

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: Andrey

Last Name: Veldyaskin

Mailing Address: Markovtceva

City: Kemerovo

Country: Russia

State or Province: Kemerovskaya obl

ZIP/Postal Code: 650003

Email Address: veldos@mail.ru

Organization Name:

Comment: Hello, I'm not agree with this document as this one restricts my rights to have the freedom to control my gadgets, computers, phones, AP, routers etc. So can't do any open projects, we can't make difference in this world, we can't make it a better place. This document brings 1984.

I'm Russian, and I know what I'm telling, my country do the same things and it's getting worse and worse!

It's not a good idea at all.

Although the FCC acts in USA, really it works all around the world.

Please don't approve the document!

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: Marchione

Mailing Address: 4819 Blackberry Way

City: Pittsburgh

Country: United States

State or Province: PA

ZIP/Postal Code: 15201

Email Address: loganmarchione@gmail.com

Organization Name:

Comment: FCC,

Please reconsider the effects this proposed rule would have. So many amazing open-source projects have sprung up in the past years, due to engineers and developers having the freedom to modify code. I completely understand your need to protect certain spectrums and frequencies, but please do not completely block the installation and modification of open-source software onto wireless devices.

To demonstrate the importance of wireless freedom, see below:

- 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.
- Mesh networking which helps first responders in emergencies, also helps provide anonymity, creates a backup/alternative communications network, will become more difficult than it needs to be with these new rules.
- 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.

As another example, consider the followings companies/projects that have grown out of the ability to modify wireless software:

-DDWRT

-OpenWrt

-Cyanogenmod

Again, I respectfully ask that you consider the repercussions of this proposed rule.

Logan

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: Regentov

Mailing Address: Kuskovskaya street 25-1-12

City: Moscow

Country: Russia

State or Province: Moscow

ZIP/Postal Code: 111141

Email Address: vasily@regentov.ru

Organization Name: Incareer LLC

Comment: I need a firmware rewrite ability for any of my devices. Too many organisations work under the US law field. So if you prevent firmware modification, you infringe on the my own rights of Russian Federation Citizen. I disagree with such 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: Keith

Last Name: Weinstock

Mailing Address: 9 Orchard St E

City: Califon

Country: United States

State or Province: NJ

ZIP/Postal Code: 07830

Email Address:

Organization Name:

Comment: It is incredibly important to have the option of installing open source firmware on our devices. It is open to ridicule, open to improvement, open to praise and transparent for all to see. Please do not block our means to 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: Adam

Last Name: Newman

Mailing Address: 1407 Bernard St

City: Denton

Country: United States

State or Province: TX

ZIP/Postal Code: 76201

Email Address: amnewman08@gmail.com

Organization Name:

Comment: As a computer/technology focused engineer, hobbyist, and American I'd encourage the FCC not to promote and manufacturer based limitation on consumer devices. Controlling our own devices is critical to experimentation and innovation. Additionally, manufacturers seldom put real effort into improving the software used in wireless networking devices beyond a product's release. Before this rule there is a strong open source effort from many Americans to take what manufacturers start with and allow many wireless network devices to evolve with additional features, security, and stability. I'd urge the FCC to promote these American's efforts instead of stop them, and not 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: Richard

Last Name: Bowers

Mailing Address: 13048 Bourne Pl

City: BRISTOW

Country: United States

State or Province: VA

ZIP/Postal Code: 20136

Email Address: richard.bowers@gmail.com

Organization Name:

Comment: I am writing to protest the implementation of your new ruleset, which appears to be designed to prevent activities that are required for research and development, to keep the internet operating in strange environments, and to provide the ability for people to learn skills inside the USA.

I work in research and development, working on projects for various clients that often require using commercial hardware as a basis due to cost rather than rolling our own software defined radio. Locking out that approach will increase the costs to our customers, which include the US Government.

Locking down firmware on consumer products does not fundamentally improve security or performance. Someone smart enough to install DD-WRT successfully on a router could just as easily wire in a new amplifier or remove shielding in a microwave, and ruin their neighbors' day. However, it does prevent people from learning how to write firmware, learning what the different components of a SoC are, or understanding how to prevent their hardware from interfering with others by allowing them to change the settings proactively.

In my home in a suburban DC metro area, I can see 7 WiFi networks. The router that's required by my provider is already locked down, and despite paying for an "advanced" router, I can't get a signal to my entire house. Commercial bridges haven't provided enough service, but a pair of ancient routers running DD-WRT are sufficient to keep my house connected. Just looking on the internet, you'll find that I'm not alone. There are a lot of people who ask questions about how to fix things in their house or place of business, and find that the only way to do it is to engineer something that does the trick.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Kevin

Last Name: Watson

Mailing Address: 60 Pleasant St Apt 407

City: Arlington

Country: United States

State or Province: MA

ZIP/Postal Code: 02476

Email Address: knw257@gmail.com

Organization Name:

Comment: Hello,

I'm writing to express my opposition to the currently proposed rule regarding RF devices. As currently proposed, the rule would prevent consumer modifications to existing RF devices, including the ubiquitous technology known colloquially as 'Wi-Fi'. These rules would prevent the customization of Wi-Fi devices such as routers, modems, smartphones, computers, and other Internet of Things devices from receiving user-created, custom software. This is problematic for a number of reasons.

