

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: Troy

Last Name: Deck

Mailing Address: 1690 33rd Ave

City: San Francisco

Country: United States

State or Province: CA

ZIP/Postal Code: 94122

Email Address: troy.deque@gmail.com

Organization Name:

Comment: I would like to respectfully voice my opposition to these rules, as they limit the ability of individuals to install the software of their choosing on their own devices. This has dangerous implications as a form of regulatory capture that makes open source router software impossible.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jonathan

Last Name: Ouellet

Mailing Address: 3730 Adam app4

City: Montreal

Country: Canada

State or Province: Quebec

ZIP/Postal Code: h1w 1z4

Email Address: jonathanouellet9@gmail.com

Organization Name:

Comment: As a consumer and GNU enthousiast I think it should be everyone right to be able to modify electronic equipement they own as they please. Locking those equipements down is dangerous and irresponsable. Who says equipements I own don't contain backdoor for an hostile gouvernement to spy on me, sounds like that's what your boss is trying to accomplish FCC, make it easier for your boss (the gouvernement) to spy on me. Tryin to force me to take it and do nothing about it by changing the rules. It's not by creating regulation and rules that you will stop hackers and make the world more secure.. You will just piss them off and make them work harder.

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: Billy

Last Name: Merfeld

Mailing Address: 2707 W Harris Ave

City: San Angelo

Country: United States

State or Province: TX

ZIP/Postal Code: 76901

Email Address:

Organization Name:

Comment: Implementing this would 1) greatly reduce consumer choice in securing their wireless routers and 2) greatly decrease security.

DD-WRT has superior performance and security options compared to built in firmware for most devices. By limiting, or downright putting DD-WRT out of business, you are opening up many Americans to running old, out of date code once companies decide their device is no longer supported. That's a shame. Do not limit our choice to improve our 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: J

Last Name: King

Mailing Address: 14252 Culver Dr. A-915

City: Irvine

Country: United States

State or Province: CA

ZIP/Postal Code: 92614

Email Address: tbirdsaw@gmail.com

Organization Name:

Comment: Hello.

I respectfully request the FCC reconsider the effect this may have on the open source software that has been used to repurpose and to extend the abilities of a home wireless router.

As I understand it, while this proposal only affects the radios in the devices, the fact of the matter is that these devices are System-On-A-Chip, and therefore modifying the software of the device ALSO technically requires modifying the radio software (even if it is the same binary).

I myself prefer to only purchase devices which offer OpenWRT support, either directly or indirectly, since it gives me, the customer and the user, much more control over a device. It means that I am able to use a device to it's fullest extent, rather than what someone arbitrarily limited.

In addition, for the general public, there are security and safety concerns as well. The ability to update the software to block bugs and security holes is a vital need for these devices, and when a manufacturer decides to no longer support a device, it is on the user to take action. With this restriction, a user cannot load a third-party firmware on the device that would allow for the flaws to be repaired.

General researchers, including college students and doctorates alike, work in a field of wireless networking, helping to advance the future of the wireless network spectrum. Putting this ban in place prevents them from easily doing their work, and for a poor college student, would require a potentially prohibitive "administrative costs" to give them the ability to do their research.

I respectfully request that the above points be taken into consideration. Thank you for your time.

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: Jesse

Last Name: Sticka

Mailing Address: 17959 SW Cereghino Lane

City: Sherwood

Country: United States

State or Province: OR

ZIP/Postal Code: 97140

Email Address: jsticka@gmail.com

Organization Name:

Comment: Thank you for taking the time to read my comment. I would like to express my concern with this proposal as an avid wireless technology user. With the constant increase in technology so many of the devices you purchase today are no longer manufactured or supported within a couple years after the original purchase date, leaving them vulnerable for new attacks for the remaining life of the device. All of the routers I operate in my house are several years old and if it had not been for the work of individuals much smarter than myself, who have modified the firmware and made an alternative version. I would not be able to use these devices today without risking my entire network to an easy attack and these routers would be thrown away contributing to the growing electronic landfill.

I am a firm believer in the open source community and believe that security when left to the masses is much better than when it is kept behind closed doors and left to an individual company. Just as Unix/Linux has become the de facto standard OS for public servers on the internet I believe that the custom firmwares being produced today for wireless routers will become so much more secure and reliable than those originally released by the manufacturer that we would be putting current and future companies/governments at risk by making the modification of these firmwares illegal.

If I purchase a device I should own it and should be free to modify it as I see necessary this is especially true when it comes to securing a device. As the "Internet Of Things" is being embraced in every device in our house our wireless router is as critical to our home security as the dead bolt on our front doors and I don't want to be told I'm not allowed to install a new dead bolt that is going to keep me and my family secure.

Thanks again for taking the time to read my concerns.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jason

Last Name: Cavanaugh

Mailing Address: 4124 Warbler Dr

City: Fort Collins

Country: United States

State or Province: CO

ZIP/Postal Code: 80526

Email Address:

Organization Name:

Comment: When my Netgear WNDR-3700 router decided to stop working properly, the only available course of action aside from buying a new piece of equipment, was trying Open Source software called "dd-wrt."

