

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Joshua

Last Name: Gill

Mailing Address: 8910 Sourwood Ct.

City: Indianapolis

Country: United States

State or Province: IN

ZIP/Postal Code: 46260

Email Address:

Organization Name:

Comment: While this might only apply to some higher frequency routers, the fact that we can't own and modify our own things it disconcerting. Next will you modify radios to never be opened because with a few parts we can get policeband frequencies? is it a crime to use your own things? everything about this has the tone of some company ready to sell me something that I won't be able to change, which is why people hate cable and mobile internet service. You have to buy all the channels we include or else. you can't change your equipment or else. Please reconsider, it is software and even updating software is changing it.

While this might only apply to some higher frequency routers, the fact that we can't own and modify our own things it disconcerting. Next will you modify radios to never be opened because with a few parts we can get policeband frequencies? is it a crime to use your own things? everything about this has the tone of some company ready to sell me something that I won't be able to change, which is why people hate cable and mobile internet service. You have to buy all the channels we include or else. you can't change your equipment or else. Please reconsider, it is software and even updating software is changing 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: Anonymous

Last Name: Anonymous

Mailing Address: 75 Rev Dr. Martin Luther King Jr Blvd Saint Paul

City: Saint Paul

Country: United States

State or Province: MN

ZIP/Postal Code: 55101

Email Address: null

Organization Name: null

Comment: Dear Sirs and Mesdames:

The freedom and privacy of Americans will be compromised should the proposed rule on Equipment Authorization and Electronic Labeling for Wireless Devices passes.

I oppose it.

While a majority of the rule focuses on wireless spectrum, the balance focuses on software and the modification thereof. The inclusion of software for certification and the prohibition of modification to it is akin to a giant neon sign spelled TROUBLE.

Locking consumers out of modifying devices they purchase by way of a permissions system from the manufacturer doesn't fix anything. Manufacturers are required to submit their products to the FCC for certification. The hardware needs to fit specification so it doesn't work beyond the spectrum for which it was licensed. Including software is an overreach.

Please consider this:

"Right now, the FCC is considering a proposal to require manufacturers to lock down computing devices (routers, PCs, phones) to prevent modification if they have a "modular wireless radio"[1][2] or a device with an "electronic label"[3]. The rules would likely:

- 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." Source for the quote above: <https://archive.is/tGCKU#selection-21.0-95.158>

That doesn't sound much like spectrum control to me. It reads more like an attempt to rid the marketplace of hobbyists and alternative operating systems for computers. Thomas Edison is rolling over in his grave over this.

Whether this proposed rule as summarized above is from a well-meaning person or a malcontent software lobbyist, I cannot say. Either way, this is a problem that stifles innovation and the personal freedom of Americans.

The United States has suffered any number of hacker attacks in recent days, many attributable to communist countries. The irony that under the proposed rule, those communists would have more freedom to innovate such attacks that we would have to fight it.

Sincerely,

Concerned in Minnesota

Dear Sirs and Mesdames:

The freedom and privacy of Americans will be compromised should the proposed rule on Equipment Authorization and Electronic Labeling for Wireless Devices passes.

I oppose it.

While a majority of the rule focuses on wireless spectrum, the balance focuses on software and the modification thereof. The inclusion of software for certification and the prohibition of modification to it is akin to a giant neon sign spelled TROUBLE.

Locking consumers out of modifying devices they purchase by way of a permissions system from the manufacturer doesn't fix anything. Manufacturers are required to submit their products to the FCC for certification. The hardware needs to fit specification so it doesn't work beyond the spectrum for which it was licensed. Including software is an overreach.

Please consider this:

"Right now, the FCC is considering a proposal to require manufacturers to lock down computing devices (routers, PCs, phones) to prevent modification if they have a "modular wireless radio"[1][2] or a device with an "electronic label"[3]. The rules would likely:

- 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." Source for the quote above: <https://archive.is/tGckU#selection-21.0-95.158>

That doesn't sound much like spectrum control to me. It reads more like an attempt to rid the marketplace of hobbyists and alternative operating systems for computers. Thomas Edison is rolling over in his grave over this.

Whether this proposed rule as summarized above is from a well-meaning person or a malcontent software lobbyist, I cannot say. Either way, this is a problem that stifles innovation and the personal freedom of Americans.

The United States has suffered any number of hacker attacks in recent days, many attributable to communist countries. The irony that under the proposed rule, those communists would have more freedom to innovate such attacks that we would have to fight it.

Sincerely,

Concerned in Minnesota

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: Spencer

Last Name: Ragen

Mailing Address: 104 S Marion Ave

City: Wenonah

Country: United States

State or Province: NJ

ZIP/Postal Code: 08090-1925

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.

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: Doug

Last Name: Walker

Mailing Address: 125 w stonewall dr

City: front royal

Country: United States

State or Province: VA

ZIP/Postal Code: 22630

Email Address: federalregister@dougwalker.us

Organization Name:

Comment: Don't be stupid. No matter what you do I'll still be able to run whatever I want in a virtual machine.

Do you really want to piss off all the really smart people?

Don't be stupid. No matter what you do I'll still be able to run whatever I want in a virtual machine.

Do you really want to piss off all the really smart people?

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Christopher

Last Name: Ferrante

Mailing Address: 7604 Laurel Ridge Court

City: Laurel

Country: United States

State or Province: MD

ZIP/Postal Code: 20707

Email Address: cferra@gmail.com

Organization Name:

Comment: Ultimately this is a bad idea for open source and highly functional firmwares for devices that are purchased by consumers. Please revise this rule to allow for free and open third party firmwares on devices!

Ultimately this is a bad idea for open source and highly functional firmwares for devices that are purchased by consumers. Please revise this rule to allow for free and open third party firmwares on 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: Steven

Last Name: Hamilton

Mailing Address: 758 Bayard Street

City: Teaneck

Country: United States

State or Province: NJ

ZIP/Postal Code: 07666

Email Address: shambleh@yahoo.com

Organization Name:

Comment: I am entering this comment officially requesting that the FCC NOT implement rules that would take away the ability of individual home users to install the software of their choosing on their computing devices. The ability for the average person to make changes and updates to their own hardware is crucial to the efforts of wireless networking research depends on the ability of researchers to investigate and modify their devices. Researchers, in this case, could include anyone from a professor at a university to the average college student or even a single person working to develop the next start-up in their basement (something that has been the source of innovation in this country for the past several years in an immense way).