First, in the current marketplace for these devices, manufacturers rarely give users the choice of software which is being run on their hardware. Teams of dedicated individuals often work very hard to create software customizations to better meet the needs of consumers. These customizations often take the form of security enhancements not yet released by manufacturers, functionality improvements and introductions, user interface enhancements and customizations, and other changes which benefit the customers. As these customizations are typically open-source, they are reviewed by a large community of users for possible security flaws and bugs - a process the manufacturers are not subject to.

Second, hotspot wifi is becoming a larger industry in this country and around the world. The ability to install custom software designed to allow Wi-Fi access without compromising network security, and possibly charging an access fee, are keystones of this. Additionally, many forms of commerce are reliant upon customization of Wi-Fi. Examples include wireless Point-of-Sale systems, inventory control systems, security camera systems and many others.

In sum, the rules as currently proposed will lead to a stifling of innovation and user choice in the technology market, and should be revised to preserve these crucial keys to the industry at large.

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: Thomas

Last Name: Ossman

Mailing Address: 33 Buckwheat Drive

City: Denver

Country: United States

State or Province: PA

ZIP/Postal Code: 17517

Email Address:

Organization Name:

Comment: Hello,

I respectfully ask that the FCC does not implement rules that take away the ability of users to install the software of their choosing on their computing devices. There are many reasons why these rules would harm both public and private entities. First, wireless networking research depends on the ability of researchers to investigate and modify their devices. Second, users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Third, 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. Finally, and most importantly, Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Cody

Last Name: Lee

Mailing Address: 731 Robert Burns Drive

City: Nashville

Country: United States

State or Province: TN

ZIP/Postal Code: 37217

Email Address: codyflee@gmail.com

Organization Name:

Comment: To Tom Wheeler and the Employees of the Federal Communications Commission, I write you today with a great amount of concern regarding the latest proposal to restrict the open and free use, implementation, and research of alternative wireless and computing systems by citizens of the United States. As someone who makes a living working in the Information Technology field, I find this extremely disturbing.

I strongly believe that the ability of all citizens alongside federally approved researchers (but not necessarily in conjunction with them) 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. Had it not been for the current liberty and freedom that we as citizens of the United States have been granted, I never would have discovered, enjoyed, and eventually found a love for these IT related things, ultimately making a career from it.

On the subject of liberty and freedom, it is not at all acceptable to live in a free society and have our use of technology 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.

Furthermore, information security is paramount in today's world and I have personally found that it is often alternative operating systems that offer a higher degree of internal systems security. This kind of security usually is 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. Being in IT, I have to make sure that my company remains compliant to multiple regulations such as HIPAA and HITECH, and that usually means implementing a fix to an issue well before a company will even acknowledge there is a problem.

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.

Ultimately, I have fully purchased the equipment and own it out right, and therefore I should be able to modify it as I see fit.

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: andrew

Last Name: hawkes

Mailing Address: Carpenters Close Wragby

City: Lincoln

Country: United Kingdom

State or Province: Lincs

ZIP/Postal Code: LN85JT

Email Address: geekyhawkes@gmail.com

Organization Name: Private

Comment: This regulation strangles the tech industry and hugely limits the development and sustainment of an open source approach to electronics. There seems to be few benefits offered by this legislation and instead it would seem to be an over reach of regulation, that has not been asked for based on any real need.

Without open source and firmware advances then we would not Linux, cyanogenmod and many other critical software applications. Being able to apply custom firmware to radio devices enhances capabilities without effecting the FCC bands/clearances reducing waste, environmental impact and also helping cash strapped companies, customers and government departments WORLD WIDE continue to function.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: William

Last Name: Cole

Mailing Address: 107 Charles St.

City: N. Cape May

Country: United States

State or Province: NJ

ZIP/Postal Code: 08204

Email Address: bcole3@comcast.net

Organization Name:

Comment: This is a terrible proposal. It reduces the creativity which stimulates 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: Kyle

Last Name: Smitz

Mailing Address: 3810 Davis Place NW #302

City: Washington

Country: United States

State or Province: DC

ZIP/Postal Code: 20007

Email Address: Kyle@Smitz.net

Organization Name:

Comment: Dear FCC,

This rule extends the "War on General Computing" discussed by Corey Doctrow in 2011 against the "Internet of Things" which is an industry that is exploding in innovation right now. This will not only take away the ability of users to modify and use their device in a way that is most appropriate to their application, but it will also destroy innovation in a blooming industry.

I can point to my own company, Smitz Laboratories as an example, as we often find ourselves modifying the software in commercial off the shelf products to facilitate the quick and cheap modifications required to produce new inventions for new products. There is already too tremendous of a burden being placed upon the owners of hardware in that in many cases, the DMCA makes it impossible to modify software to create these improvements to products. Considering to remove the ability of users to write their own software to power the hardware devices they create is cruel, unnecessary, and a self-inflicted wound that will never heal correctly.

We've already seen far too much industry damage in the DMCA in that x86-assembler, a powerful language that allows real-time debugging in a run-time environment has been almost abandoned. Because the copyright industry believed that being able to inspect your operating system in real time is "too dangerous" to the music and movie industries. This has lead to a sharp decline in the number of researchers able to detect malware, virus, and other dangerous software.