A year and a half after updating my router firmware to "dd-wrt," it is still functioning properly.

As my router is a "SoC" (Silicon on Chip) device, if I was prohibited from modifying the firmware like this proposed rule would create (because the "radio" is built into the chip where the firmware resides), then I would not have a functional router and would be forced to go purchase a new piece of equipment.

Once again, the Federal Government is trying to pass rules which restrict consumer activity on devices we OWN, for what benefit? Once again the Federal Government is passing rules which have unintended consequences they don't comprehend, and one must again ask WHY?

Stay out of our business. Stop trying to police what people do with their OWN PROPERTY.

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: Vasily

Last Name: Sorry, not giving this

Mailing Address: For a reaseon, 5

City: Saint-Petersburg

Country: Russia

State or Province: Russia

ZIP/Postal Code: 190000

Email Address:

Organization Name:

Comment: Please let people run their software on their hardware. Limiting that doesn't yield much yet hinders using it for a common good and impedes the overall progress.

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: Mark

Last Name: Johnston

Mailing Address: 8644 SVL BOX

City: Victorville

Country: United States

State or Province: CA

ZIP/Postal Code: 92395

Email Address: ulatec@gmail.com

Organization Name:

Comment: There are many uses in which custom firmware is a necessary for those with knowledgeable tech backgrounds. As a user of custom router firmware, custom Android mobile firmware, and custom television firmware that all contain radios that communicate over the affected spectrum. For many such as myself, it is critical that when a manufacturer chooses to not support a device with fixes or security maintenance, that an end-user is able to modify their firmware.

The progress of wireless technologies piggybacks on researchers being able to modify hardware and software alike. Without the ability to do so will likely slow wireless innovation to an eventual halt.

Thank you for considering my situation.

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: Ryan

Last Name: Mast

Mailing Address: 9450 Gilman Drive

City: La Jolla

Country: United States

State or Province: CA

ZIP/Postal Code: 92092

Email Address:

Organization Name: University of California, San Diego

Comment: Dear FCC, please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. If the software installed on a router by the manufacturer is buggy and useless, users should be able to install Open Source firmware as a replacement that has been proven to be more reliable and secure. In addition to this, 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; so unless the FCC is planning on entering the business of fixing router firmware that manufacturers don't care about, users need the ability to fix security flaws themselves.

In addition to the ability to patch security flaws themselves, 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.

Furthermore for people in academia (and elsewhere), wireless networking research depends on the ability of researchers to investigate and modify their 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: John

Last Name: Corbett

Mailing Address: 17380 Pleasant View Ave

City: Monte Sereno

Country: United States

State or Province: CA

ZIP/Postal Code: 95030

Email Address: fccwifilockdown@pictographer.com

Organization Name:

Comment: This proposed regulation would prevent end users from defending themselves against shoddy security practices of router manufacturers. A little bit of research would reveal countless long-standing vulnerabilities in closed-source router firmware. The measures proposed here would make life easier for exploit writers because end users would not be able to switch to safer and better open source alternatives such as OpenWrt.

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: Brett

Last Name: Diercks

Mailing Address: 802 E Sunset Dr

City: Steeleville

Country: United States

State or Province: IL

ZIP/Postal Code: 62288

Email Address:

Organization Name:

Comment: This is a serious step back for what computing has given us over the years. OpenSource is the only thing people should trust. Forcing the locking down of software unviewable by the public is a violation of consumers. If a company wishes on their own means to lock down the firmware, that is their right. Consumers can decide from there whether or not to purchase from them. But to ban using Opensource on routers is a step against consumers and citizens.

OpenWRT and DD-WRT provide consumers the oppurtunity to customize their hardware to provide more functionality to limited hardware. Such as adding NAS functionality which is becoming more popular to home consumers due to less storage on more portable devices.

If this regulation goes through, it will also give a closer step into installing backdoors into our hardware which will be used to violate our freedoms and to spy on us. This is just unacceptable.

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: Purkett

Mailing Address: 805 Mesa Ct

City: Broomfield

Country: United States

State or Province: CO

ZIP/Postal Code: 80020

Email Address: andrew@purkett.com

Organization Name:

Comment: Without the ability of researchers to modify and analyze & test their devices, wireless networking would be less secure over all. Our country cannot be the last to fix security holes, which often do not come from the manufacturer's themselves, or far too long after a vulnerability is found. Under the NPRM, it will be incredibly difficult to fix serious bugs in wifi drivers, which security researchers have done in the past. If we do not have the ability to control the software on our devices, our country will lose a lot of money in commerce--Secure wifi, retail hotspot vendors, etc. will not be able to operate under these new rules. By implementing these new rules, we open up the possibility of a wave of devices which can be even more so exploited by foreign constituents, and reduce our ability to react to security and address consumer use cases which are valuable for our rapidly evolving technological marketplace.

