

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: Rey

Mailing Address: 4333 N Troy St, 3W

City: Chicago

Country: United States

State or Province: IL

ZIP/Postal Code: 60618

Email Address: dontcounttoday@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.

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: Cody

Last Name: Rude

Mailing Address: 11 Allen Street

City: Lowell

Country: United States

State or Province: MA

ZIP/Postal Code: 01852

Email Address: codyrude@gmail.com

Organization Name:

Comment: As our lives become more dependent on digital devices, it is critical that we are able to control and understand what our digital devices are doing.

Preventing end users from modifying their devices restricts basic liberties by preventing us from controlling our own belongings.

If this proposal is accepted, our personal communication will be at the mercy of corporations, who hold the keys to our digital lives.

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: Lance

Last Name: Brignoni

Mailing Address: 3313 Lake St

City: Bakersfield

Country: United States

State or Province: CA

ZIP/Postal Code: 93306

Email Address: lanceavil@gmail.com

Organization Name: Mozilla Foundation

Comment: I think this is a bad idea because it would hinder development from the open source community, which many companies rely on for firmware and embedded devices. One example is Wind River, a multi-billion dollar corporation which relies on FOSS to maintain secure firmware in millions of routers. This would be a step back for many developers, including myself. The only people modifying these types of devices are people such as myself who look for bugs to patch and write drivers 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: Tyler

Last Name: Moore

Mailing Address: 3713 Meadow Dr

City: House Springs

Country: United States

State or Province: MO

ZIP/Postal Code: 63051

Email Address: battlefield3vet55@yahoo.com

Organization Name:

Comment: Dear Federal Communications Commission,

I feel that this document will hurt the ability for people to fix problems on things they own themselves. For example, this could...

Restrict installation of alternative operating systems on your PC, like GNU/Linux, OpenBSD, FreeBSD, etc.

Prevent research into advanced wireless technologies, like mesh networking and bufferbloat fixes.

Ban installation of custom firmware on your Android phone.

Discourage the development of alternative free and open source WiFi firmware, like OpenWrt.

Infringe upon the ability of amateur radio operators to create high powered mesh networks to assist emergency personnel in a disaster.

Prevent resellers from installing firmware on routers, such as for retail WiFi hotspots or VPNs, without agreeing to any condition a manufacturer so chooses.

After the problems I had to deal with while trying to fix a problem my parents netgear router was having, locking down devices should never be allowed. Bad firmware that receives no support should be legally replaceable with open source firmware.

Sincerely,

Another concerning United States citizen.

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: Bennett

Last Name: Fredrick

Mailing Address: 2750 N. University Park Blvd

City: Layton

Country: United States

State or Province: UT

ZIP/Postal Code: 84404

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: Guy

Last Name: Clark

Mailing Address: Elm. 4cedar way

City: Wisbech

Country: United Kingdom

State or Province: Cambridgeshire

ZIP/Postal Code: PE14 0JJ

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: Nathaniel

Last Name: Garst

Mailing Address: 696 NE 24th Ave

City: Hillsboro

Country: United States

State or Province: OR

ZIP/Postal Code: 97124

Email Address: sergemerov@gmail.com

Organization Name:

Comment: I understand the desire to prevent unauthorized abuse of the spectrum by devices that have been rooted. However, I feel that this proposal "throws the baby out with the bath water", so to speak. There are two major issues, as I see it:

1. Software like DD-WRT is actually very important to the security of our Internet infrastructure. As a consequence of the software design process, many devices ship with firmware that has some number of bugs in it. This has been most evident when hacking groups have co-opted home routers to run a DDOS botnet in recent years. The solution to this is not locking down the update process, but rather the opposite: allowing consumers to update their software to remove security holes. The current structure of regulations on

Android phones, for example, allows carriers to prevent people from installing non-approved updates on their phones. However, those manufacturers often abandon said phones, leaving them in critical need of updates to keep them secure. Implementing similar rules across the board would have similar, legally enforced consequences. Manufacturers would have no incentive to patch security holes on a 5-year old device, even if the device was otherwise functional.

2. This proposal would also stop most innovation on unusual forms of networking. One promising technology that has been emerging in the last few years, for example, is mesh networking. Mesh networking has a number of advantages over traditional wifi infrastructure, including being extremely disaster-tolerant. However, legislating people to be unable to install aftermarket firmware would put a big dent in development. This technology has the potential to be extremely valuable, but because it is still in its infancy, it is unlikely to be pushed by a major manufacturer. Thus, requiring the resources of a major manufacturer to deploy code is basically a death warrant.