The router industry in particular has been shown to have egregious security vulnerabilities, and removing this capability from consumers will for example freeze the efforts of thousands of innovative minds in examining BIOS software for wifi devices and discovering vulnerabilities. Mind you, it won't stop the cyber criminals.. it will only stop the hobbyist developers that fuel innovation in the modern economy.

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: Korey

Last Name: Ingersoll

Mailing Address: 2634 William Short Cir Apt 400

City: Herndon

Country: United States

State or Province: VA

ZIP/Postal Code: 20171-4465

Email Address:

Organization Name:

Comment: 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.

Do not take our freedom!

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: Chris

Last Name: Blatchley

Mailing Address: 94 Boston Ave, Apt 1

City: Medford

Country: United States

State or Province: MA

ZIP/Postal Code: 02155

Email Address: chris@chrisblatchley.com

Organization Name:

Comment: This is an unnecessary closing of an otherwise good and extremely useful ecosystem of open source software. This will also in all likelihood pose a major security threat not being able to ship security updates, and only makes internet infrastructure less secure. I oppose this proposal and look forward to a continuing thriving of open source software in radio attached hardware.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Todd

Last Name: Smith

Mailing Address: 110 Scott Acres

City: Scott Depot

Country: United States

State or Province: WV

ZIP/Postal Code: 25560

Email Address: todd.smith@camc.org

Organization Name:

Comment: The ability to modify equipment has been upheld by the FCC numerous times. Why would you suddenly invalidate previous rulings? Replacing firmware on phones; routers and other communication equipment to support after a vendor stops is a necessary component to preserving the economy.

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: Thomas

Last Name: Holbrook II

Mailing Address: 708 N Warren St

City: Warrensburg

Country: United States

State or Province: MO

ZIP/Postal Code: 64093

Email Address: thenixedreport@gmail.com

Organization Name:

Comment: I am writing today to say that I do not support the proposed rules that would require manufacturers to lock down any device that has a modular wireless radio. While security is understandable, these proposed rules would also prevent the following:

- 1.) Wireless networking research for the purpose of improving related technologies.
- 2.) The ability for individuals to fix security holes in their devices when manufacturers refuse to do so.
- 3.) The ability for individuals to write wifi device drivers for improved performance and better security.
- 4.) Billions of dollars of commerce from vendors of secure wifi and retail hotspots as a result of installing custom firmware on devices of their choosing.

Furthermore, this could pose problems for individuals who wish to run operating systems other than Microsoft Windows or Apple OS X on their desktop and mobile computers as they often have modular wireless radios installed in order to connect to wireless networks.

Please do not implement these rules as you could render numerous business owners criminals, which would be devastating to our economy. 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: Nathan

Last Name: Bohman

Mailing Address: 2845 S 800 E

City: Salt Lake City

Country: United States

State or Province: UT

ZIP/Postal Code: 84106

Email Address: natrinicle@gmail.com

Organization Name:

Comment: Dear FCC,

A regulation such as the one proposed would be a major step backwards for wireless research, repair/replacement of faulty device software, and the general nature of open source software. Many people depend on developers writing software to fix and improve devices after manufacturers release hardware with buggy software and do nothing to improve it over time. Prohibiting modification of devices with wireless cards would prevent a lot of research into new wireless technologies and would increase e-waste as consumers had no choice but to upgrade their hardware instead of upgrading the software running on it. Please don't hurt innovation and increase e-waste in an attempt to stop others from breaking current regulations.

Sincerely,

Nathan Bohman

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: frank

Last Name: Lukey

Mailing Address: lukey@willowhouse5.freemove.co.uk

City: Sheffield

Country: United Kingdom

State or Province: South Yorkshire

ZIP/Postal Code: S36 6BR

Email Address:

Organization Name:

Comment: I object because:

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

people 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: Peter

Last Name: Johnson

Mailing Address: 826 Western Dr.

City: Santa Cruz

Country: United States

State or Province: CA

ZIP/Postal Code: 95060

Email Address: pete@coho.org

Organization Name: Beyond Circuits

Comment: I 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. Reasons for this include, but are 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.

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: Douglas

Last Name: Neary

Mailing Address: 2130 Oliver Ave

City: San Diego

Country: United States

State or Province: CA

ZIP/Postal Code: 92109

Email Address:

Organization Name:

Comment: Please do not implement this rule.

It is vital that I am able to install software on any device I purchase. I have to be able to install 3rd party software to fix security holes that manufacturers of devices either cannot or will not fix in a timely fashion.

Home routers are a prime example of a device where manufacturers produce an insecure product and refuse to update/fix their firmware. Without such 3rd party firmware providers such as dd-wrt, tomato, and open wrt, I would be stuck with an insecure router and no way to fix the router. This could lead to my entire home network being compromised.

Keep the Internet secure. Don't 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: Eric

Last Name: Donahue

Mailing Address: 165 Cherry Ln

City: Ingleside

Country: United States

State or Province: IL

ZIP/Postal Code: 60041

Email Address:

Organization Name:

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.