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: Yifan

Last Name: Tian

Mailing Address: 673 E Maria Ln

City: Tempe

Country: United States

State or Province: AZ

ZIP/Postal Code: 85284

Email Address:

Organization Name:

Comment: jesus christ are you guys even trying to hide the fact that you all are fucking Nazi scum who want to control everything

I have documented what I have written here so if any of you fucks try to come arrest me I will post this shit somewhere people will see 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: Will

Last Name: Robinson

Mailing Address: 2140 E Tremont Ave APT 7C

City: Bronx

Country: United States

State or Province: NY

ZIP/Postal Code: 10462

Email Address:

Organization Name:

Comment: I strongly object to this proposal.

Please do not take away our ability to install software of our choosing on our devices. Also we need to retain the ability to fix security holes in our devices when the manufacturer fails to.

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: Maler

Mailing Address: 2630 NW 89 AVE

City: Sunrise

Country: United States

State or Province: FL

ZIP/Postal Code: 33322

Email Address: chris@thegreenman.us

Organization Name:

Comment: Please do not remove the ability for end users to install and use their own software on wifi routers. As a parent of an elementary school age child, I rely on software from third parties to supply easy-to-use, secure parental controls (dd-wrt) to my wifi router, as my internet service provider (AT&T) does not provide any content filtering or parental controls with their supplied wifi hardware. This third party software is essential in keeping my daughter safe online. Please do not remove my ability to protect my child online.

Thank you,

Christopher John Maler

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: Verdon

Mailing Address: 3921 Planeview Dr.

City: Beavercreek

Country: United States

State or Province: OH

ZIP/Postal Code: 45431

Email Address:

Organization Name:

Comment: I understand the intentions behind this suggested mandate but I have to object. Limiting what consumers can do with their own property is pretty un-American to begin with, and when it comes to wireless radio tech it unduly hinders the choices that we, the end users of these devices can make. To paraphrase Mark Twain, limiting our access to wifi firmware to try and make wifi safer is like telling a man he can't have a steak just because a baby can't chew 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: Jeremy

Last Name: Mizell

Mailing Address: 1994 S Ivory Ct

City: Aurora

Country: United States

State or Province: CO

ZIP/Postal Code: 80013

Email Address:

Organization Name:

Comment: The new proposed rules contain restrictions that could unfairly, and harmfully restrict reasonable modification of electronic devices. In its scope, it encroaches on many aspects of use, including those not normally regulated by the FCC.

Restricting the free alteration, and replacement of device firmware, imposes overly burdensome, and largely unenforceable, or impracticable restrictions. These restrictions would have many effects.

- \* Restricting wireless networking researchers, whom depend on the ability to change device firmware.
- \* Hindering open source software development, including finding and solving bugs found in vendor supplied drivers.
- \* Many secure wi-fi vendors, and custom hotspot services, depend on utilizing custom firmware to offer their services.
- \* Restrictions would likely be applied to all parts of a device, including parts of the device that are not responsible for radio control, simply because it is too costly to support two sets of device firmware.

Finally, I believe it is unnecessarily burdensome to the consumer, unfairly taking away freedoms without sufficiently justifying the loss. Many new innovations and new industries were created by users modifying, and learning from their devices. These new rules would make that difficult.

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: Zachary

Last Name: Holmes

Mailing Address: 1101 23rd Ave Se

City: Minneapolis

Country: United States

State or Province: MN

ZIP/Postal Code: 55414

Email Address:

Organization Name:

Comment: I am against making it illegal to modify radio 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: Andrew

Last Name: Boyett

Mailing Address: 750 Miller St

City: San Jose

Country: United States

State or Province: CA

ZIP/Postal Code: 95110

Email Address:

Organization Name:

Comment: I am deeply concerned by the verbage in this proposal that prohibits the modification to firmware by third-parties without going through the FCC certification process. If I interpreted the proposed changes correctly, this would end most US-based involvement in several technology communities that are responsible for a substantial amount of innovation, specifically the open-source router firmware, open-source mobile phone firmware, and software-defined radio (SDR) communities.

There has been a general trend towards more and more of the radio functionality being moved into a firmware blob loaded into the radio at runtime by the general operating system running on the device. Imposing these new limitations would likely result in most device manufacturers preventing modification/replacement of the entire device firmware, not just the radio. This requirement of signed firmware would end the ability to legally use projects like OpenWrt, CyanogenMod, and GNU-radio. The vast majority of modifications from these projects do not affect the RF transmission on the devices. Restricting the modification of the radio firmware itself makes sense, but it is unclear to me at this time whether the wording used in this proposal considers the application processor and radio(s) within a System-on-Chip (SOC) package to be separate units or one combined unit. Please expand on whether this proposal limits the modification of application processor code separate from the radio firmware code.

