

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: Christopher

Last Name: Highet

Mailing Address: 4 Teakwood Ln

City: Barnegat

Country: United States

State or Province: NJ

ZIP/Postal Code: 08005-1817

Email Address: chrish78@gmail.com

Organization Name: null

Comment: Public servants of the Federal Communications Commission,

It is with great concern that I write you today regarding the latest proposal to restrict free use and research by private citizens of alternative wireless and computing systems.

The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology.

On the subject of liberty it is not at all acceptable that, given we live in a free society, our use of technology should be dependent upon federal approval of certain manufacturer's technology nor should our separate but intersecting third party devices be limited by some arbitrarily concocted regulations. It is not within the federal government's powers or mandate to codify specific software and hardware solely on the basis that it lies outside standard mainstream consumer products. Further, information security is paramount in today's world and often alternative operating systems offer a higher degree of internal systems security not found in most popular and conventional forms of consumer products. The FCC could find itself in quite a precarious position should a large number of citizens find their data in the hands of unscrupulous individuals which could have been averted were they able to use alternative technology systems but were denied due to the FCC's own regulatory measures.

Americans must also be able to secure their own data when the companies we rely on abstain from patching their own security flaws. That the FCC would be considering a proposal which could leave private citizens at the mercy of individuals operating outside the boundaries of the law is worrisome to say the least and in the past it has often been the case that privacy gaps and security flaws in wireless hardware which transmits sensitive data has been fixed as a result of the efforts of private individuals. This and many similar actions would be banned under the NPRM.

The FCC may also run afoul of the First Amendment to the Constitution by limiting those citizens who seek to use alternative methods and hardware to transmit wireless data as a matter of political principals and the desire to express political dissent through legitimate consumption practices. The NPRM would stifle this very legitimate speech, protected under the First Amendment, and may find itself on the wrong side of Constitutional Law and Supreme Court precedent.

I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

It is with great concern that I write you today regarding the latest proposal to restrict free use and research by private citizens of alternative wireless and computing systems.

The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their

own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology.

On the subject of liberty it is not at all acceptable that, given we live in a free society, our use of technology should be dependent upon federal approval of certain manufacturer's technology nor should our separate but intersecting third party devices be limited by some arbitrarily concocted regulations. It is not within the federal government's powers or mandate to codify specific software and hardware solely on the basis that it lies outside standard mainstream consumer products. Further, information security is paramount in today's world and often alternative operating systems offer a higher degree of internal systems security not found in most popular and conventional forms of consumer products. The FCC could find itself in quite a precarious position should a large number of citizens find their data in the hands of unscrupulous individuals which could have been averted were they able to use alternative technology systems but were denied due to the FCC's own regulatory measures.

Americans must also be able to secure their own data when the companies we rely on abstain from patching their own security flaws. That the FCC would be considering a proposal which could leave private citizens at the mercy of individuals operating outside the boundaries of the law is worrisome to say the least and in the past it has often been the case that privacy gaps and security flaws in wireless hardware which transmits sensitive data has been fixed as a result of the efforts of private individuals. This and many similar actions would be banned under the NPRM.

The FCC may also run afoul of the First Amendment to the Constitution by limiting those citizens who seek to use alternative methods and hardware to transmit wireless data as a matter of political principals and the desire to express political dissent through legitimate consumption practices. The NPRM would stifle this very legitimate speech, protected under the First Amendment, and may find itself on the wrong side of Constitutional Law and Supreme Court precedent.

I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely bad" category of regulatory ideas.

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: Nathan

Last Name: Reed

Mailing Address: 3505 Pleasant Ave

City: Allentown

Country: United States

State or Province: PA

ZIP/Postal Code: 18103

Email Address:

Organization Name:

Comment: These rules do not seem like a good idea. They will make it harder for Americans and others to innovate and learn about new technologies by blocking hobbyist implementations. Blocking custom router firmware and other unsigned code with access to wifi firmware will allow router companies to restrict features in their firmware without any fear of customers being able to unlock them. Overall, these rules are more restrictive on the American customer who wishes to modify and hack on their own hardware that they purchased.

These rules do not seem like a good idea. They will make it harder for Americans and others to innovate and learn about new technologies by blocking hobbyist implementations. Blocking custom router firmware and other unsigned code with access to wifi firmware will allow router companies to restrict features in their firmware without any fear of customers being able to unlock them. Overall, these rules are more restrictive on the American customer who wishes to modify and hack on their own hardware that they purchased.

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: Van Giang

Last Name: Ho

Mailing Address: 42 Fleetwood Circuit

City: Woodvale

Country: Australia

State or Province: WA

ZIP/Postal Code: 6026

Email Address: giangho@gmail.com

Organization Name:

Comment: Vote Against.

Firmware are the same as software which needs to be maintained. If there were bugs or security vulnerability discovered but not fixed it could lead to disastrous consequences.

Please don't pass this regulation. Ask instead companies to release the firmware to open source community when they no longer provide updates.

Thanks

Vote Against.

Firmware are the same as software which needs to be maintained. If there were bugs or security vulnerability discovered but not fixed it could lead to disastrous consequences.

Please don't pass this regulation. Ask instead companies to release the firmware to open source community when they no longer provide updates.

Thanks

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: Roel

Last Name: van Westerop

Mailing Address: Herman de Manlaan 6

City: Rosmalen

Country: Netherlands

State or Province: Noord-Brabant

ZIP/Postal Code: 5242CW

Email Address: rvwesterop@hotmail.com

Organization Name:

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

Additional points of emphasis:

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

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

Additional points of emphasis:

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

Last Name: Brown

Mailing Address: 100 Institute Road

City: Worcester

Country: United States

State or Province: MA

ZIP/Postal Code: 01609

Email Address: lebrown@wpi.edu

Organization Name:

Comment: Any rule that limits the software that a user can install on their own devices is at odds with preserving their freedom, and unreasonably limits innovation. Customization in software and hardware is an integral part of American innovation and ingenuity. Additionally, as most development kits are priced out of feasibility for individuals, this takes away the potential for new products to be developed.

