can be maintained by the end user, are available from at the Save WiFi project: [https://libreplanet.org/wiki/Save\\_WiFi](https://libreplanet.org/wiki/Save_WiFi)

As a user of open source firmware on my home router, I ask that the proposed change be rejected by the FCC. Full details of the problems this policy will cause, and the need for open source firmware that can be maintained by the end user, are available from at the Save WiFi project: [https://libreplanet.org/wiki/Save\\_WiFi](https://libreplanet.org/wiki/Save_WiFi)

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: Koshak

Mailing Address: 835 Wuthering Heights Drive

City: Colorado Springs

Country: United States

State or Province: CO

ZIP/Postal Code: 80921

Email Address: rlkoshak@gmail.com

Organization Name: self

Comment: Dear FCC,

These new regulations as written have the potential to significantly restrict innovation and limit the ability for users to learn about, research, modify, and repair their wireless devices, particularly in cases where the device is built such that the computer part of the device and the wireless part of the device are included on the same chip.

These rules will prevent me from installing the software of my choice on devices that I own. It will prevent researchers and home tinkerers from investigating and developing new wireless capabilities with existing devices (e.g. adding home automation to a stock wifi router) by preventing them from modifying the software. It will prevent me and other American citizens from fixing security flaws in our owned devices should the manufacturer choose not to do so, something that is more than just theoretical but has actually happened. It will also limit the ability of companies in many industries that rely on the ability to modify how a wireless device like a wifi router operates.

These new regulations will also be another situation where the concept of ownership will be eroded by applying a law or regulation in a way never intended (see John Deere preventing farmers from fixing their own tractors using copyright laws and the Digital Millennium Copyright Act).

Thank you

Dear FCC,

These new regulations as written have the potential to significantly restrict innovation and limit the ability for users to learn about, research, modify, and repair their wireless devices, particularly in cases where the device is built such that the computer part of the device and the wireless part of the device are included on the same chip.

These rules will prevent me from installing the software of my choice on devices that I own. It will prevent researchers and home tinkerers from investigating and developing new wireless capabilities with existing devices (e.g. adding home automation to a stock wifi router) by preventing them from modifying the software. It will prevent me and other American citizens from fixing security flaws in our owned devices should the manufacturer choose not to do so, something that is more than just theoretical but has actually happened. It will also limit the ability of companies in many industries that rely on the ability to modify how a wireless device like a wifi router operates.

These new regulations will also be another situation where the concept of ownership will be eroded by applying a law or regulation in a way never intended (see John Deere preventing farmers from fixing their own tractors using copyright

laws and the Digital Millennium Copyright Act).

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: Andrea

Last Name: Cocito

Mailing Address: Residenza Golfo 262

City: Milano

Country: Italy

State or Province: MI

ZIP/Postal Code: 20139

Email Address: andrea@cocito.eu

Organization Name:

Comment: This set of rules would simply kill the possibility to use Open Source firmare in any device.

Effects would be:

- a. As closed source and proprietary solutions have a long history of security update failure and latency this would LOWER the overall security
- b. As vendors have no interest to release updates for already-sold devices this would again LOWER the security
- c. For the same reason as "b." this would negate the possibility to people ho own a deive to obtain access to technological improvements, increasing the obsolency of devies
- d. As it is quite easy to reverse enginner and change illegally the firmware/software on any modern device this would be NO OBSTACLE to any persone with illegal/bad intentions
- e. As the lack of public/peer-reviewed audit of firmware and software, possible only on open source solutions, would lower the chance to discover and address issues, security weaknesses and bugs, people aimed at actions as in "d." like terrorists, cyber criminals, foreign agents and so on will be advantaged in their activity.

This proposal is simply insane, probably sponsored by a pool of private companies selling devices and, surely, handled by a "commitee".

This set of rules would simply kill the possibility to use Open Source firmare in any device.