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: Brian

Last Name: O'Connell

Mailing Address: 1801 Tierra Libertia

City: Escondido

Country: United States

State or Province: CA

ZIP/Postal Code: 92026

Email Address: bjoconnell@gmail.com

Organization Name: none

Comment: Good People,

It is obvious that control and preservation of the RF spectrum is very important to both our economic health and our national security. But restricting a consumer's ability to load software to a router does not protect the RF spectrum in any meaningful manner, and has significant potential dangers to our economy and security.

In 1991, the Linux kernel (the 'core' to a Unix-like computer operating system) was given to the scientific and engineering community, which rapidly expanded and perfected it to spawn the many Linux distributions that fit most personal or professional use profiles. Linux and BSD variants now run the internet. for over 15 years, I have used Linux both personally and professionally. It tends to be more reliable and more secure than most commercially available computer operating systems. The same principle of robustness and security is the reason that I have chosen 'Tomatoe' firmware for my home router. The default (commercial) firmware shipped with most residential routers is seldom updated after security flaws are found, so can be a significant risk to the average home network.

It is not logical to offer solutions to non-existent problems. Alternate firmware is not the problem. The end-user loading of alternate firmware has no documented and measurable effect on preservation of RF spectrum. And if the router uses Software-Defined-Radio, the designer can still limit the hardware's frequency characteristics for the transmitter.

The economic danger to the consumer and user of routers can be significantly increased by the inability to patch faulty commercial firmware.

Respectfully Submitted,

Brian J. O'Connell

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: Mark

Last Name: Frankenfield

Mailing Address: 12018 Ghent Cr

City: Orlando

Country: United States

State or Province: FL

ZIP/Postal Code: 32825

Email Address:

Organization Name:

Comment: I don't believe this regulation is going to actually prevent the issue you are trying to prevent, especially with relation to power output.

All the end user would need to do is hookup an external amplifier to boost the signal power to the antenna.

As well, I think you will find that this will stifle the industry. Over the last 15 years, how many home and even professional routers have been sold? Millions. The cat is already out of the bag. Your only going to secure Channel and Frequency for new devices, that consumers will not want to now buy. They will continue to use older models.

Finally while your intent is only to secure the Channel and Power output, because of the state of the industry, most device now use SOC type hardware. Locking out one feature requires locking out all ability to customize the device with a third party firmware.

Honestly, this is akin to trying to Censor Pirate Radio in the 1970's.

To put it bluntly, I'm a taxpayer NOT in favor of this proposed Rule.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Karl

Last Name: Hedderich

Mailing Address: 826 Orchard Grove

City: East Liverpool

Country: United States

State or Province: OH

ZIP/Postal Code: 43920

Email Address:

Organization Name:

Comment: Please do not create any rules that would limit users from running the software of their choice on their hardware. Without this freedom our networks will become less secure, our country will become less innovative, and Americans will be less free as a 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: Edward

Last Name: Welbon

Mailing Address: 3637 Turkey Creek Drive

City: Austin

Country: United States

State or Province: TX

ZIP/Postal Code: 78730

Email Address: edward.h.welbon@gmail.com

Organization Name: None

Comment: Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. This would have many negative effects including but not limited to.

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.

In particular I am VERY opposed to any rule that would restrict installation of alternative operating systems on my PC (e.g., GNU/Linux, OpenBSD, FreeBSD, etc.). Given the realities of hardware design reuse, it will likely be impossible to simply choose a PC without a radio (so please refrain from suggesting such a mechanism as a recourse).

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: Fred

Last Name: Frazelle

Mailing Address: P. O. Box 5709

City: Calexico

Country: United States

State or Province: CA

ZIP/Postal Code: 92232

Email Address: frazelle09@gmail.com

Organization Name:

Comment: Dear FCC

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

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 your kind attention to this matter.

Respectfully,

fred frazelle

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: Derek

Last Name: Archer

Mailing Address: 641 Cottonwood Drive

City: Richland

Country: United States

State or Province: WA

ZIP/Postal Code: 99352

Email Address:

Organization Name:

Comment: I respectfully ask that the FCC not implement rules that take away the ability of users to install the software of their choosing on their computing devices for reasons which include, but are not limited to, the following:

-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. These rules would prohibit this and would therefore undermine the security of the internet at large.

-Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM, even if manufacturers choose not to fix these bugs.

-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.

-Development of mesh networking technologies which could help first responders in emergencies, also helping to provide anonymity, creating a backup/alternative communications network, will become more difficult than it needs to be with these new rules.

-Amateur radio enthusiasts, whom have helped develop new radio technologies and techniques, would find it much more difficult to conduct their investigations and research as they have done for decades in the public interest, at no cost to the American people.

-Users should be able to manipulate and control all aspects of their devices.

-Manufacturers will likely employ digital locks in the easiest manner they can rather than worrying about letting you still use your device fully to the extent of the law. This means you get locked out of other things, cannot check for back doors, etc... It's cheaper to implement a lock that encompasses the entire device rather than trying to individually lock or unlock each little line of code depending on the legalities.