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: aleksei

Last Name: kkkk

Mailing Address: estonia, tallinn,kopli str 33

City: tallinn

Country: Estonia

State or Province: harjumaa

ZIP/Postal Code: 10113

Email Address: niemi@solo.ee

Organization Name:

Comment: why I can't use my router with alternative 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: Benjamin

Last Name: Rayfield

Mailing Address: 1141 Hardin Rd, Dallas, NC 28034

City: Dallas

Country: United States

State or Province: NC

ZIP/Postal Code: 28034

Email Address: ben@humanai.net

Organization Name:

Comment: Could this interfere with the normal operation of "UDP hole punching" and other workarounds for directly sending and receiving messages between NAT addresses?

Most people have NAT addresses, and many high performance kinds of computing and streaming depend on their ability to communicate directly instead of going through the client/server paradigm.

Its not something NATs were designed to do, but NATs were not something IPv4 was designed to do. Its layers upon layers of workarounds. If you're planning on enforcing some kind of identifying through network connections, then these workarounds would no longer work.

https://en.wikipedia.org/wiki/UDP_hole_punching

https://en.wikipedia.org/wiki/Network_address_translation

Would it still be legal to operate grids of opensource hardware across large distance which are not obligated to any specific certificate authority or group of them chosen by anyone?

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: Elija

Last Name: Hart

Mailing Address: 2870 E College Ave #305

City: Boulder

Country: United States

State or Province: CO

ZIP/Postal Code: 80303

Email Address: hartz@gmail.com

Organization Name:

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. Americans must also be able to secure their own data when the companies we rely on abstain from patching their own security flaws. It is often the case that privacy gaps and security flaws in wireless hardware which transmits sensitive data are fixed as a result of the efforts of private individuals. It is troubling that the FCC is considering a proposal which leaves citizens at the mercy of manufacturers who often demonstrate an unwillingness or inability to secure their customers' data.

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 rejecting this measure.

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: Christie

Mailing Address: 11865 Calhan Hwy

City: Calhan

Country: United States

State or Province: CO

ZIP/Postal Code: 80808

Email Address: brianc1969@yahoo.com

Organization Name:

Comment: To Whom it may concern:

I would respectfully ask that you not implement the rules which 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 the researchers to modify the software running on their test devices. This rule would prevent the research needed to ensure overall wireless networking security.

Additionally, without the ability to replace firmware on wifi routers, users are at the mercy of manufacturers to update the devices with security patches. I understand not all, probably even most, users will install 3rd party firmware on such devices, but there are a good number of us who do, because we care about the security of our networks.

Sincerely,

Brian Christie

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: Hodge

Mailing Address: 11A McCarran Blvd

City: Las Vegas

Country: United States

State or Province: NV

ZIP/Postal Code: 89115

Email Address: afdozerman@gmail.com

Organization Name: United States Air Force

Comment: It has been brought to my attention that rules are being considered in the rewrite of the FCC's guidance on "modular radios" such as those in cell phones and laptops that would severely limit or completely negate the ability of the end user to alter the firmware (or otherwise alter the function of the transmitter) in any way, due to the legal necessitation of the company that produced the product to "lock down" the modular radio chip. I, along with many others like me, find this abhorrent at best.

There are many of us in the technology sector who believe that a device, once bought, belongs to the user to use as they see fit, in the spirit of the freedoms put forth by our founding fathers. A large, central part of this belief is the belief that the user has the right to run alternative software on said device and the right to view the "source code" of any software associated with it. This right is also a national security interest, in that it allows trained professionals to audit code for cybersecurity threats otherwise kept hidden. In addition, "locking down" modular radios

- A) Restricts the ability to install alternative operating systems on a personal computer, such as GNU/Linux, OpenBSD, FreeBSD, etc.
- B) Prevents research into advanced wireless technologies, ie. mesh networking and bufferbloat fixes
- C) Bans installation of custom firmwares on Android smartphones and other mobile platforms
- D) Discourages the development of alternative free and open source WiFi firmware, to include OpenWrt
- E) Infringes upon the ability of amateur radio operators to create high powered mesh networks to assist emergency personnel in a disaster, such as those who carried ever-important messages for the victims of Hurricane Katrina to their families
- F) Prevents resellers from installing firmware on routers, such as for retail WiFi hotspots or VPNs without agreeing to any condition a manufacturer so chooses.

In the spirit of a free America and for software freedom everywhere, I will be paying close attention to the politicians who vote in accordance with these views and will encourage may others to vote as I have.

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: Hudson

Mailing Address: 1300 S Pleasant Valley

City: Austin

Country: United States

State or Province: TX

ZIP/Postal Code: 78741

Email Address: scott.w.hudson@gmail.com

Organization Name:

Comment: If enacted, this will prevent companies and end-users from being able to push software updates to wireless access points whenever bugs or vulnerabilities are discovered, which creates serious security issues for all parties involved, including the government.

It's very understandable that the government wants to take steps to be able to more effectively monitor traffic and cut down on potential obstacles in the process, but this is a misguided effort that was clearly conceived without the help or guidance of the tech industry and threatens not only US commerce, but everyone's security. As a tech professional and software engineer, it alarms me that such proposals are becoming so commonplace in our society.

Imagine Cisco discovers a vulnerability, (or better yet, someone outside of the company discovers one.) Hopefully, this person would alert the proper parties of the issue, who would then need to issue a software update to fix the problem. This proposal would not only slow down the process of being able to implement a fix, it would completely de-incentivize users from doing so. And this impacts you too. If my 35-person company can't secure our network from an unforeseen vulnerability, then what makes me believe that you guys, a ~2.8 million strong entity with a horrendous record of security (see OPM hack) will benefit from such outrageous legislation as well?