I write these comments because, as it stands now, a manufacturer does not have real incentive to update their software after first release. If a bug is found which could allow a device to be taken over, it is very unlikely for a prompt update, or even an update at all, to come from the original manufacturer. Locking down updates to these companies does not help, and may in fact cause the opposite effect, by leaving more software vulnerable.

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: Clinton

Last Name: Collins

Mailing Address: 120 Crescent Drive

City: Bristol

Country: United States

State or Province: VA

ZIP/Postal Code: 24201

Email Address: clinton.collins@gmail.com

Organization Name:

Comment: I think the direction of this legislation is misguided. Instead of limits the physical hardware, you are limiting software, which, stifles innovation, research, open source efforts, and device reuse. I am a software developer, and one of the first major projects I contributed to, and gained lots of knowledge was an open source firmware for a wireless router. The firmware enhanced the features of the router quite a bit, as well as helped hone my skills as a developer. Experimentation and tinkering should not be limited. If anything should be limited, it should be at the hardware level, and even then, I am hesitant. I would imagine there is a certain set of offenders, and working with those offenders would be the best course of action in my opinion.

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: Snook

Mailing Address: 75 W 5th Ave Apt 429

City: San Mateo

Country: United States

State or Province: CA

ZIP/Postal Code: 94402

Email Address: chris.snook@gmail.com

Organization Name:

Comment: The ability to modify code on a computing device is an essential foundation to maintaining the security of devices and networks. We have recently seen many cases where device manufacturers and distributors have taken months to patch critical security flaws, forcing users to install mitigating software or alternative operating systems on their own. There are also several important open source projects that maintain operating systems for wireless devices that implement features that cannot be found in commercial products, such as privacy enhancements and accessibility for handicapped users. Many of these are substantially more secure than the commercial operating systems they replace, and more quickly updated to fix discovered security vulnerabilities. They are usually based on the same open source code as the commercial versions, but they're maintained by expert users who continue to take an interest in the security of their devices long after its manufacturer has ceased production and focused development resources on new models, which happens very quickly in the mobile device market.

While security measures to prevent malicious or compromised applications from altering radio configurations are clearly desirable, most mobile operating systems already have robust access control mechanisms to prevent that. When they fail, it is often due to convenience features or back doors implemented by device manufacturers that are not present in the open source code from which they are derived. Security measures that prevent a user from intentionally installing their own operating systems would harm security research and end users who rely on alternative operating systems for enhanced security and functionality.

The Commission should implement a rule that would require protection of software-defined radio code and configuration against inadvertent or malicious modification, and ban undisclosed back doors, but also guarantee that users who choose to replace their device's operating system with an alternative will have the ability to 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: Ian

Last Name: M.

Mailing Address: Withheld

City: Zebulon

Country: United States

State or Province: NC

ZIP/Postal Code: 27597

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.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Robert

Last Name: Perce

Mailing Address: 2810 Hemphill Park Apt 238B

City: Austin

Country: United States

State or Province: TX

ZIP/Postal Code: 78705

Email Address: robert.perce@gmail.com

Organization Name:

Comment: Limitations like this proposal indicate would cripple the hobbyist and advanced personal users from using their devices to their full potential. It would prevent using channels people shouldn't, but at far too high of a cost. It should not be illegal to own a device that could commit illegal acts - just because murder is illegal, for example, I should not be restricted from buying a kitchen knife. Just because certain channels are not in the consumer spectrum, I should not be restricted from applying capability to access those channels as a side effect of legitimate improvements.

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: Antoine

Last Name: Duplantie Grenier

Mailing Address: 3652 ave Laval

City: Montreal

Country: Canada

State or Province: Quebec

ZIP/Postal Code: h2x3c9

Email Address: antoinedup@gmail.com

Organization Name: thales

Comment: remove the ownership of the person who buy the device, 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: Gerard

Last Name: Godone-Maresca

Mailing Address: 2 Judith Ct

City: Middletown

Country: United States

State or Province: RI

ZIP/Postal Code: 02842

Email Address: ggodonemaresca@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.

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: Clinton

Last Name: Barnes

Mailing Address: 1528 Canyon Rose Way

City: Las Vegas

Country: United States

State or Province: NV

ZIP/Postal Code: 89108

Email Address: Clint@clintonbarnes.com

Organization Name:

Comment: I oppose the suggested rule change. While the number of devices has increased, the FCC is attempting to make it more difficult to have devices operate properly in a situation that they are not. Instead of restricting the devices, the FCC needs to give more airspace around these bands and allow consumers to use it. I believe that this really is overstretching your bounds and shouldn't be considered at all.