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: Max

Last Name: Kalashnikov

Mailing Address: 2252 Cabrillo Ave

City: Santa Clara

Country: United States

State or Province: CA

ZIP/Postal Code: 95050

Email Address:

Organization Name:

Comment: I ask that the FCC not implement rules that take away the ability of Americans to install the software of their choosing on their computing and networking devices.

Wireless networking research depends on the ability of researchers to investigate and modify their devices. Such rules would make that effectively impossible on commercially available hardware.

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so or delays in providing a fix after the vulnerability becomes known. This situation is extremely common. End 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, depend on the ability of end users and companies to install the software of their choosing on hardware they have 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: David

Last Name: Dean

Mailing Address: PO Box 6684

City: Breckenridge

Country: United States

State or Province: CO

ZIP/Postal Code: 80424

Email Address: david@sundialcommunications.com

Organization Name: Sundial Communications, Inc.

Comment: At Sundial Communications, we use open Wi-Fi firmware to provide Internet service to thousands of subscribers. Our business and my customers rely on this firmware because it is more reliable and stable than the firmware provided by the manufacturers. By using open firmware, we have reliable and stable equipment and we don't have to constantly reboot our access points.

If you ban third-party modifications to the firmware, you will create a perverse situation whereby illegal Wi-Fi firmware will be more reliable than legal, non-modified equipment. This would be a terrible outcome for everyone and it would be counter-productive toward the goal of regulatory compliance.

Sincerely,

David Dean

Sundial Communications, Inc.

888-378-1357 x404

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: Aaron

Last Name: Messer

Mailing Address: 972 Cooperage Way

City: Vancouver

Country: Canada

State or Province: British Columbia

ZIP/Postal Code: V6B0C3

Email Address: aaronmessenger@gmail.com

Organization Name:

Comment: I urge the FCC to not implement these rules. They take away the ability of users to install the software of their choosing on their computing devices. Users should be able to install whatever operating system, software, or firmware they desire. Users and researchers must be able to investigate and modify their devices in order to fix bugs, fix security flaws, and add or change functionality.

These rules would prevent research into advanced wireless technologies, like mesh networking and bufferbloat fixes. This would infringe upon the ability of amateur radio operators to create high powered mesh networks to assist emergency personnel in a disaster.

These rules put billions of dollars of commerce at stake. Companies such as secure wifi vendors and retail hotspot vendors depend 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: Paul

Last Name: Niehuser

Mailing Address: 215 Norwich Drive

City: South San Francisco

Country: United States

State or Province: CA

ZIP/Postal Code: 94080

Email Address:

Organization Name:

Comment: Dear Sirs,

I strongly disagree with the proposed ruling.

Paul niehuser

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Matthew

Last Name: Bradley

Mailing Address: 2488 Hornsgate Dr.

City: Mississauga

Country: Canada

State or Province: Ontario

ZIP/Postal Code: L5K2C5

Email Address: matthew.bradley@ryerson.ca

Organization Name:

Comment: Greetings.

This proposed legislation violates the basic right for persons to install whatever software onto a device they own that they wish. It would be unreasonable to buy a computer, being required to never replace the operating system (especially in the case of a fault, more on that below) which is installed from the start. The scope of the proposed legislation covers not only the software directly interacting with the radio itself, but often the entire device operating system, encompassing much higher-level functionality ie. in the case of a wifi router, how firewalls are implemented and can be configured, to how network storage hosted on the device is set up. This is due to the fact that the majority of devices are implemented as a system-on-a-chip, putting the main system and it's cpu/storage on the same die as the radio. These are all functions which the end user has the right to customize to fit their needs, and are far abstracted from the radio itself, but nonetheless are swept up under the current legislation.

Furthermore, locking the firmware shipped with the device into it and disallowing changes made by the end user may prevent important (especially, but not limited to, first-party) bug-fixes and patches from being installed. This is important, especially in the field of networking (with especially strong emphasis on wireless networking) where exploits and vulnerabilities are found on a constant almost day-to-day basis, and are not just limited to higher-level software, but to lower level software that may be interacting with the radio as well. This not only leaves any users of the devices extremely vulnerable, but also may in some cases undermine the proposed legislation itself, by preventing the correction of software bugs which may have an adverse affect, in the case that the proposed legislation is proposed for the protection of the radio band(s) in question.

This situation is aggravated by both the incompetence of some manufactures, the unwillingness of others to produce patches, as well as the benefits of open source firmware. There have been numerous instances of manufactures of wireless devices including serious mistakes in their software, only to do similar-quality work when responding to faults found in their products. Manufactures may also fail to provide any support at all for a variety of reasons, including but not limited to a lost interest in the product or no interest in providing any form of meaningful support after sale. Here it should be noted, allowing the manufacturer to update their own firmware by allowing them unique access to do so is ineffective.