Any rule that limits the software that a user can install on their own devices is at odds with preserving their freedom, and unreasonably limits innovation. Customization in software and hardware is an integral part of American innovation and ingenuity. Additionally, as most development kits are priced out of feasibility for individuals, this takes away the potential for new products to be developed.

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: Ernest

Mailing Address: 902 S Walden St

City: Aurora

Country: United States

State or Province: CO

ZIP/Postal Code: 80017

Email Address: null

Organization Name: null

Comment: This is a bad rule that will limit and curtail personal freedom to use enhanced functionality of many devices. Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. This ruling could open up vulnerabilities in older hardware that will likely be exploited.

This ruling will also limit what users may do with their personal devices. 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 pass this onerous legislation.

This is a bad rule that will limit and curtail personal freedom to use enhanced functionality of many devices. Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. This ruling could open up vulnerabilities in older hardware that will likely be exploited.

This ruling will also limit what users may do with their personal devices. 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 pass this onerous legislation.

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: Maximus

Last Name: Zeebra

Mailing Address: Street

City: Orlando

Country: United States

State or Province: FL

ZIP/Postal Code: 32811

Email Address: null

Organization Name: null

Comment: This is a terrible idea in practice and a step in the wrong direction. There need not be further restrictions on hardware/software, rather further loosening up in regards to installing whatever software you want, on any given piece of hardware.

This pretty much restricts everyone from installing any operating system of their choice on ANY device which have wireless. This includes ALL computer, all mobile devices and many more.

In real freedom, no hardware should come restricted with one operating system. Ideally ALL users should be presented with many options of which operating system they want to install. Such a proposal as this is draconic and pretty much buries the idea of cooperating on hardware firmware/drivers and letting the user install anything they want on top of that.

This proposal removes freedoms of the user, freedom that does not really exist very much today, but at least still is possible.

In an ideal world all electronic devices would be delivered with a single kernel, which all hardware companies worked on and integrated their drivers/firmware in. This would leave it entirely up to the user, on ANY device, which type of operating system they want to have on their device, including Android, Ios, Windows, GNU or any other system.

This is a terrible idea in practice and a step in the wrong direction. There need not be further restrictions on hardware/software, rather further loosening up in regards to installing whatever software you want, on any given piece of hardware.

This pretty much restricts everyone from installing any operating system of their choice on ANY device which have wireless. This includes ALL computer, all mobile devices and many more.

In real freedom, no hardware should come restricted with one operating system. Ideally ALL users should be presented with many options of which operating system they want to install. Such a proposal as this is draconic and pretty much buries the idea of cooperating on hardware firmware/drivers and letting the user install anything they want on top of that.

This proposal removes freedoms of the user, freedom that does not really exist very much today, but at least still is possible.

In an ideal world all electronic devices would be delivered with a single kernel, which all hardware companies worked on and integrated their drivers/firmware in. This would leave it entirely up to the user, on ANY device, which type of operating system they want to have on their device, including Android, Ios, Windows, GNU or any other 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: Josh

Last Name: Lovison

Mailing Address: 275 E Green St #1640

City: Los Angeles

Country: United States

State or Province: CA

ZIP/Postal Code: 91101

Email Address: jlovison@gmail.com

Organization Name: null

Comment: A great deal of the innovation in the software that runs on hardware with radios (routers, and especially smartphone), is very heavily influenced by open source or community driven modifications.

Heck, Apple's original AppStore was a near exact copy of the community "Installer.app" that was used on jailbroken iPhones at a time when Apple was saying that web apps were sufficient for mobile app needs.

Android is even more heavily influenced by community mods, and it is arguable that those modifications are a considerable factor in its competitive edge against Apple (many of the features unique to Android in official updates were first developed in community modifications).

So while radios being improperly used on disallowed bands, etc, is not ideal, this needs to be weighed against the extreme benefit of having a hobbiest niche doing the heavy lifting of prototyping concepts through modifications that manufactures later incorporate. Without this element, the progress of new ideas in the software space for devices with radios will slow greatly.

A great deal of the innovation in the software that runs on hardware with radios (routers, and especially smartphone), is very heavily influenced by open source or community driven modifications.

Heck, Apple's original AppStore was a near exact copy of the community "Installer.app" that was used on jailbroken iPhones at a time when Apple was saying that web apps were sufficient for mobile app needs.

Android is even more heavily influenced by community mods, and it is arguable that those modifications are a considerable factor in its competitive edge against Apple (many of the features unique to Android in official updates were first developed in community modifications).

So while radios being improperly used on disallowed bands, etc, is not ideal, this needs to be weighed against the extreme benefit of having a hobbiest niche doing the heavy lifting of prototyping concepts through modifications that manufactures later incorporate. Without this element, the progress of new ideas in the software space for devices with radios will slow greatly.

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: david

Last Name: milbut

Mailing Address: 139 shoemaker st

City: dunmore

Country: United States

State or Province: PA

ZIP/Postal Code: 18512

Email Address: aikodude@yahoo.com

Organization Name: null

Comment: NO. leave the freedom to tinker, repair and modify our bought and paid for devices alone. please stop all the meddling in the markets!

maybe you can take a year or so off from making new regulations and decide on a several hundred existing regulations that you can retire!

NO. leave the freedom to tinker, repair and modify our bought and paid for devices alone. please stop all the meddling in the markets!

maybe you can take a year or so off from making new regulations and decide on a several hundred existing regulations that you can retire!

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: Chad

Last Name: Valente

Mailing Address: 1645 East Thomas Rd.

City: Phoenix

Country: United States

State or Province: AZ

ZIP/Postal Code: 85016

Email Address: insignificantuser@gmail.com

Organization Name: null

Comment: This rule is ridiculous. I bought a thing, it should be mine to do with how I like. This is on par with being unable to do my own car maintenance or modification because the car might be used to commit a crime. I can't think of more than one way to say unnecessary governmental overreach, so instead I'm just going to copy it five times.