This will completely destabilize our nation's IT infrastructure in ways that none of us can fathom, and thus will only make it easier for those who seek to commit cyber crimes. This proposal will be easier to penetrate networks, mask identities through rogue proxies, and grant wider network access to an already-weakened infrastructure.

Please listen to the tech industry and do not go through with this. It doesn't just hurt us, it hurts you just as much. The only difference is that we as tech professionals can fathom the possibilities of this legislation, and the Feds don't seem to be able to. Trust your citizens, we are not your enemies.

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: Chin

Mailing Address: 1961 Wolfsnare Road

City: Virginia Beach

Country: United States

State or Province: VA

ZIP/Postal Code: 23454

Email Address:

Organization Name:

Comment: Thank you for allowing my comments to be heard. Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Wireless networking research depends on the ability of researchers to investigate and modify their devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Eirik

Last Name: Falck

Mailing Address: Norge

City: Oslo

Country: Norway

State or Province: Oslo

ZIP/Postal Code: 1234

Email Address:

Organization Name:

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.

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: Cox

Mailing Address: 3350 harrison st. Apt 239

City: kingman

Country: United States

State or Province: AZ

ZIP/Postal Code: 86409

Email Address: russ10cox@gmail.com

Organization Name:

Comment: I would just comment that security should be in place such that "..radios operating in these bands cannot be modified." should be modified to "..radios operating in these band cannot be modified without the consent of the owner of the radio...". To say otherwise would sound like the FCC is telling the owners that they cannot modify there own equipment, even if the equipment would still meet all other emission regulations. This would in effect make innovation 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: Justin

Last Name: Warrick

Mailing Address: 1509 Osage Dr

City: North Little Rock

Country: United States

State or Province: AR

ZIP/Postal Code: 72116

Email Address: Jacw20@hotmail.com

Organization Name: National Guard Bureau IT Training Center

Comment: I am concerned that the administrative burden for 3rd party modifications to an existing device by requiring a new FCC ID will hinder hobbyist modifications to fix documented issues with routers and other devices when the original vendor fails to timely update the firmware in the device or the device is out of the normal lifecycle. An example of this would be the DD-WRT firmware that improves the management of traffic and signal broadcast/reception in some routers.

Reference:

39. The Commission proposed, for certified device operating under all rule parts, to require that any party making changes without the authorization of the original grantee of certification must obtain a new grant of certification and a new FCC ID.

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: Collier

Mailing Address: 1329 Carlisle Avenue

City: Dayton

Country: United States

State or Province: OH

ZIP/Postal Code: 45420

Email Address: jqcollier@gmail.com

Organization Name:

Comment: Open source firmware has been the foundation for a number of innovations, such as Arduino, Raspberry Pi, and DD-WRT. Removing the ability to create new functionality will stifle American development and innovation. Other nations will begin to take the lead in new advancements in technology, as some already have. Additionally, this regulation could have an adverse impact on U.S. tech companies, like Juniper Networks, Buffalo Technologies, and pfSense, when developers look to more development friendly devices outside the U.S.

In order to keep tech innovation thriving in the U.S., please vote against this regulation.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Mark

Last Name: Komarinski

Mailing Address: 45 Ridgeway Ave

City: Billerica

Country: United States

State or Province: MA

ZIP/Postal Code: 01821

Email Address: mkomarinski@wayga.org

Organization Name:

Comment: While understanding the requirements that devices need to operate in the allotted spectrum, locking out third party firmware is counterproductive. Adding third party firmware such as DD-WRT or OpenWRT extends the capability of the devices by adding in functions not identified by the OEM but generally not impacting the frequencies the device operates on. For example, adding in VPN endpoints or acting as a web server. Placing limits within the radio firmware (rather than the SoC firmware - see Android-based cell phones) seems to be a better way of accomplishing this goal while giving maximum flexibility to consumers.

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: Whitehouse

Mailing Address: 1025 Valleyview Drive

City: Marion

Country: United States

State or Province: IA

ZIP/Postal Code: 52302

Email Address: transaction@joelwhitehouse.com

Organization Name:

Comment: In response to 80 FR 46922, I propose striking paragraph (e).

I am an embedded developer and security researcher with more than a decade of industry experience. I oppose requirements to prevent upgrades to the firmware of any component, including the SDR implementation of consumer and commercial hardware.

In his lecture "Cybersecurity as Realpolitik" given to Black Hat USA 2014, Dan Geer described a present reality in which the security of typical consumer network device has an expiration date. Because the firmware implementations are non-trivial, exploits will inevitably be found in them. Once an exploit is found, if the vulnerable device cannot be upgraded, the only defense against the exploit is to discard the device itself. Restricting embedded device owners in any way from upgrading their device firmware leaves them vulnerable to attacks and puts American information at risk.

The FCC is interested in regulating output waveforms and RF power levels, not the main system firmware that savvy consumers are familiar with configuring or replacing. I am aware the SDR implementation which generates waveforms is usually separate from the main system firmware and can be secured separately. However the baseband RF processor is still critical to the security of the device; minute errors in the transmitter implementation may leave a device vulnerable to side channel analysis such as timing attacks. Errors in the receiver implementation may allow an attacker to take complete control of the system by using a specially crafted transmission. The RF processor MUST be re-programmable for a device to be defensible.