Additionally, Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. It is unfortunate that this is something that needs to be addressed but too often do we see companies not making an effort to resolve issues in a timely fashion because doing so may not be as profitable as other endeavors. In the past, users have 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 hot-spot vendors, depends on the ability of users and companies to install the software of their choosing. Please preserve this ability for all Americans now and forever.

I am entering this comment officially requesting that the FCC NOT implement rules that would take away the ability of individual home users to install the software of their choosing on their computing devices. The ability for the average person to make changes and updates to their own hardware is crucial to the efforts of wireless networking research depends on the ability of researchers to investigate and modify their devices. Researchers, in this case, could include anyone from a professor at a university to the average college student or even a single person working to develop the next start-up in their basement (something that has been the source of innovation in this country for the past several years in an immense way).

Additionally, Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. It is unfortunate that this is something that needs to be addressed but too often do we see companies not making an effort to resolve issues in a timely fashion because doing so may not be as profitable as other endeavors. In the past, users have 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 hot-spot vendors, depends on the ability of users and companies to install the software of their choosing. Please preserve this ability for all Americans now and forever.

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: Blake

Last Name: Everhart

Mailing Address: 1235 Redacted for reasons

City: Columbus

Country: United States

State or Province: OH

ZIP/Postal Code: 43231

Email Address: lars4life@gmail.com

Organization Name: null

Comment: As an IT professional, I take exception to the any rules that prevent me from changing the software on products I own. If properly configured open source software us more secure an allows me the freedom to customize hardware that I own. I honestly do not understand how people who legally purchase hardware can have the software locked. Sometimes companies do not update vulnerabilities or drop support of a product in favor of something newer. Having the ability to load my own or open sourced software keeps that hardware relevant and keeps me from wasting my money buying something that I do not need to.

I understand the want to make products more secure and I agree that products should be more secure. This is the wrong way to go about it.

I want the ability and should have the ability to secure my own data, hardware in a manner of my choosing. Being in the IT world I will read about an online threat or vulnerability and it will be several months before its patched. Me being able to close that gap myself keeps my home and my jobs data safe. Most of the time outside sources find and provide better and faster resolutions to these issues than the company that owns the hardware.

As an IT professional, I take exception to the any rules that prevent me from changing the software on products I own. If properly configured open source software us more secure an allows me the freedom to customize hardware that I own. I honestly do not understand how people who legally purchase hardware can have the software locked. Sometimes companies do not update vulnerabilities or drop support of a product in favor of something newer. Having the ability to load my own or open sourced software keeps that hardware relevant and keeps me from wasting my money buying something that I do not need to.

I understand the want to make products more secure and I agree that products should be more secure. This is the wrong way to go about it.

I want the ability and should have the ability to secure my own data, hardware in a manner of my choosing. Being in the IT world I will read about an online threat or vulnerability and it will be several months before its patched. Me being able to close that gap myself keeps my home and my jobs data safe. Most of the time outside sources find and provide better and faster resolutions to these issues than the company that owns the 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: Joseph

Last Name: Gonzalez

Mailing Address: 3850 Swordfish Dr.

City: Cherry Valley

Country: United States

State or Province: IL

ZIP/Postal Code: 61016

Email Address: solarpm@comcast.net

Organization Name:

Comment: Hello,

As an informed college educated technology hobbyist and semi-political activist that currently resides in the United States of America, Illinois, Cherry Valley, 61016. My state and its representatives currently cannot afford to support yet another needless taxation agenda that would only further reduce the quality of life of the Union. Albeit another method to collect sorely needed tax revenue rite now the quality of life in this country is poor and after reading B. Benchhoff's web article titled, "Save WiFi: Act Now To Save WiFi from the FCC, (2015)" I cannot help but to feel strongly opposed to the latest FCC proposition and its undiscussed legal costs to implement if it were to become federal law.

Here are my main discrepancies with the RF firmware modification proposition:

- 1) This proposition is much too broad in scope and could bring a whole slew of legal challenges and expenditures that could introduce needless taxation into existence.
- 2) The publication date of the proposed FCC law is August 6th 2015 and the main website < <https://www.federalregister.gov/articles/2015/08/06/2015-18402/equipment-authorization-and-electronic-labeling-for-wireless-devices> > only takes comments until September 8th 2015. This is far too short a time period for any real public interest to be drawn up against this proposed FCC guideline.
- 3) Too few people probably even know about this proposed FCC law to say anything about such a topic regarding modifications of RF firmware.
- 4) The main web resource that takes comments or petitions has an overly complex outlay on how to submit any discrepancy about the proposed FCC law regarding modding RF firmware.
- 5) Not discussed in the cited article are the United States reasons for choosing not to involve themselves with trying to create a more transparent nation that already does far to little to replace, offset, or supplement the taxes people must pay for quality security and upgrades that could be better managed if businesses were to become more proactive and allow or inform their work force to query such topics like modding the firmware of RF devices.
- 6) Instead of fast tracking the development of more harmful federal laws meant to incriminate the individual committing RF firmware crimes more ought to be done to hold accountable the businesses that do not create secure devices. Businesses should be held accountable and the federal courts ought to monetarily penalize the businesses depending on the nature of the exploit. For example, if the exploit of a RF firmware were used in a terrorist plot then I would strongly favor criminalizing the individual(s) in such a case versus someone simply finding a means to exploit an RF firmware then seek to create a patent to profit from the development of others or pose as an undercover federal agent that has inside knowledge of hobbyists or the common researchers that must often closely involve themselves with hacker groups.
- 7) More effort should be placed into improving the data collection methods of ISP or software programs that assist ISP's regarding the materials, particularly the educated about the content they are researching.