Unnecessary governmental overreach, unnecessary governmental overreach, unnecessary governmental overreach, unnecessary governmental overreach, unnecessary governmental overreach. Please don't do this.

This rule is ridiculous. I bought a thing, it should be mine to do with how I like. This is on par with being unable to do my own car maintenance or modification because the car might be used to commit a crime. I can't think of more than one way to say unnecessary governmental overreach, so instead I'm just going to copy it five times. Unnecessary governmental overreach, unnecessary governmental overreach, unnecessary governmental overreach, unnecessary governmental overreach, unnecessary governmental overreach. Please don't do this.

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: Anonymous

Last Name: Anonymous

Mailing Address: 15836 Strickland Ct

City: Charlotte

Country: United States

State or Province: NC

ZIP/Postal Code: 28277

Email Address: mt_xing@live.com

Organization Name: null

Comment: This is a bad idea. Please don't.

This is a bad idea. Please don't.

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: Hector

Last Name: Hernandez

Mailing Address: 409 High St SE, Apt A

City: Albuquerque

Country: United States

State or Province: NM

ZIP/Postal Code: 87102

Email Address: hectorgabehernandez@gmail.com

Organization Name: null

Comment: This is not such a good idea. Sure, Mr. Joe Consumer won't really want (or know how) to unlock their phone's bootloader to install a custom operating system. They won't really need to side-boot Linux on their Mac or PC. Sure. But this regulation would severely hurt the people who do.

There is no reason to limit this sort of customization if it doesn't hurt the manufacturer / ISP/ service provider directly or indirectly. This is a hobby for a lot of people - for others, it's a livelihood. Many people do this simply because they do not like a few aspects of a phone (whether it be jailbreaking an iPhone or rooting an Android device). This companies create their operating systems on the basis of what their market research has told them what the majority of consumers like. But that's just it; if there is a majority there will always be a minority. And that minority shouldn't suffer by having their right to tinker and customize their devices taken away. They have purchased these devices outright and should be able to customize them as they please.

This is not such a good idea. Sure, Mr. Joe Consumer won't really want (or know how) to unlock their phone's bootloader to install a custom operating system. They won't really need to side-boot Linux on their Mac or PC. Sure. But this regulation would severely hurt the people who do.

There is no reason to limit this sort of customization if it doesn't hurt the manufacturer / ISP/ service provider directly or indirectly. This is a hobby for a lot of people - for others, it's a livelihood. Many people do this simply because they do not like a few aspects of a phone (whether it be jailbreaking an iPhone or rooting an Android device). This companies create their operating systems on the basis of what their market research has told them what the majority of consumers like. But that's just it; if there is a majority there will always be a minority. And that minority shouldn't suffer by having their right to tinker and customize their devices taken away. They have purchased these devices outright and should be able to customize them as they please.

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: sean

Last Name: peat

Mailing Address: 4248 moraga st

City: san francisco

Country: United States

State or Province: CA

ZIP/Postal Code: 94122

Email Address: truks755@gmail.com

Organization Name: null

Comment: please dont allow manufacturers to lock devices and not allow modifications.

please dont allow manufacturers to lock devices and not allow modifications.

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: will

Last Name: rogers

Mailing Address: 2323 9th ave se

City: olympia

Country: United States

State or Province: WA

ZIP/Postal Code: 98502

Email Address: null

Organization Name: null

Comment: Do not lock down anything. We have a right to ownership and by that we are allowed to tinker with things we own. Don't give that right away because of fear

Do not lock down anything. We have a right to ownership and by that we are allowed to tinker with things we own. Don't give that right away because of fear

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: Anonymous

Last Name: Anonymous

Mailing Address: 1402 Holloman Dr

City: College Station

Country: United States

State or Province: TX

ZIP/Postal Code: 77845

Email Address: null

Organization Name: null

Comment: There is never a need to lock down or restrict a device. Why limit a device and its capabilities when technology is there to advance us as a society? How can we as a society advance with roadblocks we set up for ourselves. Leaving technology open source doesn't create danger or vulnerability, hindering a person and their will does.

There is never a need to lock down or restrict a device. Why limit a device and its capabilities when technology is there to advance us as a society? How can we as a society advance with roadblocks we set up for ourselves. Leaving technology open source doesn't create danger or vulnerability, hindering a person and their will does.

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: Bill

Last Name: Conn

Mailing Address: 44686 301st St

City: Volin

Country: United States

State or Province: SD

ZIP/Postal Code: 57072

Email Address: null

Organization Name: null

Comment: I understand the intentions of these proposed rules and agree that limiting devices from interfering with spectrum space they shouldn't have access to is a good thing. However requiring that devices have locked firmware will have the unacceptable affect of locking hardware owners out of controlling their own hardware. This is also a huge blow to open source software and development of open source wireless solutions. The onus of following the laws and regulations should stay on the owners of the device where it currently is. The vast majority of users aren't even going to think about flashing their firmware, only the tinkerers and enthusiasts who drive much innovation through theses open source communities attempt these sorts of things. These are people who are already familiar with the rules in place for spectrum sharing and would be at a low risk for violating them. The proposed rules for locking firmware will close down many avenues that these enthusiasts use to innovate and experiment. Please reconsider implementing the proposed firmware locking rules for Wireless Devices.

Thank you,

Bill Conn

I understand the intentions of these proposed rules and agree that limiting devices from interfering with spectrum space they shouldn't have access to is a good thing. However requiring that devices have locked firmware will have the unacceptable affect of locking hardware owners out of controlling their own hardware. This is also a huge blow to open source software and development of open source wireless solutions. The onus of following the laws and regulations should stay on the owners of the device where it currently is. The vast majority of users aren't even going to think about flashing their firmware, only the tinkerers and enthusiasts who drive much innovation through theses open source communities attempt these sorts of things. These are people who are already familiar with the rules in place for spectrum sharing and would be at a low risk for violating them. The proposed rules for locking firmware will close down many avenues that these enthusiasts use to innovate and experiment. Please reconsider implementing the proposed firmware locking rules for Wireless Devices.