Effects would be:

- a. As closed source and proprietary solutions have a long history of security update failure and latency this would LOWER the overall security
- b. As vendors have no interest to release updates for already-sold devices this would again LOWER the security
- c. For the same reason as "b." this would negate the possibility to people ho own a deive to obtain access to technological improvements, increasing the obsolency of devies
- d. As it is quite easy to reverse enginner and change illegally the firmware/software on any modern device this would be NO OBSTACLE to any persone with illegal/bad intentions
- e. As the lack of public/peer-reviewed audit of firmware and software, possible only on open source solutions, would lower the chance to discover and address issues, security weaknesses and bugs, people aimed at actions as in "d." like terrorists, cyber criminals, foreign agents and so on will be advantaged in their activity.

This proposal is simply insane, probably sponsored by a pool of private companies selling devices and, surely, handled by a "commitee".

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: Ravi

Last Name: Terala

Mailing Address: 24464 NE 1st Ct

City: Sammamish

Country: United States

State or Province: WA

ZIP/Postal Code: 98074

Email Address:

Organization Name:

Comment: I am a regular user of custom firmware for at least two of my routers. The custom firmware provides much greater features using open source software, allowing me to utilize the hardware capabilities to the fullest. I don't use it to exploiting the airwaves in any other way and fully honor the limits established by the FCC.

Most of the devices these days use the open airwaves to communicate with the rest of the world. All of these IoT devices come with firmware, often linux/android based with extensive ability to hack/modify and improve these devices.

Limiting custom firmware for these devices will not serve any purpose other than curtailing customer freedom and limiting innovation. I strongly urge FCC to not take any actions limiting customer freedom in using custom firmware to gain maximum benefit out of the hardware they paid for.

I am a regular user of custom firmware for at least two of my routers. The custom firmware provides much greater features using open source software, allowing me to utilize the hardware capabilities to the fullest. I don't use it to exploiting the airwaves in any other way and fully honor the limits established by the FCC.

Most of the devices these days use the open airwaves to communicate with the rest of the world. All of these IoT devices come with firmware, often linux/android based with extensive ability to hack/modify and improve these devices.

Limiting custom firmware for these devices will not serve any purpose other than curtailing customer freedom and limiting innovation. I strongly urge FCC to not take any actions limiting customer freedom in using custom firmware to gain maximum benefit out of the hardware they 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: H Jared

Last Name: Agnew

Mailing Address: 2101 Wilson Blvd Suite 1001

City: Arlington

Country: United States

State or Province: VA

ZIP/Postal Code: 22201

Email Address: hjagnew@dalabs.com

Organization Name: D A LABS L. L. C.

Comment: Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Specifically I am concerned with the following issues.

- (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.

Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Specifically I am concerned with the following issues.

- (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.

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: Dustin

Last Name: Strickland

Mailing Address: 6329 Valhalla Dr

City: Douglasville

Country: United States

State or Province: GA

ZIP/Postal Code: 30135

Email Address: dustin.h.strickland@gmail.com

Organization Name: Tekno Research

Comment: A largely unneeded regulation. Encrypting radio software such that it can't be changed by end users or software developers will create more trouble than it's worth. Why restrict them? Certainly there are not many people writing custom RF radio drivers that cause excessive noise. But there are many individuals and companies, myself included, that enjoy the freedom of being able to load aftermarket software onto their devices. All of my personal routers run a variant of DD-WRT because it has capabilities not found in the stock firmware of any consumer-grade equipment. Features like VLANs, OpenVPN etc. are invaluable to hobbyists, small businesses and IT professionals. Further, the freedom to modify a product that you have purchased is, I feel, fundamental and while I am glad that you are taking public commentary on this proposal I am very disappointed that the proposal was not immediately shot down in consideration of its ethical implications. Ethical problems aside, in the absence of the freedom to use consumer radios as intended by their end-users, will you be creating a market for poorly-made bootleg RF radios that will multiply the issues you're wishing to combat? While I understand the FCC's utility and the considerations it must make in order to carry out its duties, you must be asked: Do you really wish to crack down on and possibly even exacerbate a small problem by keeping us all from using our devices as we want?