Creating policies blindly without surveying those most closely involved with such articles, content, is clearly an irresponsible way to go about conducting big business irregardless of the amount of revenues involved in one ore more accounts. Also not discussed are the repercussions for individuals that continue the work of others that use such devices but work in different job roles. Like, what rites exist for those who are not directly involved with atrocious actions and heinous plots if someone else were to haphazardly? or unknowingly activate modded software or plug-in a device(s) that do not yet exist which could put into motion a chain of events even beyond ones death. What about the conflicts that might exist for lawful agents researching a deceased hackers code?

Lastly, looking at this topic full-circle so to speak there clearly exists no definate seperation between businesses, political leaders, and the minority that currently involves themselves most closely with such topics. Future agendas like this blindly point the finger and essentially make anybody the target, or wrongly accused. One must not forget this topic includes all lesser roles like educational systems that heavily rely on and largely support the technological empire the world has made to date. I leave you with this thought: how will homework worked on beyond the class need to differ in the future if this idea passes? Will students need to expose themselves and their identities to school servers that get hacked time and time again? How will our government manage these servers and what data will they be allowed to college when the student is signed-in? Our our childrens books spreading ideas that might otherwise need to be censored due to such law and is this possibly constitutional violation?

Hello,

As an informed college educated technology hobbyist and semi-political activist that currently resides in the United States of America, Illinois, Cherry Valley, 61016. My state and its representatives currently cannot afford to support yet another needless taxation agenda that would only further reduce the quality of life of the Union. Albeit another method to collect sorely needed tax revenue rite now the quality of life in this country is poor and after reading B. Benchoff's web article titled, "Save WiFi: Act Now To Save WiFi from the FCC, (2015)" I cannot help but to feel strongly opposed to the latest FCC proposition and its undiscussed legal costs to implement if it were to become federal law.

Here are my main discrepencies with the RF firmware modification proposition:

- 1) This proposition is much too broad in scope and could bring a whole slew of legal challenges and expenditures that could introduce needless taxation into existence.
- 2) The publication date of the proposed FCC law is August 6th 2015 and the main website < <https://www.federalregister.gov/articles/2015/08/06/2015-18402/equipment-authorization-and-electronic-labeling-for-wireless-devices> > only takes comments until September 8th 2015. This is far too short a time period for any real public interest to be drawn up against this proposed FCC guideline.
- 3) Too few people probably even know about this proposed FCC law to say anything about such a topic regarding modifications of RF firmware.
- 4) The main web resource that takes comments or petitions has an overly complex outlay on how to submit any discrepancy about the proposed FCC law regarding modding RF firmware.
- 5) Not discussed in the cited artifle are the United States reasons for choosing not to involve themselves with trying to create a more transparent nation that already does far to little to replace, offset, or supplement the taxes people must pay for quality security and upgrades that could be better managed if businesses were to become more proactive and allow or inform their work force to query such topics like modding the firmware of RF devices.
- 6) Instead of fast tracking the development of more harmful federal laws meant to incriminate the individual committing RF firmware crimes more ought to be done to hold accountable the businesses that do not create secure devices. Businesses should be held accountable and the federal courts ought to monitarily penalize the businesses depending on the nature of the exploit. For example, if the exploit of a RF firmware were used in a terrorist plot then I would strongly favor criminalizing the individual(s) in such a case versuse someone simply finding a means to exploit an RF firmware then seek to create a patent to profit from the development of others or pose as an undercover federal agent that has inside knowledge of hobbyists or the common researchists that must often closely involve themselves with hacker groups.
- 7) More effort should be placed into improving the data collection methods of ISP or software programs that assist ISP's regarding the materials, particularly the educated about the content they are researching.

Creating policies blindly without surveying those most closely involved with such articles, content, is clearly an irresponsible way to go about conducting big business irregardless of the amount of revenues involved in one ore more accounts. Also not discussed are the reproussions for individuals that continue the work of others that use such devices but work in different job roles. Like, what rites exist for those who are not direcly involved with atrocious actions and heineous plots if someone else were to haphazardly? or unknowingly activate modded software or plug-in a device(s) that do not yet exist which could put into motion a chain of events even beyond ones death. What about the conflicts that might exist for lawful agents researching a deceased hackers code?

Lastly, looking at this topic full-circle so to speak there clearly exists no definate seperation between businesses, political leaders, and the minority that currently involves themselves most closely with such topics. Future agendas like this blindly point the finger and essentially make anybody the target, or wrongly accused. One must not forget this topic includes all lesser roles like educational systems that heavily rely on and largely support the technological empire the world has made to date. I leave you with this thought: how will homework worked on beyond the class need to differ in the future if this idea passes? Will students need to expose themselves and their identities to school servers that get hacked time and time again? How will our government manage these servers and what data will they be allowed to college when the student is signed-in? Our our childrens books spreading ideas that might otherwise need to be censored due to such law and is this possibly constitutional violation?

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: Anderson

Mailing Address: 11014 Sagecanyon Dr.

City: Houston

Country: United States

State or Province: TX

ZIP/Postal Code: 77089

Email Address: indomidable@gmail.com

Organization Name:

Comment: I'm concerned about some of the wording in here, were it would be impossible for me to change the software/firmware on my computing devices...I already find the DMCA to only take away my rights as a Citizen. I pay a Sales tax not rental fee for my property, Ex. Router, PC/PC Components. So, rules that exclude my choices or those of my fellow citizens from doing research/modification of our devices, which we all know come shipped with security faults, where some manufacturers don't bother or are unable to provide fixes for these issues. Take 3. Responsible Parties for Certified Equipment

29. The grantee of certification is responsible for the compliance of the certified equipment. When another party modifies a device through either hardware or software changes without the authority of the original grantee, or incorporates a certified device into another host device, that party becomes responsible for the modified device's compliance and must obtain a new FCC ID for its product.

Translation in order for me to get drivers for my Wi-Fi card they can only come from X vendor (Horrible idea), When I put a Wi-fi card in my PC/Laptop whatever I may need to register with the FCC. Why?

Simply put this means only the vendor controls where the device can be used and what software can be run on it. Guaranteed monopoly in the guise of simplification of rules.

So, if the rule solely protects the "Rights" of the Vendor who's protecting the "Owners Rights" or are we renters?

Or is there some simplified application I can fill out saying I want to run OpenWRT on my Wi-Fi Router?