Thank you,

Bill Conn

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: Anonymous

Last Name: Person

Mailing Address: 200 Campbell St.

City: Durand

Country: United States

State or Province: MI

ZIP/Postal Code: 48429

Email Address:

Organization Name: null

Comment: I would be very opposed to locking down devices with "modular wireless radios" because it takes away from the freedom of the user.

Freedom is something that is prevalent in the United States and as such, it should continue to be so, in any way shape or form. By locking down electronic devices you are taking away from the freedom of the user.

Jailbreaking or rooting is a form of expression of freedom, by locking down these devices, you are removing the ability to express that freedom. The purchaser of an electronic device should be allowed full control over their device and not be mandated to follow strict governmental guidelines pertaining to the use of the device.

On one hand, the advantage of locking down devices is that they are more secure, and are therefore less vulnerable to attack from a malicious party. On the other hand, freedom of control over electronic devices is taken away. Please do not take away our freedom. I urge you not to take action regarding this.

I would be very opposed to locking down devices with "modular wireless radios" because it takes away from the freedom of the user.

Freedom is something that is prevalent in the United States and as such, it should continue to be so, in any way shape or form. By locking down electronic devices you are taking away from the freedom of the user.

Jailbreaking or rooting is a form of expression of freedom, by locking down these devices, you are removing the ability to express that freedom. The purchaser of an electronic device should be allowed full control over their device and not be mandated to follow strict governmental guidelines pertaining to the use of the device.

On one hand, the advantage of locking down devices is that they are more secure, and are therefore less vulnerable to attack from a malicious party. On the other hand, freedom of control over electronic devices is taken away. Please do not take away our freedom. I urge you not to take action regarding this.

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: Johnathon

Last Name: Root

Mailing Address: 97 Bay State Road

City: Boston

Country: United States

State or Province: MA

ZIP/Postal Code: 02215

Email Address: johnathon.root@gmail.com

Organization Name: null

Comment: This seems overreaching and possibly illegal. Consumers should be able to modify software on the devices they purchase even if they have RF devices, especially for things like (for example) installing custom/third-party operating systems on laptops or phones. I do not support this policy and do not think it should be enacted.

This seems overreaching and possibly illegal. Consumers should be able to modify software on the devices they purchase even if they have RF devices, especially for things like (for example) installing custom/third-party operating systems on laptops or phones. I do not support this policy and do not think it should be enacted.

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: Luis

Last Name: Rodas

Mailing Address: 385 Eppd Bridge Road unit 17

City: Athens

Country: United States

State or Province: GA

ZIP/Postal Code: 30606

Email Address: LuisRRodas@gmail.com

Organization Name: null

Comment: No. I am not renting the device in question, I am purchasing it. If I want to change anything about it I should be able to. I decide that not the seller or manufacture.

No. I am not renting the device in question, I am purchasing it. If I want to change anything about it I should be able to. I decide that not the seller or manufacture.

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: Christopher

Last Name: Tang

Mailing Address: 1745 sw edgeing Dr.

City: Corvallis

Country: United States

State or Province: OR

ZIP/Postal Code: 97333

Email Address: Crazypizzak2@gmail.com

Organization Name: null

Comment: This is garbage. If I purchase a product I should be able to tweak it how I see fit. Year ago I bought a router and it functioned well for a while but began to have problems, I didn't want to shell out another 150\$ so I install dd-wrt a custom firmware. This bought my router back to life and I today I am happy with the performance. Same goes with outdated cell phones I have owned long ago, I was able to revive them by installing custom operating systems and use them long enough that the battery started to degrade. Locking down devices is a bad thing, not only is it going to upset people that like their things to be their things but it will contribute to the mind set that once something is broken you should buy a new one instead of fixing the perfectly good thing that you already have.

In this day and age a toilet with WiFi is likely to happen and I'd like to be able to unclog it regardless if I'm allowed to or not.

This ruling is garbage. Stop catering to large companies.

This is garbage. If I purchase a product I should be able to tweak it how I see fit. Year ago I bought a router and it functioned well for a while but began to have problems, I didn't want to shell out another 150\$ so I install dd-wrt a custom firmware. This bought my router back to life and I today I am happy with the performance. Same goes with outdated cell phones I have owned long ago, I was able to revive them by installing custom operating systems and use them long enough that the battery started to degrade. Locking down devices is a bad thing, not only is it going to upset people that like their things to be their things but it will contribute to the mind set that once something is broken you should buy a new one instead of fixing the perfectly good thing that you already have.

In this day and age a toilet with WiFi is likely to happen and I'd like to be able to unclog it regardless if I'm allowed to or not.

This ruling is garbage. Stop catering to large companies.

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: Darrien

Last Name: Glasser

Mailing Address: 617 Middlesex Turnpike

City: Billerica

Country: United States

State or Province: MA

ZIP/Postal Code: 01821

Email Address: darrienglasser@outlook.com

Organization Name: null

Comment: The idea of locking computers (mobile or not) down to specific and possibly proprietary operating systems is simply ridiculous. For those without the capital to afford proprietary operating systems, this makes home built computers (desktops or the like) impossible. And for those who would like to load alternative operating systems on their computer (GNU/Linux, BSD, etc.), or it is critical that they do so for their jobs, this proposal is twice as ridiculous. I'm currently typing this out right now, on my laptop, running Linux, and as a Computer Science Major (with a field eventually in the same area), it is essential that I'm able to run Linux, and other open source operating systems on my computer. Simply running the default OS would not be feasible.

Alternatively, when talking about mobile devices (e.g. smartphones, tablets, etc.), most mobile devices lose support from manufacturers after two years longest. For anybody looking to keep a mobile device for more than two years, or someone who buys a mobile device, say, a year after it is released, and then decides to keep it for two years, the ability to load third party/aftermarket OSes onto the device is very necessary, as older versions of the OS do not get security updates once the OEM stops supporting it.