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: Antonio

Last Name: Panzera

Mailing Address: 1911 Roland Dr

City: Hanford

Country: United States

State or Province: CA

ZIP/Postal Code: 93230

Email Address: apanzera@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.

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: Theo

Last Name: Tosini

Mailing Address: Theo Tosini

City: Bethesda

Country: United States

State or Province: MD

ZIP/Postal Code: 20817

Email Address:

Organization Name:

Comment: While interference is a problem, our freedom is too. Existing laws already allow law enforcement to find and punish people illegally using the RF spectrum. However, this new proposal would allow the government to punish people for having the ability to break the law, not actually breaking it. Allowing end users to change firmware on embedded wireless devices such as routers allows for new research on wireless technologies to continue, lets emergency personnel create mesh networks, and allows users and professionals to patch major security vulnerabilities that manufacturers refuse to fix (such as a remote-administration bug in many routers that has been in many devices, even new devices, for nearly a decade). The security of our networking infrastructure relies heavily on citizen's ability to develop new technologies and customize devices. Please let this continue, while still punishing bad actors.

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: Jay

Last Name: Faulkner

Mailing Address: 125 Cambon Dr Apt 8F

City: San Francisco

Country: United States

State or Province: CA

ZIP/Postal Code: 94132-2509

Email Address: jay@jvf.cc

Organization Name:

Comment: As someone who makes a living working on open source software and open hardware, the proposed rules are very concerning to me. Requiring wireless devices to have locked-down firmwares completely eliminates open source firmware from being possible. This would be an unfair limitation on competition and mean that moving forward, no device in America would be able to have fully audited, open source firmware and software and still be generally useful.

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: Pastuszek

Mailing Address: 3600 Valley Meadow Dr.

City: Bensalem

Country: United States

State or Province: PA

ZIP/Postal Code: 19020-4214

Email Address: apastuszek@gmailcom

Organization Name: Citizen of the United States

Comment: No, no, no and no!

Please stop trying to restrict what I can do with my personal property. It's MINE. I paid for it, I can do as I please with 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: Andreas

Last Name: Echavez

Mailing Address: 406 Montezuma St

City: Rio Vista

Country: United States

State or Province: CA

ZIP/Postal Code: 94571

Email Address: oceanplexian@gmail.com

Organization Name:

Comment: My name is Andreas, I live in Rio Vista California and I utilize software-defined radio for hobbyist and non-commercial purposes, I've also studied as a student pilot and have, in personal experience, used radio for the purposes of responding in critical, life-threatening situations, as well as for personal enjoyment.

I take issue with the statement "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.", because I do not believe it will be effective, I think it will cause undue burden on manufacturers and inventors, and I consider this to be a serious issue because the audience of people who might participate in modification of software-defined radio is the same demographic that invents technology, designs and develops new forms of communication, and encompasses some of the most respectful, self-aware technologists in the country. A good example of less restrictive regulation functioning in practice is with the FAA, for example, and their less restrictive regulation of experimental and ultralight aircraft (assuming those aircraft are under a certain weight and meet certain characteristics), and I think that their policy fosters an inventive spirit.

I would like to see the FCC amend this section, and focus on more on transparent communication, cooperative dialog with the community, and educational programs that encourage people to be good RF neighbors. I think those measures would be far more effective and encourage the type of future where we can both protect the integrity of wireless spectrum and build positive relationships between hobbyists and the FCC.

Thank you,
Andreas

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: Curti

Last Name: West

Mailing Address: 168 Mass Ave

City: Boston

Country: United States

State or Province: MA

ZIP/Postal Code: 02215

Email Address: CurtissAWest@gmail.com

Organization Name:

Comment: This proposed rule is far too broad and would severely limit the ability of people in this country to maintain true ownership over their own property.

It is already illegal to knowingly disrupt radio communications. No product that an amateur could acquire could accidentally cause enough of a disruption to warrant this sort of wide blanket rule.

This would disrupt or outright prevent any enthusiast from modifying a personal computer, remote controlled toy, or television remote. These regulations would harm the people most likely to go into and have positive effect on the tech sector and will hamper America's technological prowess in the following years.

There are rules in place already that limit what sort of RF interference can be emitted. Those should be enforced more uniformly before more laws are implemented.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Michael

Last Name: Koch

Mailing Address: Ellernkamp 12

City: Hiddenhausen

Country: Germany

State or Province: Nordrhein-Westfalen

ZIP/Postal Code: 32120

Email Address: m.koch@emkay443.de

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: Brad

Last Name: Ruxton

Mailing Address: 2 Buffum St

City: Pawtucket

Country: United States

State or Province: RI

ZIP/Postal Code: 02860

Email Address:

Organization Name:

Comment: This rule would hurt consumers only to benefit the profit margins of businesses. When we buy a device, we own the device and should be able to install anything that we want on it. Locking us out of that ability goes against everything in the industry. It prevents enthusiasts from experimenting with projects in their spare time. These projects are how we make advancements in the field.