Furthermore, the RF processor must be re-programmable even if the new firmware isn't signed by the device's OEM. Firmware packages such as OpenWRT have shown that after-market implementations are often better secured than OEM firmware. Restricting consumers to using only vendor published firmware often means there are no updates available at all. Any restriction on firmware updating will leave some device owners vulnerable.

The devices affected by these rules are hopefully not used to directly protect National Security. But much of America's intellectual property flows over simple home wifi routers every day. It is untenable to leave millions of American consumers defenseless against these kinds of attacks. Please striking paragraph (e) and avoid weakening the United State's network infrastructure security.

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: McCormick

Mailing Address: 1352 11th Ave Apt 1

City: San Francisco

Country: United States

State or Province: CA

ZIP/Postal Code: 94122

Email Address:

Organization Name:

Comment: I am commenting 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. 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, and retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

The FCC regulatory interest in this matter appears to arise from concerns that radio emissions may be altered in some devices through these types of software i.e., users may increase the transmit power of a WiFi router above an allowed threshold. I would suggest that (a) this is in point of fact very rarely done by users of this kind of software, and is not a driving reason that people wish to modify their software, and that (b) the FCC would be hard pressed to find enough concrete examples of any unwanted interference arising from this type of activity to justify this sweeping regulation, that far exceeds the minimum requirement to limit transmit power thresholds, and greatly impinges on many other important, unrelated rights and activities.

Thank you very much for taking the time to consider this comment.

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: Bert

Last Name: Nielson

Mailing Address: 2432 Woodhill Court

City: Crescent Springs

Country: United States

State or Province: KY

ZIP/Postal Code: 41017

Email Address:

Organization Name:

Comment: While it is a challenge for the FCC to implement changes to accommodate the changing nature of how devices are added to the wireless spectrum, the measures to ensure that SDR radio devices are unable to be modified seems heavy handed and of negative benefit to the end user.

It is no secret that manufacturing is driven by a need to create new and better products, however, in this effort, small, inexpensive devices are released and forgotten. Already there are millions of cell phones unable to run official software because manufacturers have decided that they were no longer worth supporting. In many of these cases, it has been the end user community that has engaged in patching, fixing and porting the necessary software.

Software, by it's very complexity, has bugs. Software defined radios are no exception. Worse, by implementing paper regulations, we place the entire onus on fixing these bugs in the hands of the manufacturer who has little financial incentive to patch. Why should a company patch, when it could release new hardware that fixes the problem and require their customers to buy the new version to get the problem fixed.

There has been significant innovation as a result of SDR devices. Whether it's tracking satellites and the ISS or inventing new modes of communication, it's all been possible through the plethora of inexpensive system on chip devices. This level of innovation allows for new and creative use of the radio spectrum and is an integral part of the function of the FCC.

I believe that the rules outlined in the NPRM do not sufficiently address the problem of keeping the spectrum protected yet allowing the innovation and protection afforded by third parties in SDR 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: Charles

Last Name: Bullock

Mailing Address: 42 Fayette St.

City: Cambridge

Country: United States

State or Province: MA

ZIP/Postal Code: 02139-1112

Email Address:

Organization Name:

Comment: Please do not implement any rules that prevent me from installing alternative software on devices with wireless capability. I've been doing exactly that for nearly a decade now, with wireless routers and old smartphones, in order to extend their useful life and make them more functional. The manufacturers of such devices might make a good product initially, but they stop offering new software packages within a year or two, and then your device just slowly slips behind the march of technology.

I've used open wireless router firmwares such as DD-WRT and OpenWRT to dramatically improve the functionality of my personal devices rather; I've used third-party Android firmwares to keep an older smartphone running faster and with more usability after the OEM decided it wasn't cost-effective to push out new operating system upgrades. In both cases, a major bonus of the third-party firmwares was the incorporation of all the security patches and bug fixes that had been found since the last official update; installing third-party software for my wireless devices makes them more secure, too.

As I read it, the proposed rule here will make it illegal for me to patch and update my personal devices after their support period from the manufacturer has long ended. In the end, this makes my life as a private citizen more difficult and costs me substantially more money, and it isn't looking like I benefit at all. Please reconsider this rule, or modify it to leave exceptions for everyone out there who wants to keep their hard-purchased devices running.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: William

Last Name: Millard

Mailing Address: 1511 Artesia Blvd, Unit 4

City: Manhattan Beach

Country: United States

State or Province: CA

ZIP/Postal Code: 90266

Email Address: william.millard@cox.net

Organization Name:

Comment: Hello Federal Communications Commission,

I respectfully request that the FCC refrain from creating rules that restrict the ability of users to modify the software on their own devices. This is a comment concerning Notice of Proposed Rule Making, ET Docket No. 15-170, FCC 15-92, 80 FR 46900.

Wireless networking research depends on the ability of researchers to investigate and modify their devices. As an example: under NPRM, I could not have finished my senior project (the concluding project for my computer science curriculum at Cal Poly San Luis Obispo). These modifications are seldom permanent, and are experimental by nature. Even if some illegal broadcasting takes place, it would likely be accidental or for a very brief period of time.