Finally, putting in place such a rule would shut down projects like the Raspberry Pi (a singleboard computer that people can load any OS they want onto), which is used to teach computer science, and server fundamentals/simple programming to students and hobbyists. Such a rule would be hugely detrimental to those attempting to learn computer science on their own, and scrap many in-school projects where the learning is dependent on such devices, and their ability to load alternative operating systems on the device.

All in all, this rule is not feasible, and simply does not make sense to implement. It would disrupt far too much, with little to no gain.

The idea of locking computers (mobile or not) down to specific and possibly proprietary operating systems is simply ridiculous. For those without the capital to afford proprietary operating systems, this makes home built computers (desktops or the like) impossible. And for those who would like to load alternative operating systems on their computer (GNU/Linux, BSD, etc.), or it is critical that they do so for their jobs, this proposal is twice as ridiculous. I'm currently typing this out right now, on my laptop, running Linux, and as a Computer Science Major (with a field eventually in the same area), it is essential that I'm able to run Linux, and other open source operating systems on my computer. Simply running the default OS would not be feasible.

Alternatively, when talking about mobile devices (e.g. smartphones, tablets, etc.), most mobile devices lose support from manufacturers after two years longest. For anybody looking to keep a mobile device for more than two years, or someone who buys a mobile device, say, a year after it is released, and then decides to keep it for two years, the ability

to load third party/aftermarket OSes onto the device is very necessary, as older versions of the OS do not get security updates once the OEM stops supporting it.

Finally, putting in place such a rule would shut down projects like the Raspberry Pi (a singleboard computer that people can load any OS they want onto), which is used to teach computer science, and server fundamentals/simple programming to students and hobbyists. Such a rule would be hugely detrimental to those attempting to learn computer science on their own, and scrap many in-school projects where the learning is dependent on such devices, and their ability to load alternative operating systems on the device.

All in all, this rule is not feasible, and simply does not make sense to implement. It would disrupt far too much, with little to no gain.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: tom

Last Name: lukeywood

Mailing Address: tomlukeywood@fastmail.co.uk

City: sheffield

Country: United Kingdom

State or Province: South Yorkshire

ZIP/Postal Code: s66fb

Email Address: tomlukeywood@fastmail.co.uk

Organization Name: null

Comment: I ask the FCC to not implement these rules that would stop people from changing the software on there routers.

if people have no means of changing the firmware on there router they will be unable to fix security holes in there device when the manufacturer will not do so.

users have in the past fixed serious security bug in there wifi drivers, which would be banned under the NPRM.

taking away peoples freedom to improve there routers firmware and to use the router as they wish is completely not necessary.

if users are using there routers in ways that would have a negative impact on RF transmissions then this behavior alone should be illegal.

I ask the FCC to not implement these rules that would stop people from changing the software on there routers.

if people have no means of changing the firmware on there router they will be unable to fix security holes in there device when the manufacturer will not do so.

users have in the past fixed serious security bug in there wifi drivers, which would be banned under the NPRM.

taking away peoples freedom to improve there routers firmware and to use the router as they wish is completely not necessary.

if users are using there routers in ways that would have a negative impact on RF transmissions then this behavior alone should be illegal.

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: Cole

Last Name: Danis

Mailing Address: 13042 E 28th St

City: Tulsa

Country: United States

State or Province: OK

ZIP/Postal Code: 74134

Email Address: danis.cole@gmail.com

Organization Name: null

Comment: This is a bad idea. A HORRIBLE IDEA. There shouldn't be limitations on what I can do with a device, unless it's specifically harming the carrier in some way. I bought the device - it's mine.

As a group are literally destroying the ideas, and freedoms of the American people.

This is a bad idea. A HORRIBLE IDEA. There shouldn't be limitations on what I can do with a device, unless it's specifically harming the carrier in some way. I bought the device - it's mine.

As a group are literally destroying the ideas, and freedoms of the American people.

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: Alexandr

Last Name: Abdulov

Mailing Address: thrxdesu@gmail.com

City: Minsk

Country: Belarus

State or Province: Minsk

ZIP/Postal Code: 22017

Email Address: null

Organization Name: null

Comment: U.A.S you are crazy :/

U.A.S you are crazy :/

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: Bettke

Mailing Address: 626 Idrathernot post mystreetaddress

City: Myrtle Beach

Country: United States

State or Province: SC

ZIP/Postal Code: 29579

Email Address: null

Organization Name: null

Comment: This proposal is very concerning as it hinders my ability to explore as researcher, software engineer, and general computer enthusiast.

Vendors are already notoriously bad at providing security patches. This is why I choose to use third-party software and on occasion write my own firmware for my wireless devices.

This proposal is anti-consumer. If I buy a device I should be free to modify it as I please. If the concern is tampering that results in harmful interference, a blanket ban on software modification is overkill and inappropriate. Abuse of the spectrum is a separate matter entirely. As long as the device remains compliant and uses the wireless spectrum in an approved manner, the software running on it should be no business of the FCC or vendors.

This proposal is very concerning as it hinders my ability to explore as researcher, software engineer, and general computer enthusiast.

Vendors are already notoriously bad at providing security patches. This is why I choose to use third-party software and on occasion write my own firmware for my wireless devices.

This proposal is anti-consumer. If I buy a device I should be free to modify it as I please. If the concern is tampering that results in harmful interference, a blanket ban on software modification is overkill and inappropriate. Abuse of the spectrum is a separate matter entirely. As long as the device remains compliant and uses the wireless spectrum in an approved manner, the software running on it should be no business of the FCC or vendors.

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: Joel

Last Name: Martin

Mailing Address: 3012 Franciscan Drive

City: Arlington

Country: United States

State or Province: TX

ZIP/Postal Code: 76015

Email Address: fcc@martintribe.org

Organization Name:

Comment: Locking down WiFi access points so that only authorized firmware images can be loaded will have the effect of stifling the huge amount of innovation that happens in the custom firmware space. Open Source firmwares for wifi access points will effectively be killed due to the integrated SoC (System on a Chip) nature of most modern access point/consumer routers.