Reject this rule, full stop.

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: Sauvageau

Mailing Address: 2-3535 Masson

City: Montreal

Country: Canada

State or Province: Quebec

ZIP/Postal Code: H1X 1S1

Email Address: eric@lostrealm.ca

Organization Name:

Comment: The third party firmware market is a driving force for innovation and product functionality. A lot of (perfectly legal and harmless) product features first started in a third party firmware product, and was eventually integrated into manufacturer's official firmware.

While some of these projects can indeed provide functionalities that allow for circumventing channel and power output limitations, that does not mean that the entire third party firmware market is doing so.

It is my belief, both as a long-time user and a third party firmware developer myself that forcing manufacturers to flat out prevent the flashing of a third party firmware will be harmful to the market, and deny end users of choice (for cases where an original manufacturer's firmware would be devoid of advanced features and/or contain unfixed security holes and/or has software defects and/or are no longer being supported by the original manufacturer.

Therefore, I recommend that the scope of these rules be reduced to only ensuring that the radio components are operating within the legal parameters, possibly by shifting the solution to a hardware limitation, rather than a software limitation.

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: joe

Last Name: berger

Mailing Address: joeberger@gmail.com

City: forest hills

Country: United States

State or Province: NY

ZIP/Postal Code: 11375

Email Address: joeberger@gmail.com

Organization Name: average citizen

Comment: 20 years ago - before we all had cellphones, i would watch my old tube tv set, and have to listen to a nearby cab company dispatcher step on my over the air tv antenna signal in a residential neighborhood. i figured out which office it came from, filed multiple complaints with the fcc, yet this behavior continued unabated till eventually all the drivers had cell phones and the over powered dispatch broadcast radio was no longer in use. nothing about this situation surprised me - if people can get away with breaking the law - they will, and if regulators are underfunded to stop law breakers, they won't.

so here we are 20 years later, and everyone and everything is online. electronics manufacturers and isp/telco/cable companies want the fcc to make sure nobody can modify their consumer equipment and "step on" anyone else signal like that cab company did to me 20 years ago. the difference now is everything is addressable - ISP's instantly know every MAC and public IP in use on their networks. this mean if anyone is making too much noise and stepping on other networks and wrecking havok, it's a simple matter to shut them down as you can instantly know what IP/MAC is used, which ISP hosts them, and with a couple of keystrokes take that noisy offender offline. this isn't something an underfunded regulator can't do, nor something an authorized profit driven company can't do under some official fcc mandate.

the point being - the fcc needs to take a closer look at what is motivating all these gadget makers and corporate network hosts to keep end users from modifying their devices. do they really need this to protect their networks, when some automated system could just as easily cut off any offending endpoint? or are they simply using this issue as an elaborate justification to to keep end point feeding their profitable corporate metadata collection departments.

if we learned anything in 2015 from the irs hack, federal security application hack, and the ashley madison hack - it's that governments and corporations can't be trusted to keep our privacy safe, and our private data getting into the wrong hands can be life changing. the few people savvy enough to modify their devices to improve privacy and drop the performance hit suffered from all that corporate intrusion, should not have to suffer for the continued incompetence of others, just to keep metadata sellers and proven ineffective terrorism watchdogs happy.

bottom line is the fcc can keep everyone happy by continuing to allow end users to modify their devices, while at the same time crafting guidelines allowing corporate hosts to cut off modified device behavior that is clearly deleterious to their networks, and to orchestrate some sort of simple fast appeals process to get the offenders back online after they have remedied whatever was allegedly causing any network distress. the fcc must allow privacy advocate groups to help draft such guidelines to ensure the corporate players are not simply creating more roadblocks for them to exploit.

I trust myself with my own privacy, not any government and not any corporation. Don't take what little power I have to

maintain that privacy away, under the guise of preserving network integrity from threats that don't exist, or maintaining corporate profit centers already growing fat and rich off my metadata. Look at what's going on right now with Window 10 upgrading. most are relinquishing privacy and "trusting" microsoft with their OS use metadata, while some (like myself) would rather use a more cumbersome OS like Unix for the sake of my privacy. do not take that freedom to choose how we use our online devices away from the few of us unwilling to surrender what little online privacy we still have the power to control.