A largely unneeded regulation. Encrypting radio software such that it can't be changed by end users or software developers will create more trouble than it's worth. Why restrict them? Certainly there are not many people writing custom RF radio drivers that cause excessive noise. But there are many individuals and companies, myself included, that enjoy the freedom of being able to load aftermarket software onto their devices. All of my personal routers run a variant of DD-WRT because it has capabilities not found in the stock firmware of any consumer-grade equipment. Features like VLANs, OpenVPN etc. are invaluable to hobbyists, small businesses and IT professionals. Further, the freedom to modify a product that you have purchased is, I feel, fundamental and while I am glad that you are taking public commentary on this proposal I am very disappointed that the proposal was not immediately shot down in consideration of its ethical implications. Ethical problems aside, in the absence of the freedom to use consumer radios as intended by their end-users, will you be creating a market for poorly-made bootleg RF radios that will multiply the issues you're wishing to combat? While I understand the FCC's utility and the considerations it must make in order to carry out its duties, you must be asked: Do you really wish to crack down on and possibly even exacerbate a small problem by keeping us all from using our devices as we want?

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: Alex

Last Name: Sparks

Mailing Address: 3719 Stadium Blvd Apt I20

City: Jonesboro

Country: United States

State or Province: AR

ZIP/Postal Code: 72404

Email Address: [asparks@techfriends.com](mailto:asparks@techfriends.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.

Alex Sparks

Software Developer

Tech Friends, Inc.

870.933.6386

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.

Alex Sparks

Software Developer

Tech Friends, Inc.

870.933.6386

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: Abraham

Last Name: Hoffman

Mailing Address: 11545 N Frank Lloyd Wright Blvd

City: Scottsdale

Country: United States

State or Province: AZ

ZIP/Postal Code: 85259

Email Address: abhoffman@paypal.com

Organization Name: PayPal, Inc.

Comment: The forced encryption of firmware is a mistake. The internet has been able to grow because restrictions like these were not in place. If this proposal is enacted, it will mean a serious loss to freedom.

Please dismiss this proposal!

The forced encryption of firmware is a mistake. The internet has been able to grow because restrictions like these were not in place. If this proposal is enacted, it will mean a serious loss to freedom.

Please dismiss this proposal!

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: Jon

Last Name: Califf

Mailing Address: PO Box 8

City: North Bonneville

Country: United States

State or Province: WA

ZIP/Postal Code: 98639

Email Address: jon@silverstarindustries.com

Organization Name: Silver Star Industries, Inc.

Comment: This is incredibly un-american. Criminals are still going to break the law and use radios however they want. This is simply a type of protectionism, guaranteeing that closed-source companies will rule the market. This will simply punish innocent people by locking them into proprietary firmware. Enforce the existing law governing the way radios should be used instead.

This is incredibly un-american. Criminals are still going to break the law and use radios however they want. This is simply a type of protectionism, guaranteeing that closed-source companies will rule the market. This will simply punish innocent people by locking them into proprietary firmware. Enforce the existing law governing the way radios should be used instead.

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: Franco

Last Name: Lanza

Mailing Address: via 2 giugno 5/b

City: Lonate Pozzolo

Country: Italy

State or Province: Varese

ZIP/Postal Code: 21015

Email Address: franco@nexlab.it

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: giovambattista

Last Name: vieri

Mailing Address: via lucca 33

City: roma

Country: Italy

State or Province: rm

ZIP/Postal Code: 00100

Email Address:

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. To my knowledge, 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. To my knowledge, 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: Lehi

Last Name: Toskin

Mailing Address: 3671 Granite Way

City: Wellington

Country: United States

State or Province: NV

ZIP/Postal Code: 89444

Email Address:

Organization Name:

Comment: The proposed regulation would possibly make it so that it is impossible to modify router firmware. Not only is this proposed regulation overbroad, but it forces proprietary software on hardware that has efficient and popular open source alternatives in the wild already. Proprietary software is, by definition, immoral and harmful to users. If the rule is passed I would have no choice but to boycott wireless routers that make it impossible to modify the firmware.

The proposed regulation would possibly make it so that it is impossible to modify router firmware. Not only is this proposed regulation overbroad, but it forces proprietary software on hardware that has efficient and popular open source alternatives in the wild already. Proprietary software is, by definition, immoral and harmful to users. If the rule is passed I would have no choice but to boycott wireless routers that make it impossible to modify the firmware.