In these cases open source firmware, as well as closed source third-party alternatives have often been hailed as a fantastic solution, by providing patches to common/specific issues. This support is also far more up-to-date, and may extend the utility of the device by providing many new features (such as file hosting, again in the example of wifi routers). This counter-intuitively brings additional sales to manufacturers, as it brings additional value to their product at no cost. Open source firmware specifically also allows for more effective detection of bugs, and their more rapid

correction. (case in point: the open source encryption implementation openSSL contained a bug which was more quickly detected and corrected due to openSSL's open source nature than would have otherwise likely have been the case) Such firmware and its benefits to companies, users, and security as a whole would be impossible if the firmware on devices were locked-in to prevent replacement or modification.

Finally, a variety of 3rd party research, from security of the devices themselves (essential for unbiased review) to new technologies preformed by companies, institutions, and enthusiasts is only possible if the firmware in a device can be freely modified. Security experts need to be able to experiment with the firmware of a device in order to test for weaknesses and potential fixes, and the development of new technologies involving devices likewise requires the ability to modify their software.

It is important to note that advancements which do not directly involve the radio of the device are also prevented under the proposed legislation, as the devices are (as noted above) often highly integrated, featuring the main system (cpu, memory, storage, peripherals) on the same chip as the radio. One example of this is the recent discovery of wifi routers as a source of cheap 3d-printer hosts, through the installation of an open source firmware (openWRT) which allows the further installation of octoprint 3d printer host software. This use of cheap wifi routers as an affordable 3d printer host device is entirely unrelated to their possession of a radio, but would be prevented if it were made impossible to modify the device's firmware and highlights the importance of an end-user's right to use whatever firmware they choose.

-Matthew B

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: Darryl

Last Name: Quinn

Mailing Address: 5914 Pacco Ln

City: Magnolia

Country: United States

State or Province: TX

ZIP/Postal Code: 77354

Email Address: k5dlq@arrl.net

Organization Name: AREDN - Amateur Radio Emergency Data Network

Comment: I respectfully ask that the FCC not impose this rule. I am a Part97 user of these devices and regularly load open source firmware on them to facilitate emergency communications in times of infrastructure failure and disaster training. If we were prohibited from using our licensed frequencies by locking down these radios, it would be a detriment to our communities and our served agencies.

Thank you,

Darryl Quinn

K5DLQ - Extra Class Operator

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: Carlson

Mailing Address: 16095 Cleveland St

City: Redmond

Country: United States

State or Province: WA

ZIP/Postal Code: 98052

Email Address:

Organization Name:

Comment: Please see the attached file.

This rule proposal to update the certification rules of RF devices is overdue, and its goals are generally in keeping with the FCC's mandate to regulate wireless communications and prevent harmful interference. The proposal's reductions in paperwork and compliance burden are welcome.

#### 80 FR 46903 ISSUES:

Wireless devices are moving towards tighter integration, and software RF components are also increasingly closely integrated with non-RF software functionality. If these rules were to take effect as proposed, the text could be construed to broadly forbid software modification to the device, limiting user choices and preventing desirable software changes which might actually be beneficial to FCC compliance.

The requirements also impose a burden on all RF device manufacturers to provide reasonable protection against unauthorized modifications. This provision is unclear as to what would constitute a reasonable defense -- would such defenses be required to resist the use of an external programmer, or of forcibly removing memory devices from the system to modify their contents?

The requirement for disclosure of protection details might also increase the likelihood of them being compromised. Companies frequently rely on security by obscurity to hamper unauthorized modifications. Unscrupulous third parties may use certification documents to gain insight into circumventing software protections, and even long-term trade secret protection may not protect against all possible disclosures. Users would then have no legal recourse to defend against compromise if the manufacturer does not issue an authorized software remedy, which may increase the vulnerability of wireless devices to malware.

#### SUGGESTIONS:

Any mention of explicit device manufacturer protection against unauthorized software modifications in this page and 80 FR 46906 should be removed, as this issue is already addressed by the proposed 80 FR 46904. Any third party performing software modifications to wireless devices without the manufacturer's consent will incur responsibility for continued compliance under the text of 80 FR 46904. Manufacturers already have incentives to make modifications to critical parts of their system software difficult in order to increase security against malware, so removing this requirement will not lead to devices permitting sweeping changes to all aspects of their software.

This suggestion addresses all three issues above, by shifting the burden of continued compliance to the party performing the modification. Users could then continue to legally make changes that do not affect RF performance, and third party software which enables uncertified modes of operation or increases wireless interference could still be legally targeted for causing devices to operate outside of their certifications.

This suggestion would also permit hobbyists, researchers, labs, and other independent firms to continue to make limited software changes for test, research, and personal use cases as provided by the existing "not for resale" exemption, without having to manually defeat extra protections against unauthorized software. Such activities are vital for continued improvements in certified device RF performance and for educational purposes.

#### 80 FR 46906 ISSUES:

Imported wireless devices which may emit excessive interference or operate in unlicensed modes are undesirable, and importation of uncertified devices should be prohibited. However,

unauthorized or counterfeit components can slip into a supply chain from numerous sources, and not all importers or end users may be fully knowledgeable of the true source of their wireless products. As proposed, the rules might penalize buyers or resellers in the United States who unknowingly import non-compliant wireless devices.