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: Cetta

Mailing Address: 211 Avalon Pines Dr

City: Coram

Country: United States

State or Province: NY

ZIP/Postal Code: 11727

Email Address: cetta.john@gmail.com

Organization Name:

Comment: To the FCC and whom it may concern:

I am a United States citizen from New York who is concerned about your proposed rule for Equipment Authorization and Electronic Labeling for Wireless Devices. I am concerned that the proposed rule as currently written will limit and restrict legitimate software choices for consumer electronics, and for personal and mobile computing devices. I am further concerned that the rule as written will limit the availability of open source alternatives to proprietary platforms. For example, in the mobile context, original equipment manufacturers (OEMs) of Android devices are often slow, sluggish and neglectful in pushing out critical security updates and operating system upgrades to their users. Therefore, many users of these devices must turn to open source alternatives in order to patch the security holes neglected by OEMs. I am concerned that your rules as currently written will force OEMs to lock down their devices so as to prevent consumers from choosing open source alternatives.

This result is the exact opposite result the FCC should seek to achieve. OEMs currently engage in significant anti-competitive behavior already. For example, many devices come bundled with unwanted, unnecessary, obtrusive programs installed by the OEM, which are often difficult to remove if the consumer decides she does not want these programs. Requiring OEMs to further lock down their devices would only service to embolden anti-competitive behavior by OEMs at the expense of American consumers.

Specifically, the proposed rules would lead to locked-down devices that prevent consumers from using an open source fix to a bug in a device's WiFi drivers that an OEM has neglected to fix. The proposed rules would further prevent consumers from using custom, open source software that includes additional functionality left out of OEM versions. For example, many consumers use OpenWrt software on their home WiFi routers so that they can use a VPN on their home network because the OEM of their router did not include even basic VPN functionality in their pre-packaged software. By forcing OEMs to locked down their devices to prevent users from installing these alternatives, the FCC rules will serve to limit consumer choice.

Instead of limiting consumer choice to the often anti-competitive pre-installed OEM options, the FCC should seek to revise its proposed rules to produce results that broaden and enhance consumer choice.

Sincerely,
John Cetta

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: Abdullah

Last Name: Mardini

Mailing Address: 6600 Van Aalst BLVD

City: Fort Benning

Country: United States

State or Province: GA

ZIP/Postal Code: 31905

Email Address: superppl@gmail.com

Organization Name:

Comment: This ruling creates a number of problems, namely due to that manufacturers do not know how to appropriately support their devices, and do not care to know how. Major security bugs usually remain unsolved indefinitely on many devices.

Users today can mitigate this issue by installing open source 3rd party software on their devices, replacing the default software. This closes many outstanding security vulnerabilities, brings new features to the device, and allows users to use their devices far after the manufacturer has ceased support for it, which can be alarmingly short.

By blocking users from altering the software on their devices, the FCC would harm many users by forcing them to use manufacturers unsupported software on the devices, and to buy new devices to receive simple software fixes. This would also contribute greatly to electronic waste.

Most importantly, this may do precious little for the skilled who will modify their devices regardless and use their devices in an unregulated manner. The demand for those skills and human nature will result in a market of unregulated devices, such as what is seen in modified video game consoles capable of playing pirated software.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Dustin

Last Name: Cudd

Mailing Address: 2922 Gwendolyn Way

City: Rancho Cordova

Country: United States

State or Province: CA

ZIP/Postal Code: 95670

Email Address: dustin.cudd@gmail.com

Organization Name:

Comment: Consumers should be able to modify or replace the firmware/operating system on their network devices freely.

Such support can allow the community to patch security issues long after the manufacture ends support as well as resolve any other issues that may arise.

Furthermore, since most devices use opensource, BSD style licensed software for many important parts of their functionality, it goes strongly against the spirit and values inherent in those projects and licenses to disallow access, modification, or community development.

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: Joseph

Last Name: Blaim

Mailing Address: 1210 north streamwood apt 1A

City: lansing

Country: United States

State or Province: MI

ZIP/Postal Code: 48917

Email Address: ccdr@aol.com

Organization Name:

Comment: As an American citizen, technology consumer, and IT professional, I ask that you please not pass this proposal. The restriction on consumer modification of devices, especially software modification is frankly horrifying. This would be a radical, extreme, and fundamental change to the nature of many tech devices, particularly those which have had the greatest success, growth and beneficial impact on consumers' lives, software driven devices. This strikes right at the heart of what has defined the computing industry, what has made it so successful, and allowed for the rapid advancement of new capabilities: flexibility, adaptability and consumer control.