This will also effectively increase the insecurity of WiFi routers because it will not prevent motivated attackers from exploiting firmware vulnerabilities. Access point OEMs are notoriously bad about providing timely security patches. Locking down WiFi access points will not solve that problem. In fact, it will make WiFi access point security worse because users will be unable to take security into their own hands and install trusted third party open source firmware images that are kept up to date with security patches.

This will personally impact me because I always install open source firmware images on my access points so that I am able to use more powerful and secure firmware images than the OEM provides.

This proposed rule change will provide a false sense of security while taking away power from end-users and putting it into the hands of unreliable and inconsistent OEM manufacturers.

Locking down WiFi access points so that only authorized firmware images can be loaded will have the effect of stifling the huge amount of innovation that happens in the custom firmware space. Open Source firmwares for wifi access points will effectively be killed due to the integrated SoC (System on a Chip) nature of most modern access point/consumer routers.

This will also effectively increase the insecurity of WiFi routers because it will not prevent motivated attackers from exploiting firmware vulnerabilities. Access point OEMs are notoriously bad about providing timely security patches. Locking down WiFi access points will not solve that problem. In fact, it will make WiFi access point security worse because users will be unable to take security into their own hands and install trusted third party open source firmware images that are kept up to date with security patches.

This will personally impact me because I always install open source firmware images on my access points so that I am able to use more powerful and secure firmware images than the OEM provides.

This proposed rule change will provide a false sense of security while taking away power from end-users and putting it into the hands of unreliable and inconsistent OEM manufacturers.

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: Neal

Last Name: Becker

Mailing Address: 6810 Falstone Dr

City: Frederick

Country: United States

State or Province: MD

ZIP/Postal Code: 21702

Email Address: ndbecker2@gmail.com

Organization Name:

Comment: I use dd-wrt on my home routers. One reason it's vital is that this software is regularly updated with security updates. The record of OEMs providing security updates for routers after sale is dismal. The idea of an outright ban on 3rd-party router software is far too blunt an instrument for the intended purpose.

I use dd-wrt on my home routers. One reason it's vital is that this software is regularly updated with security updates. The record of OEMs providing security updates for routers after sale is dismal. The idea of an outright ban on 3rd-party router software is far too blunt an instrument for the intended purpose.

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: Paris

Last Name: Jones

Mailing Address: 707 West 21st Street

City: Austin

Country: United States

State or Province: TX

ZIP/Postal Code: 78705

Email Address:

Organization Name:

Comment: Dear FCC,

As a long time user of OpenWrt, DDWRT, Tomato, and other third-party router firmware I humbly request that you drop proposed requirements that wifi devices lock-down their firmware.

This sweeping proposal will not just affect me, but thousands of others who rely on Linux-based after-market distributions like CyanogenMod or OpenWRT. This proposal will stifle competition and remove consumer's ability to modify their own hardware.

I hope this proposal will not go through.

Thank you.

Dear FCC,

As a long time user of OpenWrt, DDWRT, Tomato, and other third-party router firmware I humbly request that you drop proposed requirements that wifi devices lock-down their firmware.

This sweeping proposal will not just affect me, but thousands of others who rely on Linux-based after-market distributions like CyanogenMod or OpenWRT. This proposal will stifle competition and remove consumer's ability to modify their own hardware.

I hope this proposal will not go through.

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: Jacob

Last Name: Carter

Mailing Address: 1337 N 1230 W

City: Orem

Country: United States

State or Province: UT

ZIP/Postal Code: 84057

Email Address: lagonium@gmail.com

Organization Name:

Comment: I express concern about the intent and results of this regulation/rulemaking. As such, I oppose its implementation/codification as presently written.

This rule appears to require some kind of lockdown on software which interfaces with a wireless radio - these radios being and becoming more prevalent in everyday items such as computers, cell phones, tablets, watches, and even shoes.

As is usually the case with rulemaking, the terms used in the text are too broad. It could be read to mean that *any* software must be locked down and irreplaceable by the end user (consumer/purchaser).

This overreach could potentially mean that a person who purchases a computer can never change the operating system it uses (could not switch from a Microsoft product to some version of BSD or Linux for example). It could also mean that someone who purchases an Android device could not install a different OS/ROM of their choice (such as AOSP or Cyanogenmod). Why could it mean these things? Because an Operating System is 'software' that can interface with a wireless radio of some kind.

I urge the FCC not to adopt this new rule, as it would:

-Eliminate the consumer/user's right/ability to repair, modify, or re-use a device for a different purpose because they would be unable to change the software running on it

-Decrease the ability of security researchers to modify devices using wireless radios for their research purposes

-Eliminate the incentive for corporations to actually issue security or other updates to their products' software, because by not issuing updates they could force people to buy new products

-Decrease faith in the United States Governmental Agencies even further, as this is an apparent overreach and (perhaps unwitting) attempt to divest the People of America of one of their inalienable rights (the right to own property and control its use)

-Decrease user/consumer faith in the devices which they use, as they could not determine whether illegal/unlawful/annoying spying is taking place upon them within the non-open-source software which runs on the vast majority of wireless devices

-Discourage innovation and technological advancement in general by negating the ability of a user/consumer to modify software on a wireless-enabled device

I express concern about the intent and results of this regulation/rulemaking. As such, I oppose its implementation/codification as presently written.

This rule appears to require some kind of lockdown on software which interfaces with a wireless radio - these radios being and becoming more prevalent in everyday items such as computers, cell phones, tablets, watches, and even shoes.

As is usually the case with rulemaking, the terms used in the text are too broad. It could be read to mean that *any* software must be locked down and irreplaceable by the end user (consumer/purchaser).

This overreach could potentially mean that a person who purchases a computer can never change the operating system it uses (could not switch from a Microsoft product to some version of BSD or Linux for example). It could also mean that someone who purchases an Android device could not install a different OS/ROM of their choice (such as AOSP or Cyanogenmod). Why could it mean these things? Because an Operating System is 'software' that can interface with a wireless radio of some kind.