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. After the Heartbleed exploit was published, I updated all my devices that interacted with the outside world. We live in a society where cell phone companies drag their feet to push security updates to old phones. Under NPRM, those unlucky enough to have old tech will be abandoned by the fickle support of the device manufacturers. They will be left with no legal way to protect themselves.

Users in the past have fixed serious bugs in their Wi-Fi drivers. This practice would be banned under NPRM. For an example comparing Wi-Fi devices with an open philosophy versus a closed one, look no further than OpenWRT. The project is much more stable/performant on Atheros chipsets, as opposed to Broadcom (which refuses to release specs to aide in development). As a result of being more open, the Atheros chipsets perform faster and with more stability. Under NPRM, there is no option but to wait for updates from manufacturers (which may or may not happen, if the hardware is old).

Billions of dollars of commerce, such as secure Wi-Fi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing. Chilispot and Sputnik are services that were born out of necessity to provide a public service to a small group. These services exist to assist internet cafes, hotels, and hostels with managing their wireless internet. NPRM would cripple further innovation in these enterprises, and compromise the security of any surviving products.

If this proposal exists out of fear of the public running wireless devices unlawfully, consider this: in the OpenWRT project, by design, it is very difficult and risky to modify the device firmware to violate region restrictions (IE: channel limitations and transmission power restrictions). In order to succeed, a person needs to edit a binary file in flash memory. If that edit fails, the router is effectively bricked.

Oftentimes, firmware UI allows unlawful selections that are unaffected by region codes. Despite the unlawful selections, they are not used. Many firmware blobs operate silently on the restrictions of a set region code, or a conservative world code, unbeknownst to the user. Intentionally operating wireless devices with no restrictions is difficult to do, and as seen with the consequences described above risky.

NPRM's restrictions will hurt education, innovation, and security. It will make it more difficult for scientists to experiment (legally) on the forefront of wireless tech. It will discourage development and change outside the established wireless tech giants (hurting competition). And, finally, it will compromise our ability to take charge of our own security.

All this to restrict the actions of a small law-breaking minority.

The trade-offs that will result from NPRM are unacceptable. We are already under fire from electronic threats both foreign and domestic. In the best case, making wireless technology more obscure will have no effect on its security. In the worst case, NPRM will allow damaging exploits to remain hidden - possibly, until device end-of-life.

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: Austin

Last Name: Miller

Mailing Address: 809 North Drive

City: Copperas Cove

Country: United States

State or Province: TX

ZIP/Postal Code: 76522

Email Address: volker_muller55@yahoo.com

Organization Name: Me

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

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

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

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

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

Mesh networking which helps first responders in emergencies, also helps provide anonymity, creates a backup/alternative communications network, will become more difficult than it needs to be with these new rules.

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

Manufactures 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: Oleg

Last Name: Dozorov

Mailing Address: Novoyasenevskiy prospekt 5/1, Moscow, Russia

City: Moscow

Country: Russia

State or Province: Moscow District

ZIP/Postal Code: 117588

Email Address: fernitoid@ya.ru

Organization Name:

Comment: Greetings from nowhere, FCC.

You all know what a computing community is. You all know what a computer is.

Please do not forget that a computer and any microprocessor electronic devices were made to work with a custom program. Programming makes computing devices what we used to know them since Babbage and Lovelace. An microprocessor device without programming capability is a great waste of energy, nothing more.

Please remember this every time you decide to change something in the world of FCC controlled equipment. Please stay honest!

Wishing you a nice online.

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: Iain

Last Name: Brearton

Mailing Address: 608 S State St

City: Champaign

Country: United States

State or Province: IL

ZIP/Postal Code: 61820

Email Address: brearto2@illinois.edu

Organization Name:

Comment: While I understand the desire to reduce likelihood of harmful radiation to users, I do not agree that removing the ability of the user to modify the device's wireless firmware is an acceptable solution. More specifically, I am referring to paragraph 80 FR 46920, at this link: <http://www.federalregister.gov/a/2015-18402/p-289>

The proposed solution restricts research into wireless technologies at an academic level, which I propose is desirable for the present and future improvement of WiFi and other protocols. By disallowing the modification of WiFi chips to use experimental software. Such experimental software would be needed to allow research technologies like mesh networking, ambient backscatter, and bufferfloat fixes at a reasonable cost. After searching for the terms related to security, education, and experimentation in the proposed rule, it does not seem like there will be an exception to locking down chipset firmware for research/experimental devices, a fundamental problem if research into RF communication is to continue.

The proposed rule also has economic implications. Manufacturers of WiFi chipsets would gain the power to restrict who used their WiFi chipsets for various applications, such as retail WiFi hotspots or VPNs, since these applications require a finer amount of control than standard WiFi devices and thus some level of custom software. If the designer of the application is reliant on a manufacturer when designing such applications, the chipset manufacturer could misuse their position of power to force agreement to arbitrary terms. Consumers of affected devices are also impacted. Devices that restrict all software modifications in order to ease compliance with this proposed rule (as the manufacturers are economically motivated to do) would restrict the consumer's freedom to install software of their choice on hardware they own, which has not previously been restricted to this extent.