I find "The Commission proposed to enforce its importation rules against both the seller and the buyer." to be a bit disturbing if the buyer is a regular "human" citizen for personal use "family/home/research", not for resale/wholesale purposes. Personally I'd prefer the Seller to be responsible, due to the nature of all the rules that exist that no one outside the "know" even know about.

Basically, I'm all for simplification but not for broadening a vendors powers while diminishing my choices, or limiting progress for short term market value.

I'm concerned about some of the wording in here, were it would be impossible for me to change the software/firmware on my computing devices...I already find the DMCA to only take away my rights as a Citizen. I pay a Sales tax not rental fee for my property, Ex. Router, PC/PC Components. So, rules that exclude my choices or those of my fellow citizens from doing research/modification of our devices, which we all know come shipped with security faults, where

some manufacturers don't bother or are unable to provide fixes for these issues. Take 3. Responsible Parties for Certified Equipment

29. The grantee of certification is responsible for the compliance of the certified equipment. When another party modifies a device through either hardware or software changes without the authority of the original grantee, or incorporates a certified device into another host device, that party becomes responsible for the modified device's compliance and must obtain a new FCC ID for its product.

Translation in order for me to get drivers for my Wi-Fi card they can only come from X vendor (Horrible idea), When I put a Wi-fi card in my PC/Laptop whatever I may need to register with the FCC. Why?

Simply put this means only the vendor controls where the device can be used and what software can be run on it. Guaranteed monopoly in the guise of simplification of rules.

So, if the rule solely protects the "Rights" of the Vendor who's protecting the "Owners Rights" or are we renters?

Or is there some simplified application I can fill out saying I want to run OpenWRT on my Wi-Fi Router?

I find "The Commission proposed to enforce its importation rules against both the seller and the buyer." to be a bit disturbing if the buyer is a regular "human" citizen for personal use "family/home/research", not for resale/wholesale purposes. Personally I'd prefer the Seller to be responsible, due to the nature of all the rules that exist that no one outside the "know" even know about.

Basically, I'm all for simplification but not for broadening a vendors powers while diminishing my choices, or limiting progress for short term market value.

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: Collyer

Mailing Address: 3825 Ice Age Drive

City: Madison

Country: United States

State or Province: WI

ZIP/Postal Code: 53719

Email Address: ericcollyer@gmail.com

Organization Name:

Comment: I recommend that the FCC RESCIND its Proposed Rule, Document number 2015-18402 regarding wireless devices. The Proposed Rule is overbroad, would harm many communities of Americans, and is not warranted by the facts on the ground.

Although the FCC has the power to regulate equipment that generates radio frequencies, this is a heavy-handed rule that could be addressed other ways. Specifically, I am concerned about the ability of third parties to modify and create new firmware for consumer routers.

The proposed rule would require that router manufacturers lock down the RF portion of the router to obtain FCC approval. This lock down would prevent modification to the radios power, frequencies, etc to prevent it from radiating outside the specified limits. This is a laudable goal, but the application of this rule as written would result in undesirable consequences.

In practice, most radio functions are very tightly wedded to all the other factors of the hardware/software. The most likely way manufacturers would likely lock down the RF operation would be to make it impossible to modify any of the code in the routers.

There would be a number of adverse consequences both for me personally, to consumers in the US, and the networking industry. These consequences can be ameliorated by allowing the owners of routers to install their own code.

1) Security of the router. It is well known that vendor-supplied firmware for consumer routers often contain flaws. Just last week, the CERT released knowledge of a vulnerability to Belkin routers. See <http://www.kb.cert.org/vuls/id/201168> The ability to install well-tested, secure firmware into a router benefits all consumers. The ability for a person to update their own router on a regular basis (as opposed to many manufacturers seemingly lackadaisical schedule) preserves security.

2) Research into the field of computer networking. Non-traditional research efforts (outside academia) lead to real improvements in the state of computer networking. An example is the CeroWrt project that developed the fq\_codel algorithm. <http://www.bufferbloat.net/projects/cerowrt> The result of this multi-year effort was a major advance in performance for all routers. The fq\_codel code has been accepted into the Linux kernel and now runs in hundreds of millions of devices. As a member of the team that worked on this, I assert that without the ease of modification of a consumer router to prove out the ideas, this improvement would likely not have occurred.

3) Personal learning environments. Individuals, as well as network professionals, often use these consumer routers as

test beds for increased understanding of network operation. Losing the ability to reprogram the router would make it more expensive, if not prohibitive, for Americans to improve their knowledge and become more competitive.

4) I would incorporate all the other talking points listed on the Save WiFi page at:  
[https://libreplanet.org/wiki/Save\\_WiFi](https://libreplanet.org/wiki/Save_WiFi)

5) Finally, I want to address the FCC's original concern that these consumer routers are SDRs, and they must not be operated outside their original design parameters. While the goal of reducing radio frequency interference is important, the FCC has failed to demonstrate that the widespread practice of installing/updating firmware in consumer routers has caused actual problems. Furthermore, the FCC can use its current enforcement powers to monitor and shut down equipment that is interfering.

Creating a broad, wide-ranging rule to address a theoretical problem harms industry and individuals, and is an overreach of the rules necessary to preserve America's airwaves.

I recommend that the FCC RESCIND its Proposed Rule, Document number 2015-18402 regarding wireless devices. The Proposed Rule is overbroad, would harm many communities of Americans, and is not warranted by the facts on the ground.

Although the FCC has the power to regulate equipment that generates radio frequencies, this is a heavy-handed rule that could be addressed other ways. Specifically, I am concerned about the ability of third parties to modify and create new firmware for consumer routers.

The proposed rule would require that router manufacturers lock down the RF portion of the router to obtain FCC approval. This lock down would prevent modification to the radios power, frequencies, etc to prevent it from radiating outside the specified limits. This is a laudable goal, but the application of this rule as written would result in undesirable consequences.

In practice, most radio functions are very tightly wedded to all the other factors of the hardware/software. The most likely way manufacturers would likely lock down the RF operation would be to make it impossible to modify any of the code in the routers.

There would be a number of adverse consequences both for me personally, to consumers in the US, and the networking industry. These consequences can be ameliorated by allowing the owners of routers to install their own code.