The ability to modify the behavior of a device through new software rather than hardware is the very dining aspect of computers in all their varying forms today. This does not only include corporate software development but also personal and communal efforts such as the open source movement which have had a huge beneficial impact on the industry. This includes not only industry changing advancements and distributable products large and small, but also the space for personal experimentation, development, and agency of current and future IT professionals independent of their official training and employment. While not strictly speaking necessary, this is an overwhelming critical element in driving people into this industry and developing more capable and driven professionals. To lose this space would be devastating both for individual developers and the industry.

In addition to the overwhelming general loss this presents for consumers and technology enthusiasts, this poses a huge danger to important legitimate research in wireless technology. Wireless technology has grown explosively in recent years and had provided immasurable benefits in the day to day lives of consumers but that is not to say the change is finished, complete, or unflawed. To the contrary, this massive expansion despite its benefits has envied myriad new problems in the realms of security and privacy which must be solved. The continued research and innovation required to solve these problems and continue the momentum of current advent with additional transformative developments requires the freedom of modification which this proposal eliminates.

I fully understand the importance of protecting the spectrum from abuse and disruption. Indeed, due to the growing ubiquitousness of wireless technology, those adversely impacted by this proposal have an overwhelming interest in protecting this space and preserving it for reliable use, but the adverse effects of this proposal overwhelmingly outweigh this interest in particular given the current reliability of the spectrum and extent of abuse. While I would hardly advocate inaction, even that would easily be advisable to this destructive proposed action.

Instead of imposing limitations on the use and development of technology, I would suggest embracing it in attempting to find a solution. Current advancements are not the problem but the solution. It actually presents the opportunity for increased monitoring to detect and respond to potential abuse. Increased accessibility, simplicity, and automation of monitoring would be a huge boon which should see broad support from users of wireless technology if presented

properly. Distributed and adaptive technology in particular, whose research is threatened by this restriction could present new and innovative solutions to the problem.

In short, this is an extremely dangerous change for consumers, researchers, and developers which blocks innovation and disrupts a hugely successful industry and should be opposed as vigorously as possible.

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: Tanel

Last Name: Rauba

Mailing Address: tanel.rauba@eesti.ee

City: Viljandi

Country: Estonia

State or Province: Viljandi

ZIP/Postal Code: 71007

Email Address:

Organization Name:

Comment: The part:

For a device to be certified as an SDR, in addition to demonstrating that the device complies with the applicable technical requirements, the applicant must also demonstrate that the device contains security features to prevent the loading of software that would allow the radio to operate in violation of the Commission's rules.

will most likely kill the already meager variety we have on the global market of RF devices. Every manufacturer wants to diversify their product lines with as little trouble as possible and USA is a big part of the world market. On behalf of all those that treasure freedom of choice and control over our own property, I implore you: don't create such harmful blanket regulations. So far things have gone relatively well, don't fix what isn't broken.

The responsibility for one's actions always falls to that person. If harmful action is really spreading, just writing uniform, rigid regulations will not mitigate that. Actual surveillance, analysis and enforcement is required.

I would really like to at the very least be able to decide if I'm comfortable with, for example, my phone being loaded with adware and spyware and then LOCKED. Because that's the easiest way for manufacturers to conform to these regulations: disable software modifications to base operating system.

I am certain that many citizens of USA, the land of the free, feel the same. I would like to retain my ability to replace that software with such that I trust most and can actually review. It's bad enough we have to put up with that on levels closer to hardware. Security through obscurity never works.

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: Johnson

Mailing Address: 207 Bailey Brook Ln

City: Dickinson

Country: United States

State or Province: TX

ZIP/Postal Code: 77539-7372

Email Address:

Organization Name:

Comment: Preventing modifications to small devices by consumers creates an ideal playground for criminal hackers.

The best secure software and firmware requires updates to close security holes as they are found.

These updates are often not seen as cost effective by the manufacturer. If the consumer wants a secure device, and the manufacturer doesn't fix each vulnerability in a timely manner, they will have to throw the device away and buy a new one.

Constant replacement of such devices is not cost effective for the security conscious consumer, which include any reputable business.

Good security is accomplished through 'layers', legislating layers of weak security is the criminal hackers ideal playground.

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: Haden

Last Name: Wright

Mailing Address: 1600 highland ave

City: wilmette

Country: United States

State or Province: IL

ZIP/Postal Code: 60091

Email Address: t.hadenwright@gmail.com

Organization Name:

Comment: Please don't let this bill pass I would like to be able to openly use my 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: Rodger

Last Name: Abbit

Mailing Address: 28 Henry Street

City: Nuneaton

Country: United Kingdom

State or Province: Warwickshire

ZIP/Postal Code: CV115SQ

Email Address:

Organization Name:

Comment: This proposal by the FCC body would widely damage the personal liberties and freedoms of citizens of the United States. Restrictions on what people are able to do with devices that they should have 'ownership' of would start making the value of products non-existent, as there is no ownership with no control.