The proposed rule also has implications for devices using SOCs with integrated WiFi functionality. The requirement that "only properly authenticated software is loaded and operating the device" will likely cause SOC manufacturers to lock down the software used on the entire SOC. This would:

- A. Prevent Americans from modifying the system software in devices that they own when such software has direct access to the WiFi chipset. This is the case with most SOCs and would prevent the user from exercising their right to install the software they desire on hardware they own. Universally banning such software no matter how well tested or vetted will have a large and negative impact on free and open source software (FOSS).
- B. Prevent installation of custom firmware on a cell phone or tablet, such as on an Android device.
- C. Stop development of security fixes for bugs in manufacturer firmware. The proposed rule restricts the user's ability to mitigate the security hole themselves using FOSS, which is valuable since device or chipset manufacturers generally do not fix security-related bugs in a timely manner and also stop providing bug fixes for older devices.

Thanks for your consideration,

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Craig

Last Name: Menefee

Mailing Address: 710 E San Ysidro Blvd #740

City: San Ysidro

Country: United States

State or Province: CA

ZIP/Postal Code: 92173

Email Address: c25e7e60@opayq.com

Organization Name: self

Comment: Wifi networking and radio chips are commonly combined, so if you ban modifications to one, you ban modifications to the other. That makes this NPRM an extremely bad idea.

The unintended or never considered consequences include outlawing important router security and capability enhancements such as those of the open source Tomato and DD-WRT firmware updates. Americans need the ability to fix security holes in their devices when the usually foreign manufacturer chooses to not do so.

Other consequences will prevent wireless networking researchers from investigating and modifying their devices. This will hobble router firmware progress at a time when security flaws are popping up more frequently than ever. It will prevent Americans from closing such holes in a timely way, using well tested, frequently updated and freely available wifi firmware revisions. The result will be to open up millions of frozen-in-time devices from being adapted to block new security threats.

Users have in the past fixed serious bugs in their wifi drivers using alternative, updated firmware - something the NPRM would ban. You would leave millions of home and small business wifi users with no practical way to make their wifi routers secure again.

In addition, billions of dollars of American commerce, 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 scotch this ill-considered restriction on the digital security of American wifi users.

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: Keith

Last Name: Benoit

Mailing Address: 323 Brandywine Rd

City: Charlotte

Country: United States

State or Province: NC

ZIP/Postal Code: 28209-2205

Email Address: keith721@gmail.com

Organization Name:

Comment: Please do not limit, restrict, or deny the public's right to manage the firmware deployed on internet and wireless devices they rightfully own. Open Source and GPL projects like Linux, OpenWRT and DD-WRT have made HUGE advances in the sophistication and capabilities of home routers and wireless devices over the twenty years. Manufacturers have not provided anywhere near as much. Manufacturers typically enable and expose less than 50% of the hardware capability in devices they market. This proposed rule would directly contradict and needlessly limit the Open Source and GPL project's efforts, and the benefits they provide to so many users. I have long been a supporter of free and Open Source software projects including Linux, OpenWRT, and DD-WRT, and will continue to support them in the future. The proposed rule simply does not make sense to this informed and intelligent wireless user.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Adam

Last Name: Parduhn

Mailing Address: 317 W. Anderson St.

City: Crown Point

Country: United States

State or Province: IN

ZIP/Postal Code: 46307

Email Address:

Organization Name:

Comment: I'd like my voice to be included in the chorus of technology professionals that disapprove of the proposed rule. I fear that the proposed solution will leave my home and work networks susceptible due to slow (if at all) bug-fix/patch responses from manufacturers. I would like to continue to be able to install 3rd party firmware on my devices. The FCC's response to public support of Net Neutrality gives me hope that my voice can still be heard.

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: Samuel

Last Name: Nathan

Mailing Address: 134 Sunset Drive

City: Longview

Country: United States

State or Province: WA

ZIP/Postal Code: 98632

Email Address: var2014@comcast.net

Organization Name:

Comment: I recently became aware of this proposal and I am appreciate the opportunity to comment.

I am against this proposal in that it's broad language would practically guarantee the elimination of many beneficial practices available today.

I can see this easily applying to the use of commonplace open source software for computers using WIFI, their software and firmware, for the WIFI devices themselves,

What would be the case for amateur radio systems where the ham radio operator is designated as the builder of the system, would an additional level of FCC regulations be placed on users modifying the system and so on. Or a computer user who decides to use open source software. Would the computer user have to seek permission from the manufacturer of a particular WIFI device before upgrading or changing OS versions?

While the regulation and oversight provided by FCC rules is generally a good thing, in this case the proposed regulation would stifle amateur radio, computer enthusiasts, and the general population by forcing them to purchase locked devices and proprietary software, where they would be placed at the receiving end of the whims of the manufacturers.

In what I see as a very reasonable scenario, even a simple task like a computer user reloading Microsoft Windows on a computer with a WIFI device could reasonably be thought of as violating the language in the proposal, in that the Wireless networking drivers present in the default Windows OS build are probably not the same and latest from the WIFI system manufacturer, This could easily be interpreted as a modification to the transmitter system by using software not created by the manufacturer.

I believe there are many more examples of what I see as commonplace and beneficial situations that would be prohibited by this proposal, and I believe it would be detrimental to society at large to have such a prohibition in place.