1) Security of the router. It is well known that vendor-supplied firmware for consumer routers often contain flaws. Just last week, the CERT released knowledge of a vulnerability to Belkin routers. See <http://www.kb.cert.org/vuls/id/201168>. The ability to install well-tested, secure firmware into a router benefits all consumers. The ability for a person to update their own router on a regular basis (as opposed to many manufacturers seemingly lackadaisical schedule) preserves security.

2) Research into the field of computer networking. Non-traditional research efforts (outside academia) lead to real improvements in the state of computer networking. An example is the CeroWrt project that developed the fq\_codel algorithm. <http://www.bufferbloat.net/projects/cerowrt>. The result of this multi-year effort was a major advance in performance for all routers. The fq\_codel code has been accepted into the Linux kernel and now runs in hundreds of millions of devices. As a member of the team that worked on this, I assert that without the ease of modification of a consumer router to prove out the ideas, this improvement would likely not have occurred.

3) Personal learning environments. Individuals, as well as network professionals, often use these consumer routers as test beds for increased understanding of network operation. Losing the ability to reprogram the router would make it more expensive, if not prohibitive, for Americans to improve their knowledge and become more competitive.

4) I would incorporate all the other talking points listed on the Save WiFi page at:  
[https://libreplanet.org/wiki/Save\\_WiFi](https://libreplanet.org/wiki/Save_WiFi)

5) Finally, I want to address the FCC's original concern that these consumer routers are SDRs, and they must not be operated outside their original design parameters. While the goal of reducing radio frequency interference is important, the FCC has failed to demonstrate that the widespread practice of installing/updating firmware in consumer routers has caused actual problems. Furthermore, the FCC can use its current enforcement powers to monitor and shut down equipment that is interfering.

Creating a broad, wide-ranging rule to address a theoretical problem harms industry and individuals, and is an overreach of the rules necessary to preserve America's airwaves.

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: Wolfgang

Last Name: Smith

Mailing Address: 729 Stuart St

City: Helena

Country: United States

State or Province: MT

ZIP/Postal Code: 59601

Email Address:

Organization Name:

Comment: Please do not implement any rules that will restrict users' ability to install software of their choosing on their own devices. One of the great benefits of digital computers is their versatility. Any computer can be converted into a media player for television, it can become part of an autonomous robot, it can do anything the owner wants it to do. This is an important freedom for all users, and it should stretch to all devices, big or small. Wireless routers can be modified to block harmful malware and advertisements, they can be patched to fix critical security issues, and anything else the owner wants it to do.

The freedom to modify one's own devices is an important freedom. Please do not take it away.

Please do not implement any rules that will restrict users' ability to install software of their choosing on their own devices. One of the great benefits of digital computers is their versatility. Any computer can be converted into a media player for television, it can become part of an autonomous robot, it can do anything the owner wants it to do. This is an important freedom for all users, and it should stretch to all devices, big or small. Wireless routers can be modified to block harmful malware and advertisements, they can be patched to fix critical security issues, and anything else the owner wants it to do.

The freedom to modify one's own devices is an important freedom. Please do not take it away.

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: Lang

Mailing Address: 132 Indiana Ave

City: Elyria

Country: United States

State or Province: OH

ZIP/Postal Code: 440935

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.

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: wade

Last Name: Randolph

Mailing Address: 4232 SUNSET DR

City: LOS ANGELES

Country: United States

State or Province: CA

ZIP/Postal Code: 90027

Email Address: wade\_randolph@hotmail.com

Organization Name:

Comment: I'm asking that the FCC not implement 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 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.

The ability to run fully open source software on your devices will be severely hampered and possibly impossible with these new rules.

I'm asking that the FCC not implement 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 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.

The ability to run fully open source software on your devices will be severely hampered and possibly impossible with these new rules.

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: Daniel

Last Name: Abraham

Mailing Address: 410 Gallivan Blvd

City: Boston

Country: United States

State or Province: MA

ZIP/Postal Code: 02124

Email Address: dabraham@sweatshop.org

Organization Name: null

Comment: The proposed rule causes significant concern for information security posture. The legitimate goals of the FCC could be achieved in an alternate manner which does not cause the same widespread security vulnerabilities, by instead requiring that output power levels and any other critical parameters be limited to legal levels by a separate chip. This approach would be far superior to effectively banning proper security practice for the ENTIRE operating system and all utilities on the device, as the current proposal does.

1

The proposed rule requires that manufacturers disallow firmware updates (other than signed manufacturer updates, typically provided for only a very short time), makes it much more difficult to prevent incidents such as the \$45 million loss at TJX and the Target breach. In both cases, the victim companies were initially targeted because insecure wifi devices were in use. To reduce future occurrences of such breaches, it is imperative to be able to update devices which use wireless networking. Especially when a vulnerability such as Shellshock is discovered, it is imperative that risks be mitigated immediately.

Updates provided by the manufacturer may at first seem to be a possible solution, but are not actually a viable solution for two reasons. Manufacturers generally do not provide long-term updates, updates for devices more than about one-two years old. In many cases, no updates are offered at all to handle issues after the date of sale. It is not reasonable to anticipate that organizations and families will replace their network gear every year or two - firmware updates are needed, including for devices which are a few years old. Perhaps ESPECIALLY for devices which are a few years old.

Secondly, updates from the manufacturer are not a viable solution for more sensitive organizations due to the response time required. In the first 24 hours after the release of Shellshock, thousands of systems were compromised. It is critically important to mitigate the threat quickly. Manufacturer full updates were not available for several days to several months, as we first discussed the best long term solution and that solution propagated downstream from the authors, to the subsystem maintainers, distribution maintainers, OEM repackagers, and finally out to customers after testing at each level. In the meantime, temporary MITIGATIONS were performed on-site by network engineers and security contractors. These vital mitigations which protected sensitive networks in the interim would be illegal and prevented by manufacturer locks under the proposed rule. In simple terms, the proposal makes it illegal to manufacturer equipment which can be \_quickly\_ protected against new threats to our cyber security.