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: Kevin

Last Name: Kane

Mailing Address: 1800 Lincoln St

City: Hillsboro

Country: United States

State or Province: OR

ZIP/Postal Code: 97124

Email Address:

Organization Name:

Comment: User Freedom

As written, the rules and recommendations of the commission will prevent the installation of traditional free and open source wireless firmware such as OpenWrt. End-users often use such firmware because it better fits the users needs. Each user is better able to tailor the device to their needs. Users often set up a guest wireless network for their home or business, set up a web server at their home, create IoT hubs and other uses. The changes proposed will make such changes difficult and, in some cases, impossible.

Innovation

Innovation in network and wireless technology depends on the ability 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. HNCP, a proposed IETF proposed standard for managing home networks, is being developed using OpenWrt. Mesh networking technologies for developing stable distributed internet access are regularly implemented on OpenWrt 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. Without the ability to change the software on the device, these innovations would not have occurred. The innovations done by the community are later often picked up by the home router vendors and being integrated into their normal firmware versions for their next generations of devices.

Economic Impact

Millions of dollars of economic activity depend on third-party firmware. Major semiconductor and wireless hardware manufacturers use OpenWrt as the base of their router software.[1][2][3][4][5] At the same time, OpenWrt is managed and developed primarily by a community of individuals modifying their own routers and installing customized versions of OpenWrt on their own routers. Sometimes these routers originally had OpenWrt on them while others did not. Strong industry-community collaboration reduces the costs of maintenance and increases quality for manufacturers. This mutually-beneficial collaboration can only exist if users can replace their firmware on their router with a customized version of OpenWrt. By preventing firmware replacement, these regulations will strangle this community in the US thereby increasing costs to hardware manufacturers which could be passed along to customers and employees.

Guest Wifi hotspots businesses

Additionally, many companies, such as ones involved in creating open wireless networks for retail locations would be hampered by these regulations. Currently, many of these companies install custom firmware on off-the-shelf hardware. Under these regulations, such companies would have to either create their own hardware, an expensive proposition for small software businesses, or receive authorization from a manufacturer under any arbitrary terms the manufacturer so

chooses.

### Commercial VPN services businesses

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.

### Security

Restrictions on replacing router software will have a serious impact on security. Manufacturers are notoriously lax about providing timely security updates where such updates are provided at all. Security experts routinely recommend users replace manufacturer shipped router firmware with alternative community driven versions as a solution to this problem. In a recent security review of commercial routers, every one had critical security vulnerabilities. In most security instances replacing router firmware with third party peer reviewed firmware is the only option to solving this type of problem. While the security dangers for home users are serious, for large companies security dangers are critical. Without the ability to replace this software, large companies purchasing routers are entirely at the whim of the router maker. If this software is insecure, whether accidentally or intentionally, large American companies will be put at risk of industrial espionage.

### User Freedom

As written, the rules and recommendations of the commission will prevent the installation of traditional free and open source wireless firmware such as OpenWrt. End-users often use such firmware because it better fits the users needs. Each user is better able to tailor the device to their needs. Users often set up a guest wireless network for their home or business, set up a web server at their home, create IoT hubs and other uses. The changes proposed will make such changes difficult and, in some cases, impossible.

### Innovation

Innovation in network and wireless technology depends on the ability 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 was added to the Linux kernel to be used by the billions of users of Linux. HNCP, a proposed IETF proposed standard for managing home networks, is being developed using OpenWrt. Mesh networking technologies for developing stable distributed internet access are regularly implemented on OpenWrt 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. Without the ability to change the software on the device, these innovations would not have occurred. The innovations done by the community are later often picked up by the home router vendors and being integrated into their normal firmware versions for their next generations of devices.