I urge the FCC not to adopt this new rule, as it would:

- Eliminate the consumer/user's right/ability to repair, modify, or re-use a device for a different purpose because they would be unable to change the software running on it

- Decrease the ability of security researchers to modify devices using wireless radios for their research purposes

- Eliminate the incentive for corporations to actually issue security or other updates to their products' software, because by not issuing updates they could force people to buy new products

- Decrease faith in the United States Governmental Agencies even further, as this is an apparent overreach and (perhaps unwitting) attempt to divest the People of America of one of their inalienable rights (the right to own property and control its use)

- Decrease user/consumer faith in the devices which they use, as they could not determine whether illegal/unlawful/annoying spying is taking place upon them within the non-open-source software which runs on the vast majority of wireless devices

- Discourage innovation and technological advancement in general by negating the ability of a user/consumer to modify software on a wireless-enabled device

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: Ashok

Last Name: Rao

Mailing Address: 8818 Tallyho Trail

City: Potomac

Country: United States

State or Province: MD

ZIP/Postal Code: 20854

Email Address: ashok_rao@yahoo.com

Organization Name: Great Arbor Communications

Comment: Good Afternoon

I am the founder and President of Great Arbor Communications LLC located in Potomac, MD. We develop wireless routers for niche applications. One of our products - the GAC-252 wireless router allows users to get WiFi access with only a Dial up Internet connection. Our customers often live in parts of the country which do not have access to broadband and/or cannot afford the cost of a broadband connection. This WiFi dial up router allows them to use their smartphones, tablets, and other devices to access the Internet wirelessly. We believe we perform a valuable service for the community and our comments section on www.greatarbor.com/products.html reflects that. This low- end segment has been completely ignored by mainstream wireless router manufacturers.

As a tiny company servicing a niche market - the most effective way we could build these units was by taking COTS wireless routers and modifying the firmware with an open source Linux distribution - OpenWrt. While we only make some modifications to the IP networking layer and web interface in these router and not to the wireless portion, the underlying Linux operating system however has had to develop drivers for the wireless chips within the router. These modifications have been done by the Linux Developer community in a very responsible fashion abiding by the power emission regulations for IEEE 802.11 standard WiFi service.

Another product we offer is the Thuraya XT-Hotspot which has also been developed using the Openwrt distribution on a COTS router. This product creates a WiFi connection to Thuraya satellite data link allowing users to access the satellite data link completely wirelessly. This product has generated more than a \$100,000 in US export revenues and a significant amount of Federal and State Taxes have been incurred on sales of this product.

The new regulations being proposed by the FCC will create an enormous burden for our company. Under the rules proposed by the FCC, devices with radios may be required to prevent modifications to firmware. That means the hardware we buy will not be able to be modified and we will have to develop our own hardware and go through our own certification process. Our business cannot afford the costs and complexities associated with hardware development and certification. This will effectively kill this small business leaving thousands of current and future users without access to a WiFi Dial up connection. We also know of many small companies like Great Arbor who are using the same firmware modification procedure to create a variety of tailored products for particular market segments. The proposed regulation will stifle the innovation being created with OpenWrt and other firmware distributions around the world.

We respectfully urge the commission to not go forward with this new regulation.

Ashok Rao, Ph.D

Great Arbor Communications
Potomac, Maryland
ashok@greatarbor.com

Good Afternoon

I am the founder and President of Great Arbor Communications LLC located in Potomac, MD. We develop wireless routers for niche applications. One of our products - the GAC-252 wireless router allows users to get WiFi access with only a Dial up Internet connection. Our customers often live in parts of the country which do not have access to broadband and/or cannot afford the cost of a broadband connection. This WiFi dial up router allows them to use their smartphones, tablets, and other devices to access the Internet wirelessly. We believe we perform a valuable service for the community and our comments section on www.greatarbor.com/products.html reflects that. This low- end segment has been completely ignored by mainstream wireless router manufacturers.

As a tiny company servicing a niche market - the most effective way we could build these units was by taking COTS wireless routers and modifying the firmware with an open source Linux distribution - OpenWrt. While we only make some modifications to the IP networking layer and web interface in these router and not to the wireless portion, the underlying Linux operating system however has had to develop drivers for the wireless chips within the router. These modifications have been done by the Linux Developer community in a very responsible fashion abiding by the power emission regulations for IEEE 802.11 standard WiFi service.

Another product we offer is the Thuraya XT-Hotspot which has also been developed using the Openwrt distribution on a COTS router. This product creates a WiFi connection to Thuraya satellite data link allowing users to access the satellite data link completely wirelessly. This product has generated more than a \$100,000 in US export revenues and a significant amount of Federal and State Taxes have been incurred on sales of this product.

The new regulations being proposed by the FCC will create an enormous burden for our company. Under the rules proposed by the FCC, devices with radios may be required to prevent modifications to firmware. That means the hardware we buy will not be able to be modified and we will have to develop our own hardware and go through our own certification process. Our business cannot afford the costs and complexities associated with hardware development and certification. This will effectively kill this small business leaving thousands of current and future users without access to a WiFi Dial up connection. We also know of many small companies like Great Arbor who are using the same firmware modification procedure to create a variety of tailored products for particular market segments. The proposed regulation will stifle the innovation being created with OpenWrt and other firmware distributions around the world.

We respectfully urge the commission to not go forward with this new regulation.