2

Another problem is that the manufacturer default firmware, with all available features designed to be as easily

accessible as possible, is not appropriate for any environment in which security is a concern. A central tenet of information security, and security in general, is that the attack surface should be as small as possible - services not needed for a particular installation should not be installed and enabled. The only software which definitely cannot be exploited is software which is not installed or not enabled. Therefore, the most secure firmware tends to be that with as many features \_removed\_ as possible, with only those items required for the current role installed.

Manufacturer firmware does the exact opposite, for ease-of-use by ordinary consumers. All services which might be of use to any customer are installed, enabled, and wide open for abuse. Firmware which can be customized, trimmed down to provide only the required functionality (and therefore the smallest attack surface).

3

Lastly, these devices are frequently used as active security devices, such as firewalls and VPN endpoints. To require that these ubiquitous and therefore inexpensive devices be replaced with far more expensive niche versions branded as security devices necessarily reduces the number of security checkpoints which will be installed in networks. As an example, consider the twentyfold cost difference between a SOHO Cisco router and a Cisco firewall appliance which internally contains similar hardware. The small office can easily afford a firewall based on a third-party firmware for the ubiquitous router, and such a firewall can well meet the needs of a small office. They are unlikely to purchase a dedicated firewall from the same company costing several thousand dollars. Therefore, disallowing the third-party firewall firmware results in no firewall being used at all.

Overall, the proposed rule is creates significant security problems in a number of ways. All of these issues could be avoided, and the radio emission still controlled, by instead requiring that radio output power or other essential RF parameters be limited by a chip separate from the (upgradeable) main system.

The proposed rule causes significant concern for information security posture. The legitimate goals of the FCC could be achieved in an alternate manner which does not cause the same widespread security vulnerabilities, by instead requiring that output power levels and any other critical parameters be limited to legal levels by a separate chip. This approach would be far superior to effectively banning proper security practice for the ENTIRE operating system and all utilities on the device, as the current proposal does.

1

The proposed rule requires that manufacturers disallow firmware updates (other than signed manufacturer updates, typically provided for only a very short time), makes it much more difficult to prevent incidents such as the \$45 million loss at TJX and the Target breach. In both cases, the victim companies were initially targeted because insecure wifi devices were in use. To reduce future occurrences of such breaches, it is imperative to be able to update devices which use wireless networking. Especially when a vulnerability such as Shellshock is discovered, it is imperative that risks be mitigated immediately.

Updates provided by the manufacturer may at first seem to be a possible solution, but are not actually a viable solution for two reasons. Manufacturers generally do not provide long-term updates, updates for devices more than about one-two years old. In many cases, no updates are offered at all to handle issues after the date of sale. It is not reasonable to anticipate that organizations and families will replace their network gear every year or two - firmware updates are needed, including for devices which are a few years old. Perhaps ESPECIALLY for devices which are a few years old.

Secondly, updates from the manufacturer are not a viable solution for more sensitive organizations due to the response time required. In the first 24 hours after the release of Shellshock, thousands of systems were compromised. It is critically important to mitigate the threat quickly. Manufacturer full updates were not available for several days to several months, as we first discussed the best long term solution and that solution propagated downstream from the authors, to the subsystem maintainers, distribution maintainers, OEM repackagers, and finally out to customers after testing at each level. In the meantime, temporary MITIGATIONS were performed on-site by network engineers and security contractors. These vital mitigations which protected sensitive networks in the interim would be illegal and prevented by manufacturer locks under the proposed rule. In simple terms, the proposal makes it illegal to manufacturer

equipment which can be \_quickly\_ protected against new threats to our cyber security.

2

Another problem is that the manufacturer default firmware, with all available features designed to be as easily accessible as possible, is not appropriate for any environment in which security is a concern. A central tenet of information security, and security in general, is that the attack surface should be as small as possible - services not needed for a particular installation should not be installed and enabled. The only software which definitely cannot be exploited is software which is not installed or not enabled. Therefore, the most secure firmware tends to be that with as many features \_removed\_ as possible, with only those items required for the current role installed.

Manufacturer firmware does the exact opposite, for ease-of-use by ordinary consumers. All services which might be of use to any customer are installed, enabled, and wide open for abuse. Firmware which can be customized, trimmed down to provide only the required functionality (and therefore the smallest attack surface).

3

Lastly, these devices are frequently used as active security devices, such as firewalls and VPN endpoints. To require that these ubiquitous and therefore inexpensive devices be replaced with far more expensive niche versions branded as security devices necessarily reduces the number of security checkpoints which will be installed in networks. As an example, consider the twentyfold cost difference between a SOHO Cisco router and a Cisco firewall appliance which internally contains similar hardware. The small office can easily afford a firewall based on a third-party firmware for the ubiquitous router, and such a firewall can well meet the needs of a small office. They are unlikely to purchase a dedicated firewall from the same company costing several thousand dollars. Therefore, disallowing the third-party firewall firmware results in no firewall being used at all.

Overall, the proposed rule is creates significant security problems in a number of ways. All of these issues could be avoided, and the radio emission still controlled, by instead requiring that radio output power or other essential RF parameters be limited by a chip separate from the (upgradeable) main system.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ray

Last Name: Smith

Mailing Address: 4220 W ANGELA DR

City: GLENDALE

Country: United States

State or Province: AZ

ZIP/Postal Code: 85308

Email Address: z03789@msn.com

Organization Name:

Comment: I am asking the FCC to not implement this rule, as it removes the right of users to install software of their own choosing, such as linux. Also, this rule would limit the following:

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

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

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

Not fixing security holes either feeds cyberthreats or increases electronic waste.

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

Thank you

I am asking the FCC to not implement this rule, as it removes the right of users to install software of their own choosing, such as linux. Also, this rule would limit the following:

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

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

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

Not fixing security holes either feeds cyberthreats or increases electronic waste.

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

Thank you

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: Layman

Mailing Address: 201 E Grattan St

City: Harrisonburg

Country: United States

State or Province: VA

ZIP/Postal Code: 22801

Email Address:

Organization Name:

Comment: This proposed rule is both excessive an not necessary. Rules like this stifle innovation and learning my making experimentation illegal. Additionally this opens a huge security hole that could be abused by terrorists and others similar groups by making it illegal to patch firmware or similar software that is no longer being updated by the manufacturer to third party or open source software.