### Economic Impact

Millions of dollars of economic activity depend on third-party firmware. Major semiconductor and wireless hardware manufacturers use OpenWrt as the base of their router software.[1][2][3][4][5] At the same time, OpenWrt is managed and developed primarily by a community of individuals modifying their own routers and installing customized versions of OpenWrt on their own routers. Sometimes these routers originally had OpenWrt on them while others did not. Strong industry-community collaboration reduces the costs of maintenance and increases quality for manufacturers. This mutually-beneficial collaboration can only exist if users can replace their firmware on their router with a customized version of OpenWrt. By preventing firmware replacement, these regulations will strangle this community in the US thereby increasing costs to hardware manufacturers which could be passed along to customers and employees.

### Guest Wifi hotspots businesses

Additionally, many companies, such as ones involved in creating open wireless networks for retail locations would be hampered by these regulations. Currently, many of these companies install custom firmware on off-the-shelf hardware. Under these regulations, such companies would have to either create their own hardware, an expensive proposition for small software businesses, or receive authorization from a manufacturer under any arbitrary terms the manufacturer so chooses.

### Commercial VPN services businesses

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.

## Security

Restrictions on replacing router software will have a serious impact on security. Manufacturers are notoriously lax about providing timely security updates where such updates are provided at all. Security experts routinely recommend users replace manufacturer shipped router firmware with alternative community driven versions as a solution to this problem. In a recent security review of commercial routers, every one had critical security vulnerabilities. In most security instances replacing router firmware with third party peer reviewed firmware is the only option to solving this type of problem. While the security dangers for home users are serious, for large companies security dangers are critical. Without the ability to replace this software, large companies purchasing routers are entirely at the whim of the router maker. If this software is insecure, whether accidentally or intentionally, large American companies will be put at risk of industrial espionage.

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: Peter

Last Name: Fales

Mailing Address: 1085 Whirlaway Ave.

City: Naperville

Country: United States

State or Province: IL

ZIP/Postal Code: 60540

Email Address: federalregister.gov@fales-lorenz.net

Organization Name: Individual

Comment: I would like to register my concern about the rule which prevent end-user modifications to the firmware of wireless routers.

First, it could be difficult to enforce, and rules which can't be enforced and encourage disregard for the law.

Second, I think it's just a bad idea. While I understand the FCCs desire to have control over emissions, I think it's better served by directly regulating the emissions, not through such indirect and (in my opinion) draconian measures as restricting changes to firmware. I would draw the analogy with automobiles: This rule is like locking the hood and only giving the manufacturer the key. There are many legitimate reasons why owners or third parties need access to the engine to fix problems, perform maintenance, add features and upgrades, etc. Some people may even do this as a hobby, but even that is a legitimate and accepted use. And, yes, there are a handful of people that make changes that violate air-quality rules. But that's why the emissions laws are in place, and people understand that violating them is illegal and can result in penalties. We go after the violators, rather than locking the hood.

I would like to register my concern about the rule which prevent end-user modifications to the firmware of wireless routers.

First, it could be difficult to enforce, and rules which can't be enforced and encourage disregard for the law.

Second, I think it's just a bad idea. While I understand the FCCs desire to have control over emissions, I think it's better served by directly regulating the emissions, not through such indirect and (in my opinion) draconian measures as restricting changes to firmware. I would draw the analogy with automobiles: This rule is like locking the hood and only giving the manufacturer the key. There are many legitimate reasons why owners or third parties need access to the engine to fix problems, perform maintenance, add features and upgrades, etc. Some people may even do this as a hobby, but even that is a legitimate and accepted use. And, yes, there are a handful of people that make changes that violate air-quality rules. But that's why the emissions laws are in place, and people understand that violating them is illegal and can result in penalties. We go after the violators, rather than locking the hood.

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: Dustin

Last Name: Chesterman

Mailing Address: 37219 2nd St

City: Fremont

Country: United States

State or Province: CA

ZIP/Postal Code: 94536

Email Address:

Organization Name:

Comment: This is an outrageous proposal that would move innovation backwards in this country at a time when global markets are already pressuring the US for dominance in technical discovery and leadership. The economic drivers of today are a direct result of the freedoms of the previous decades for entrepreneurs and corporations to experiment and improve upon previous technologies. Locking down this ability is incredibly shortsighted. I would and will contribute to any campaign against this proposal or anyone championing it.