I understand that the FCC wants to make the wireless spectrum safer, but this proposal would not achieve that. Older devices would likely be configured to do the types of things you wish to prohibit, and people would find ways around the proposals. There is no solid way for the FCC to properly lock down the spectrum, merely make it harder for an initial period of around 3 months, before people figure out how to work around the limitations presented.

In conclusion, I feel that this proposal is a waste of time, and would widely harm the liberties of the citizens of the United States.

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: Hassan

Last Name: Hamoud

Mailing Address: 137-03 168th st

City: Jamaica

Country: United States

State or Province: NY

ZIP/Postal Code: 11434

Email Address:

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.

The ability to modify consumer level networking hardware is 100% needed. What many people do not consider, is what routers can do. These are essentially linux PC's running in the signal path of all of our network traffic.

Most router makers stop releasing firmware updated for their routers within around 2 years. We have 802.11ac from major router makers today that are no longer receiving security updates.

There are many routers in use today that are vulnerable to the netUSB exploit, and will never receive an official update from the company that made the router.

Furthermore, none of the 3rd party firmware allow you to violate the major FCC limits. e.g., the amplifiers on many routers are not directly controllable from the software. instead, they will be factory set to a specific gain, and then the software controllable area simply varies the input to the amplifier, thus even if you get a dev who can successfully reverse engineer the WiFi drivers (have not seen it done yet since those drivers are insanely complicated), you would still be unable to take even the highest end routers and push them beyond 1000mw.

Furthermore, this will significantly harm router sales in the country. Many companies rely on custom router software for functions such as captive portal. Many small businesses cannot afford expensive remote network filtering services for providing customers in their establishments to have internet access, while also preventing malicious users from using their connection for malicious purposes. With custom firmware, there are a wealth of tool available to perform this filtering for free to the router level. By preventing this, you will end up with 2 issues, increased online criminal activity by criminals making use of these hotspots. You will also end up with economic harm from businesses being unable to provide services which were traditionally used to attract more customers.

Networking devices with "Modular radios" have the FCC limits imposed at the hardware level, thus there is no software method of bypassing the transmit power limits. While on rare occasion, it is possible too use custom firmware to use non approved WiFi channels, no one actually uses them due to the front end hardware of the radios, there are limits that cannot be bypassed. Non approved WiFi channels, even if used, will often lack a usable transmit power, and even if by some miracle there is one without those front end imposed limits and filters, using non approved channels will mean that you are competing with non WiFi friendly frequencies, thus nothing to optimize the sharing of the airtime thus performance is sure to be worst.

Overall, this is a 100% unnecessary restriction which will only harm consumers and businesses by preventing edge use cases, and harming the security of the devices. Custom firmware ensures that the hardware continues to be useful even after the company that made the router has stopped releasing security updates. (802.11ac is a current widely use standard, the hardware is nowhere near obsolete, but there are many 802.11ac routers no longer getting updates without custom firmware, those routers are dangerous to the user owning that equipment, as well as the internet as a whole for when an attacker inevitably takes control of it and uses it for illegal activity.

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: Nick

Last Name: Bedi

Mailing Address: 1154 Keyes Ave

City: Schenectady

Country: United States

State or Province: NY

ZIP/Postal Code: 12309

Email Address:

Organization Name:

Comment: This ruling creates a number of problems, namely due to that manufacturers do not know how to appropriately support their devices, and do not care to know how. Major security bugs usually remain unsolved indefinitely on many devices.

Users today can mitigate this issue by installing open source 3rd party software on their devices, replacing the default software. This closes many outstanding security vulnerabilities, brings new features to the device, and allows users to use their devices far after the manufacturer has ceased support for it, which can be alarmingly short.

By blocking users from altering the software on their devices, the FCC would harm many users by forcing them to use manufacturers unsupported software on the devices, or to buy new devices to receive simple software fixes. This would also contribute greatly to electronic waste.

Most importantly, this may do precious little for the skilled who will modify their devices regardless and use their devices in an unregulated manner. The demand for those skills and human nature will result in a market of unregulated devices, such as what is seen in modified video game consoles capable of playing pirated software.

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: Julian

Last Name: Marchant

Mailing Address: 334 W Lake St

City: South Lyon

Country: United States

State or Province: MI

ZIP/Postal Code: 48178

Email Address:

Organization Name:

Comment: I think it's abhorrent, disgusting even, that the FCC would force companies to lock down the hardware they sell to consumers so that it is technically impossible for said consumers to break laws. This approach is rather like forcing car manufacturers to use artificial restrictions to prevent drivers from going over the speed limit. Moreover, this requirement essentially mandates the use of proprietary software, which is an injustice.