The better way to fix the issues mentioned in this document are through education and not legislation.

This proposed rule is both excessive an not necessary. Rules like this stifle innovation and learning my making experimentation illegal. Additionally this opens a huge security hole that could be abused by terrorists and others similar groups by making it illegal to patch firmware or similar software that is no longer being updated by the manufacturer to third party or open source software.

The better way to fix the issues mentioned in this document are through education and not legislation.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: T

Last Name: H

Mailing Address: Local Address

City: San Jose

Country: United States

State or Province: CA

ZIP/Postal Code: 95135

Email Address:

Organization Name:

Comment: This rule HARMS CONSUMER SECURITY!

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

This rule damages American consumers ability to manage their own networks.

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

Please consider modifying this rule to ensure consumers' ability to continue using open-source firmware on their network routers.

This rule HARMS CONSUMER SECURITY!

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

This rule damages American consumers ability to manage their own networks.

As written, the rules and recommendations of the commission will prevent the installation of traditional free and open

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

Please consider modifying this rule to ensure consumers' ability to continue using open-source firmware on their network routers.

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: Itamar

Last Name: Gilad

Mailing Address: 139 Katzanelson street, Apartment 2

City: Givatayim

Country: Israel

State or Province: IL

ZIP/Postal Code: 53258

Email Address: FCC@modprobe.net

Organization Name:

Comment: The proposed measures will force OEMs and vendors of wireless home and travel routers to prevent any ability to load alternative software on the device, since these devices almost exclusively rely on a SoC (System-on-Chip) design, where the wireless controller and the main processing unit are integrated into the same chip, and running the same software.

This will destroy an entire eco-system for users and developers of open-source firmware solutions for small routers (lead by the OpenWRT project). It will also kill the entire world of commercial product that currently enjoy that ecosystem to re-purpose the same hardware modules and SoC which exist in commercial routers, thereby potentially raising the entry costs and the end client prices for a great variety of consumer products that use WiFi.

The proposed measures will force OEMs and vendors of wireless home and travel routers to prevent any ability to load alternative software on the device, since these devices almost exclusively rely on a SoC (System-on-Chip) design, where the wireless controller and the main processing unit are integrated into the same chip, and running the same software.

This will destroy an entire eco-system for users and developers of open-source firmware solutions for small routers (lead by the OpenWRT project). It will also kill the entire world of commercial product that currently enjoy that ecosystem to re-purpose the same hardware modules and SoC which exist in commercial routers, thereby potentially raising the entry costs and the end client prices for a great variety of consumer products that use WiFi.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jeffrey

Last Name: Cuscutis

Mailing Address: 9049 Vineyard Lake Drive

City: Plantation

Country: United States

State or Province: FL

ZIP/Postal Code: 33324

Email Address: jeff.cuscutis@gmail.com

Organization Name:

Comment: Locking down these devices will not make us safer, they will just hide problems and prevent fixes, particularly those made by individuals when a device manufacturer no longer does so.

Locking down these devices will not make us safer, they will just hide problems and prevent fixes, particularly those made by individuals when a device manufacturer no longer does 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: Michael

Last Name: Knight

Mailing Address: 1199 Vance Ave

City: Memphis

Country: United States

State or Province: TN

ZIP/Postal Code: 38104

Email Address: kk4ioh@gmail.com

Organization Name: HamWAN Memphis Metro

Comment: Please do not pass this.

This a a knee jerk solution where instead of dealing with people who break laws and punishes people who need to fix their hardware or use it in other ways legally.

This would completely stop and prevent hardware that is currently available from being used for emergency communications legally under part 97 by licensed ham radio operators.

There are no other sources available for this purpose.

On more than one occasion doing this repaired hardware that I would have needed to just throw away filling the dump with metals and pollution.

Please do not pass this.

This a a knee jerk solution where instead of dealing with people who break laws and punishes people who need to fix their hardware or use it in other ways legally.

This would completely stop and prevent hardware that is currently available from being used for emergency communications legally under part 97 by licensed ham radio operators.

There are no other sources available for this purpose.

On more than one occasion doing this repaired hardware that I would have needed to just throw away filling the dump with metals and pollution.

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: carlin

Mailing Address: 4957 ney dr.

City: nanaimo

Country: Canada

State or Province: British Columbia

ZIP/Postal Code: v9v1t9

Email Address:

Organization Name:

Comment: After reading, rereading and rererereading this proposal ...

Flat out.

This is just wrong.

The long term damage in so many ways [conceivable and unforeseeable] this proposal will do is truly monstrous.

I strongly think this proposal should NOT pass.

After reading, rereading and rererereading this proposal ...

Flat out.

This is just wrong.

The long term damage in so many ways [conceivable and unforeseeable] this proposal will do is truly monstrous.

I strongly think this proposal should NOT pass.

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: Philipp

Mailing Address: 142 DeWitt Ave

City: Napa

Country: United States

State or Province: CA

ZIP/Postal Code: 94558

Email Address: idahobob@aol.com

Organization Name: Color by Number

Comment: /

My main complaint is with section b. Devices with Software-Based Capabilities.

Being able to change software is one of the best reasons to use SDR. This allows for fixing bugs, patching security holes, and for global abilities.

Not allow firmware updates will Hurt consumers by driving up cost, locking in designs, and exposure to vulnerabilities that cannot be fixed. The cost will come from both the creation and implementation of the security features (and the cat and mouse game of keeping it secure), as well as forcing a hardware replacement, instead of a simple firmware change when needed.

It will also open up huge security risks to all devices that use a SDR radio device. Consumers will not be able to update for security easily, and with zero cost, unlike having to replace the hardware.

With infrastructure devices, such as embedded controls (like thermostats, security cameras, "Internet of Things") devices, it is even more necessary to be able to easily updated. The cost of doing a physical update could be as large if not larger than the original device. Thus industrial buildings, chemical plants, power plants, etc. will be left vulnerable.

Last, forcing locked in firmware will make being able to sell (or buy) a device and use it elsewhere. For example a cell phone or router made for US market, to be taken to Japan and used there (with new firmware) then brought back to the US. The new rules would force consumers to purchase new devices, rather than temporarily retask their existing devices with a temporary firmware update.