#### SUGGESTIONS:

The proposal should explicitly state that entities accused of importing uncertified wireless devices must be proven by the preponderance of the evidence to have known that the device was non-compliant in order to be in violation. Importers or buyers who accept falsified certification information in good faith, or who receive products which differ from the advertised device in a manner which degrades wireless compliance, should be protected against receiving undue legal action.

Such issues should be taken up with the supplier who offered uncertified or counterfeit devices on the pretext of compliance. If the supplier is not under the jurisdiction of the FCC, future importation of the product in question could be prohibited until the issue is resolved.

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: Lagally

Mailing Address: 2100 NE 140th Street

City: Seattle

Country: United States

State or Province: WA

ZIP/Postal Code: 98125

Email Address: ericlagally@gmail.com

Organization Name:

Comment: The proposed rule will effectively ban the implementation of open-source software on all commercial router hardware platforms because these platforms are based on SoC platforms and it will be impossible to distinguish on a practical level between 2.4GHz systems and 5 GHz systems. While this is undeniably good for the router manufacturers, it is undeniably bad for innovation and the American economy. The U.S. prides itself on being a leader in innovation. Often this innovation arises from individuals and small companies who rapidly prototype new ideas using inexpensive commercial systems and their own open-source software solutions. Removing this capability will require these companies to invest impossibly large sums in developing their own hardware platforms or licensing same from established wireless router manufacturers. Unless a compelling argument can be made for wireless security or some other advantage, the proposed rule unnecessarily limits innovation at the expense of (often foreign) router 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: clair

Last Name: gohean

Mailing Address: 201 mary st

City: downingtown

Country: United States

State or Province: PA

ZIP/Postal Code: 19335

Email Address: cgohean@yahoo.com

Organization Name:

Comment: I would respectfully ask that this proposal not be carried out.I feel this is the most ridiculous thing I have ever heard of.This would set back technology many years and stunt the growth of open source.Unfortunately you are playing to the big corporations which run our country.We the people should have a say in this since it will effect us all.I for one if this were to pass would most likely just throw in the towel and get rid of my computers and go back to pen and paper.

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: Mark

Last Name: Tackman

Mailing Address: 6181 Fox Glen Dr

City: Saginaw

Country: United States

State or Province: MI

ZIP/Postal Code: 48638

Email Address: mt2e@Hotmail.com

Organization Name:

Comment: Open source router firmware will be killed by this proposed rule. I would like the ability to install open source software on any of my devices that I own even if it has a "radio"

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: Stephanie

Last Name: Levesque

Mailing Address: 3310 Melvin Drive

City: Wylie

Country: United States

State or Province: TX

ZIP/Postal Code: 75098

Email Address:

Organization Name:

Comment: This proposal will deter innovation in router firmware and software, and hamper educational experiences for users.

Some manufacturers are notorious for not fixing bugs in their firmware-- they leave gaping holes in it for months (In some cases, years!) and users are vulnerable to any hacker that happens to stumble upon their block. (Some of these exploits are remotely exploitable, however.)

The only way to ensure the utmost safety for consumers information and privacy is by allowing them to flash their own firmware that is regularly updated on their routers, such as LibreWRT, OpenWRT, LibreCMC, etcetera.

If this proposal is enacted, manufacturers will lock down their firmware, and make flashing alternative firmwares impossible.

Sacrificing security, privacy, and deterring innovation isn't worth solving a non-existent problem.

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: Scott

Last Name: Jordan

Mailing Address: 8302 Kalb Road

City: Henrico

Country: United States

State or Province: VA

ZIP/Postal Code: 23229

Email Address: scott@codepath.net

Organization Name:

Comment: This is totally absurd. By this logic, it would be illegal to change operating systems on my computer or change the default settings to choose a new web browser. This will be used to utterly cripple the entire computer industry.

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: da Silva

Mailing Address: PO BOX 720711

City: Houston

Country: United States

State or Province: TX

ZIP/Postal Code: 77272

Email Address: resuna@gmail.com

Organization Name:

Comment: Regarding "To minimize the potential for unauthorized modification to the software that controls the RF parameters of the device, grantees would have to implement well-defined measures to ensure that certified equipment is not capable of operating with RF-controlling software for which it has not been approved."

This, read verbatim, would seem to ban open source software for Wifi access points and routers containing Wifi access points. Given the security flaws endemic to the stock firmware in these devices, and the poor record for security updates from home/office router manufacturers, this seems to be a REALLY bad idea.

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: Kline

Mailing Address: 317 S Mulberry

City: Hagerstown

Country: United States

State or Province: MD

ZIP/Postal Code: 21740

Email Address: hippie69@gmail.com

Organization Name:

Comment: Making this ruling with harm the industry. There are times where a device is shipped with exploits, broken code, lower wifi security settings. Allowing a person to run custom firmware allows for said device to continue to function, helps prevent landfill electronics trash and offers additional functionality.

I am strongly against limiting the options a customer has once the device has been purchased. Please reconsider these regulations.