Ashok Rao, Ph.D
Great Arbor Communications
Potomac, Maryland
ashok@greatarbor.com

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: Michaal

Last Name: Rutlege

Mailing Address: 5960C Mendocino Dr

City: Dallas

Country: United States

State or Province: TX

ZIP/Postal Code: 75248

Email Address: null

Organization Name: null

Comment: Requiring that all Wi-Fi routers be locked down from consumer modification prevents end users from running custom software more suited to their personal router usage. Power users, especially, benefit from the ability to extend their routers software capabilities through third-party, often open source, router firmwares. These firmwares tend to be more robust and less vulnerable than the manufacturer's own firmware, as there tends to be a more active community behind the third-party firmware. This alleviates end user frustration on missing features, convoluted configuration interfaces (which tend to be over-complicated on manufacturer firmwares) and reduced functionality. Please do not blindly enforce this policy, we end users understand your need to ensure routers are using only approved frequencies, and most of us adhere to that on our own. Do not punish us for the actions of the few who do not wish to work within reasonable guidelines and laws.

Requiring that all Wi-Fi routers be locked down from consumer modification prevents end users from running custom software more suited to their personal router usage. Power users, especially, benefit from the ability to extend their routers software capabilities through third-party, often open source, router firmwares. These firmwares tend to be more robust and less vulnerable than the manufacturer's own firmware, as there tends to be a more active community behind the third-party firmware. This alleviates end user frustration on missing features, convoluted configuration interfaces (which tend to be over-complicated on manufacturer firmwares) and reduced functionality. Please do not blindly enforce this policy, we end users understand your need to ensure routers are using only approved frequencies, and most of us adhere to that on our own. Do not punish us for the actions of the few who do not wish to work within reasonable guidelines and laws.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Eric

Last Name: Lambart

Mailing Address: N. Oatman Ave.

City: Portland

Country: United States

State or Province: OR

ZIP/Postal Code: 97217-5834

Email Address: eric-fedreg@lambart.net

Organization Name: Self

Comment: To whom it may concern:

I am writing in response to the recently proposed rules changes regarding home wireless internet ("WiFi") routers.

Firmware from router manufacturers is notoriously insecure. So much so that many security experts recommend installing third-party firmware--see:

<http://www.cnet.com/news/top-wi-fi-routers-easy-to-hack-says-study/>

A manufacturer isn't required to provide fixes to the user even if the device is found to be insecure or operating outside of authorization, so why on earth would you propose to prevent people (and businesses) from being allowed to secure their networks?

When an old router proves to be insecure or otherwise defective, "just buy a new one" is not an acceptable alternative. It makes bad economic sense, is simply wasteful, and there is obviously NO guarantee that the new hardware will be any less flawed, or in need of patching, as the hardware it was purchased to replace.

The new rule also prevents device owners from ensuring that their router is running trustworthy firmware, free of "backdoors" and other poor security practices that are well-known to plague the hardware and software industries.

With nearly all of these routers being manufactured in China, a nation known to engage in state-sponsored espionage (industrial and otherwise), it seems ludicrous to propose that US citizens and corporations be prevented from ensuring their foreign-made routers are secure enough to protect their privacy and financial details. Many responsible corporate IT departments routinely install superior firmware to help secure their networks against hostile intrusion, and this rule would explicitly ban these network-security "best practices".

It is completely unacceptable that FCC has decided to take away yet another freedom for people (and corporations) to lawfully operate the devices they own within the current (and reasonable) regulatory practices.

Please reconsider your decision.

Sincerely,

Eric Lambart

U.S. Citizen and Software Engineer

To whom it may concern:

I am writing in response to the recently proposed rules changes regarding home wireless internet ("WiFi") routers.

Firmware from router manufacturers is notoriously insecure. So much so that many security experts recommend installing third-party firmware--see:

<http://www.cnet.com/news/top-wi-fi-routers-easy-to-hack-says-study/>

A manufacturer isn't required to provide fixes to the user even if the device is found to be insecure or operating outside of authorization, so why on earth would you propose to prevent people (and businesses) from being allowed to secure their networks?

When an old router proves to be insecure or otherwise defective, "just buy a new one" is not an acceptable alternative. It makes bad economic sense, is simply wasteful, and there is obviously NO guarantee that the new hardware will be any less flawed, or in need of patching, as the hardware it was purchased to replace.

The new rule also prevents device owners from ensuring that their router is running trustworthy firmware, free of "backdoors" and other poor security practices that are well-known to plague the hardware and software industries.

With nearly all of these routers being manufactured in China, a nation known to engage in state-sponsored espionage (industrial and otherwise), it seems ludicrous to propose that US citizens and corporations be prevented from ensuring their foreign-made routers are secure enough to protect their privacy and financial details. Many responsible corporate IT departments routinely install superior firmware to help secure their networks against hostile intrusion, and this rule would explicitly ban these network-security "best practices".

It is completely unacceptable that FCC has decided to take away yet another freedom for people (and corporations) to lawfully operate the devices they own within the current (and reasonable) regulatory practices.

Please reconsider your decision.

Sincerely,
Eric Lambert
U.S. Citizen and Software Engineer

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: Maxwell

Mailing Address: 9817 Moyer Raod

City: Damascus

Country: United States

State or Province: MD

ZIP/Postal Code: 20872

Email Address: notify@weathercloset.com

Organization Name:

Comment: I would strongly urge the Commission to avoid creating a rule which will remove the ability of the end user (and owner of the device) to load software of their choosing. If it is deemed necessary to more tightly control the behavior of radios in certain spectrums, I would urge language to very narrowly define these requirements so as to preserve the rights of the end user and owner to access modify and replace the manufacturer-provided software and/or firmware. Additionally I would urge a grandfather clause to permit those using this software today to continue doing so.

To do otherwise would be to impinge on the natural right of the owners of these devices, as well as retarding the progress of these technologies, most especially in regard to cybersecurity.

I would strongly urge the Commission to avoid creating a rule which will remove the ability of the end user (and owner of the device) to load software of their choosing. If it is deemed necessary to more tightly control the behavior of radios in certain spectrums, I would urge language to very narrowly define these requirements so as to preserve the rights of the end user and owner to access modify and replace the manufacturer-provided software and/or firmware. Additionally I would urge a grandfather clause to permit those using this software today to continue doing so. To do otherwise would be to impinge on the natural right of the owners of these devices, as well as retarding the progress of these technologies, most especially in regard to cybersecurity.