This is an outrageous proposal that would move innovation backwards in this country at a time when global markets are already pressuring the US for dominance in technical discovery and leadership. The economic drivers of today are a direct result of the freedoms of the previous decades for entrepreneurs and corporations to experiment and improve upon previous technologies. Locking down this ability is incredibly shortsighted. I would and will contribute to any campaign against this proposal or anyone championing 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: Linas

Last Name: Vepstas

Mailing Address: 1518 Enfield Road

City: Austin

Country: United States

State or Province: TX

ZIP/Postal Code: 78703-3424

Email Address: linasvepstas@gmail.com

Organization Name: OpenCog Foundation

Comment: Modifying WiFi router firmware is a standard and necessary practice to ensure system security and protection against intruders, hackers, crackers. Commercial vendors, although well-meaning, sometimes ship products with misconfigured firmware or firmware that contains known (security) bugs. Sometimes, bugs are found only after the product has left the factory; once in the hands of customers, the vendors do not offer any sort of product recall or update policies; there is no recourse for consumers other than to install their own firmware, or file for a (wasteful) class-action suit to force the vendor to fix the issue(s).

Consumers must have the ability to perform their own firmware upgrades in order to have a reliable, secure system.

Modifying WiFi router firmware is a standard and necessary practice to ensure system security and protection against intruders, hackers, crackers. Commercial vendors, although well-meaning, sometimes ship products with misconfigured firmware or firmware that contains known (security) bugs. Sometimes, bugs are found only after the product has left the factory; once in the hands of customers, the vendors do not offer any sort of product recall or update policies; there is no recourse for consumers other than to install their own firmware, or file for a (wasteful) class-action suit to force the vendor to fix the issue(s).

Consumers must have the ability to perform their own firmware upgrades in order to have a reliable, secure system.

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: Abraham

Mailing Address: 5505 Seminary Rd #1609N

City: Falls Church

Country: United States

State or Province: VA

ZIP/Postal Code: 22041

Email Address: josh@verajosh.com

Organization Name:

Comment: Typically, after-market firmware such as the Open Source DD-WRT package and Open Source drivers in operating systems are used for one of a few purposes:

- Adding support for operating systems that would not be able to get support otherwise
- Adding networking or computation-oriented features to a device that does not have them naively
- Enabling different encryption and security features than the manufacturer provided
- Resolving problematic software issues ("bugs" after a manufacturer has stopped providing support. Since manufacturers make money from the sale and not from updates, there is a not a strong economic incentive to continue to provide updates for devices.

These activities are in the public interest. The FCC ought to protect these activities. The proposal in question would provide new restrictions on devices regulated under Part 15.

So long as Part 15 is followed (i.e. the device must accept interference and may not cause interference), there is nothing in the public interest in adding these further restrictions.

There is the argument that this sort of software may be used to increase transmission power or operate on channels other than the ones which may legally be used. Many commercially available devices will operate in some kind of "international" mode which will provide channels which are not US ISM bands and may possibly vary power levels. Banning after-market software does not prevent this risk. On balance, the burden of these new regulations far outweighs any benefit that we might see from them.

Typically, after-market firmware such as the Open Source DD-WRT package and Open Source drivers in operating systems are used for one of a few purposes:

- Adding support for operating systems that would not be able to get support otherwise
- Adding networking or computation-oriented features to a device that does not have them naively
- Enabling different encryption and security features than the manufacturer provided
- Resolving problematic software issues ("bugs" after a manufacturer has stopped providing support. Since manufacturers make money from the sale and not from updates, there is a not a strong economic incentive to continue to provide updates for devices.

These activities are in the public interest. The FCC ought to protect these activities. The proposal in question would provide new restrictions on devices regulated under Part 15.

So long as Part 15 is followed (i.e. the device must accept interference and may not cause interference), there is nothing

in the public interest in adding these further restrictions.

There is the argument that this sort of software may be used to increase transmission power or operate on channels other than the ones which may legally be used. Many commercially available devices will operate in some kind of "international" mode which will provide channels which are not US ISM bands and may possibly vary power levels. Banning after-market software does not prevent this risk. On balance, the burden of these new regulations far outweighs any benefit that we might see from them.