The better solution would be to request the hardware makers to lock the radio chips to whatever region they are being sold, don't like 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: Clint

Last Name: Udy

Mailing Address: 1130 E Butler Dr

City: Phoenix

Country: United States

State or Province: AZ

ZIP/Postal Code: 85020

Email Address: clint.udy@gmail.com

Organization Name:

Comment: To restrict firmware modification is absurd. This is the equivalent of telling individuals that they cannot upgrade an electronic device.

WY phone acts as a WiFi Hotspot, suddenly, I can't upgrade my operating system to the one of my choosing. My router at home has modified firmware that improves signal significantly in the environment it's in because no manufacturer can/will do it.

The firmware in a router is the operating system, and as you may recall, Microsoft attempted to prevent the installation of competitive OS and that was found to 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: Albert

Last Name: Wright

Mailing Address: 7344 Toxaway Drive

City: Knoxville

Country: United States

State or Province: TN

ZIP/Postal Code: 37909

Email Address: [ajw@toadking.org](mailto:ajw@toadking.org)

Organization Name:

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

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

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

Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the this proposal and those like it.

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: John

Last Name: Maresca

Mailing Address: 35 School Lane

City: Cherry Hill

Country: United States

State or Province: NJ

ZIP/Postal Code: 08002

Email Address:

Organization Name:

Comment: This bill is completely unenforceable. All it will do is kill business for American companies. People that want control of their devices will just buy routers from companies outside America. Furthermore, hobbyists will still build unlocked routers. This was never a problem and doesn't need regulation.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jamie

Last Name: Nadeau

Mailing Address: 293B Titanium Private

City: Ottawa

Country: Canada

State or Province: Ontario

ZIP/Postal Code: K1C 0A5

Email Address: james2432@gmail.com

Organization Name:

Comment: Please do not let this pass! People should have the ability to install the software of their choosing. 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: Paul

Last Name: Handy

Mailing Address: 310 w 2nd st n

City: middleton

Country: United States

State or Province: ID

ZIP/Postal Code: 83644

Email Address:

Organization Name:

Comment: I would like to request that you not implement these rules that take away the ability of users to install the software of their choosing to their computing devices.

Security in RF devices is considerably compromised when they are restricted to OEM software. The history of neglect in security updates and blatant malfeasant programming by companies such as Netgear and Cisco, two of the major companies in the RF space, have shown us that personal responsibility brings better security. Under NPRM, security fixes that users have done in the past would have been banned.

On top of that, wireless network research depends on the ability of researchers to investigate and modify their devices. Much of the work done in universities, and by new startups would be made highly impractical if they could not use their devices freely.

If you want to watch billions of dollars of commerce vanish, then implement this rule; because surely it will kill secure wifi vendors, as well as retail hotspot vendors. This rule speaks out to the American populous as a blatant crony attempt to consolidate the winners in the economy. If you want to show the world how corrupt your revolving-door lobbyist-to-bureaucrat system is, then by all means, implement this rule.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Russell

Last Name: Wright

Mailing Address: 7828 Winfield Drive

City: Brighton

Country: United States

State or Province: MI

ZIP/Postal Code: 48116

Email Address: rs.wright.2014@gmail.com

Organization Name:

Comment: I respectfully request that the proposed regulation "SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES" not be implemented. The ability of users / owners of equipment such as Wi-Fi routers to modify extant software or load their own software is important for the following reasons:

- 1) Ownership means the ability to modify something as the owner sees fit. The RF emissions must still adhere to FCC rules but the software should be end-user modifiable.
- 2) The ability to modify software allows the owner to add features, improve functionality, and improve security. WiFi routers are an example where users can presently load open source software which allows customization.
- 3) Research requires that individuals be permitted to investigate and modify software.
- 4) There is a history of uncovered security "holes" in WiFi routers, for example, that were discovered by researchers and fixed by individuals when manufacturers chose not to do so. This proposed rule would prevent individual users from "patching" software in equipment they already legally own.
- 5) This country has a long history of inventions coming from individual experimenters and hobbyists who examine, investigate, modify and work with new ideas that can be expressed in software and by novel uses of devices such as WiFi routers. This proposed rule would effectively end that.
- 6) Increasingly electronics are run with software that is complex and rushed to market where "bugs" become apparent. Manufacturers do not always correct the "bugs" which leaves individual users to correct these on their own. The proposed rule will prevent individuals from fixing some of the devices they own.

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: Cindy

Last Name: Moore

Mailing Address: 3340 Byron Street

City: San Diego

Country: United States

State or Province: CA

ZIP/Postal Code: 92106

Email Address:

Organization Name:

Comment: What? No. Once I have purchased a router, I have every right to alter, fix, or otherwise modify the firmware and software on it. This should not even be a question.

Very often the standard firmware and software on these devices is buggy or otherwise suspect. Installing other available replacement code onto routers, firmware access points, etc., allows me to better protect my equipment from hackers and other malicious intrusions.