The only thing that these companies should ever have to do to comply with these sorts of regulations is not include the illegal functionality into the firmware shipped with the hardware. If a user makes a modification to the firmware or installs new firmware which causes a device to do something illegal, that is **their** responsibility. Companies are not police, nor should they be.

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: Stephens

Mailing Address: 130 Ridgewood Ln

City: Dyer

Country: United States

State or Province: IN

ZIP/Postal Code: 46311

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.

To summarize my position, I strongly oppose this rule change as well as any other that might prevent me from modifying my devices as I see fit.

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: Kristian

Last Name: Thiesson

Mailing Address: Ellehavehavegrdsvej 6 Horreby

City: Nykbing F.

Country: Denmark

State or Province: Guldborgsund

ZIP/Postal Code: 4800

Email Address: tyjuji@gmx.com

Organization Name:

Comment:

I feel this rule goes against American values and although I am not a lawyer, I would think this rule to be unconstitutional. "Land of the free", yet you seek to take away the freedom of all open source software.

This rule would not only implicate American interests, but also affect the whole world seeing as so much of free software is based in the US.

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: Ildus

Last Name: Kurbangaliev

Mailing Address: k-dus@yandex.ru

City: Moscow

Country: Russia

State or Province: Moscow

ZIP/Postal Code: 450000

Email Address: k-dus@yandex.ru

Organization Name:

Comment: First of all these rules will affect many countries (not only USA).

Secondly I think the user can have all freedom on the device that is not limited by manufacturer. He must have a possibility to install his software to devices (for example Linux or BSD on Windows preinstalled machines, or some custom firmware to other devices). Only the manufacturer can limit these things in other cases a software should not be hardly connected with a hardware only because it has wireless.

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: Hardy

Mailing Address: 3152 lake monroe RD

City: douglasville

Country: United States

State or Province: GA

ZIP/Postal Code: 30135

Email Address:

Organization Name:

Comment: I, and many others would prefer that the FCC would not implement or try to implement rules that take away the ability of users to install the software of their choosing on their computing device. Users need the ability to fix security holes in their devices when the manufacturer chooses to not do so; In the past users have fixed serious bugs in their wifi drivers, which would be banned under the NPRM.

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: Novak

Mailing Address: 320 Dakota Ave Apt 2

City: Santa Cruz

Country: United States

State or Province: CA

ZIP/Postal Code: 95060

Email Address:

Organization Name:

Comment: Dear FCC,

I am writing to you to express my concern about the possible knock-on effects of some of the requirements you recently proposed in your recent NPRM. Although unifying and streamlining the FCC requirements for devices is certainly a worthy goal, it is important to recognize that modular transmitters of the types the rules are written to apply to are often incorporated into computing devices, and I am worried that it will be very difficult for the manufacturers of these devices to "secure" their software-controlled modular transmitters and E-LABEL information against "unauthorized modification" will also prevent necessary modifications to the software that controls the computing functions of these devices.

It is vitally important that the user of a computing device be the final authority over the software that runs on said device. The device acts on their behalf, and is in some ways an extension of their mind; they are clearly authorized to make any modifications to it that they see fit, especially for the purposes of securing it from hackers or extending its useful life beyond the end of manufacturer support. However, many of these devices (Wi-Fi routers, for example) combine the software that controls the information-processing and security functions of the device with that which controls the radio transmitter. Many routers, for example, use the same Web interface to allow the user to select the country in which the device is operating (and thus the allowable radio frequencies on which it may transmit) and to configure features like parental controls and log-in passwords. If new FCC rules require device manufacturers to prevent modification of this software, it is easy to imagine a situation in which a security flaw in one of these devices cannot be repaired by its owner, because the owner is not permitted, under FCC rules, to modify the software, and because the device manufacturer has taken technical measures to ensure that they do not.

If the FCC is going to require that devices featuring software-controllable transmitters not be able to operate with software that causes them to violate FCC regulations, the FCC should allow separate self-certification of new software for such devices, and ensure that device manufacturers allow the loading of any software that maintains a device's compliance with FCC regulations, even if that software is not authorized by the original manufacturer of the device.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Sam

Last Name: Nuy

Mailing Address: no way str

City: neverland

Country: Vietnam

State or Province: no

ZIP/Postal Code: 00000000

Email Address: nonono@no.com

Organization Name:

Comment: Hardware should be open!