/

My main complaint is with section b. Devices with Software-Based Capabilities.

Being able to change software is one of the best reasons to use SDR. This allows for fixing bugs, patching security holes, and for global abilities.

Not allow firmware updates will Hurt consumers by driving up cost, locking in designs, and exposure to vulnerabilities that cannot be fixed. The cost will come from both the creation and implementation of the security features (and the cat and mouse game of keeping it secure), as well as forcing a hardware replacement, instead of a

simple firmware change when needed.

It will also open up huge security risks to all devices that use a SDR radio device. Consumers will not be able to update for security easily, and with zero cost, unlike having to replace the hardware.

With infrastructure devices, such as embedded controls (like thermostats, security cameras, "Internet of Things") devices, it is even more necessary to be able to easily updated. The cost of doing a physical update could be as large if not larger than the original device. Thus industrial buildings, chemical plants, power plants, etc. will be left vulnerable.

Last, forcing locked in firmware will make being able to sell (or buy) a device and use it elsewhere. For example a cell phone or router made for US market, to be taken to Japan and used there (with new firmware) then brought back to the US. The new rules would force consumers to purchase new devices, rather than temporarily retask their existing devices with a temporary firmware update.

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: Boorstin

Mailing Address: sboorstin@gmail.com

City: Washington, D.C.

Country: United States

State or Province: DC

ZIP/Postal Code: 20016

Email Address: sboorstin@gmail.com

Organization Name: Boorstin Inc

Comment: Please do not ban Linux by forcing manufacturers to lock down their devices. Linux is the best thing in the world since IBM.

Please do not ban Linux by forcing manufacturers to lock down their devices. Linux is the best thing in the world since IBM.

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: Waldman

Mailing Address: 17 Chelsea ct

City: Chagrin falls

Country: United States

State or Province: OH

ZIP/Postal Code: 44022

Email Address: Ansilator@hotmail.com

Organization Name:

Comment: This regulation is a bad idea. Router firmware can and should be allowed to be modified by its users for security and safety.

I urge the FCC to reject this misinformed idea.

This regulation is a bad idea. Router firmware can and should be allowed to be modified by its users for security and safety.

I urge the FCC to reject this misinformed idea.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jonathan

Last Name: Fraser

Mailing Address: omitted

City: Vancouver

Country: Canada

State or Province: British Columbia

ZIP/Postal Code: omitted

Email Address:

Organization Name:

Comment: I find paragraph 26 deeply worrying. It is a federal endorsement of that fact that when I buy a piece of equipment, I don't fully own it. While the restriction is meant specifically to limit the radio of the device the practical implementation will be a full device lockout. There are no such things as wireless routers any more, there are only computers which spend most of their time routing packets. There is very little difference between a modern wireless router and a personal tablet computer. Do the rules apply to tablets, can I not replace the firmware on those?

The truth of the matter is, users do not install third party firmware to violate rules, they do so to gain access to basic features that should be available on all routers but are conveniently omitted by the manufacturer, things such as an IPV6 firewall (yes, I purchased a router which supported IPV6 but didn't contain a firewall DIR-815) or having a DHCP server which is limited to 192.168.1.0/24 instead of all the private subnets. These are just a small sampling of the strange restrictions which router manufacturers place in their software and should exemplify the need for users to take control and manage their networks as they see fit.

While the proposed rule change is obviously designed to ensure that devices are within the FCC mandated limits for wireless, the actual implementation will not be restricted to just the wireless components and will have a chilling effect on the ability for consumers to use the hardware which they rightfully own. I respectfully submit that the FCC limits themselves to items as sold. This means that should a vendor sell third party firmware then they fall under the requirement, but forcing vendor to lock their own customers out of the equipment they rightfully own is tantamount to saying that one can only ever rent a device.

I find paragraph 26 deeply worrying. It is a federal endorsement of that fact that when I buy a piece of equipment, I don't fully own it. While the restriction is meant specifically to limit the radio of the device the practical implementation will be a full device lockout. There are no such things as wireless routers any more, there are only computers which spend most of their time routing packets. There is very little difference between a modern wireless router and a personal tablet computer. Do the rules apply to tablets, can I not replace the firmware on those?

The truth of the matter is, users do not install third party firmware to violate rules, they do so to gain access to basic features that should be available on all routers but are conveniently omitted by the manufacturer, things such as an IPV6 firewall (yes, I purchased a router which supported IPV6 but didn't contain a firewall DIR-815) or having a DHCP server which is limited to 192.168.1.0/24 instead of all the private subnets. These are just a small sampling of the strange restrictions which router manufacturers place in their software and should exemplify the need for users to take control and manage their networks as they see fit.

While the proposed rule change is obviously designed to ensure that devices are within the FCC mandated limits for

wireless, the actual implementation will not be restricted to just the wireless components and will have a chilling effect on the ability for consumers to use the hardware which they rightfully own. I respectfully submit that the FCC limits themselves to items as sold. This means that should a vendor sell third party firmware then they fall under the requirement, but forcing vendor to lock their own customers out of the equipment they rightfully own is tantamount to saying that one can only ever rent a 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: Andrea

Last Name: Neri

Mailing Address: Via Emilia 142

City: Udine

Country: Italy

State or Province: UD

ZIP/Postal Code: 33100

Email Address:

Organization Name:

Comment: I ask the FCC to refrain from implementing such measures on restricting the modification of U-NII devices. It will hamper security, commerce, and innovation.

\* manufacturers are known for their terrible record in providing security fixes, most of the devices involved are \*never\* updated during their lifetime, instead preferring to just ignore current devices and iterate on a new product. This has come to its ultimate consequences recently, when a software bug affecting a \*billion\* of smartphones has been discovered and wont be fixed for almost all of the affected devices. 3rd-party firmwares are the only safeguard against this kind of situations: manufactures are not and cannot be forced to provide security fixes.

\* Without the ability to modify the software running on these devices, nothing more than the very limited, more lucrative use cases addressed by the manufacturer would be implemented. This leaves behind advanced and/or custom scenarios which businesses could integrate on their services/products with very small costs by replacing the software.

\* Research and innovation in wireless communications, ranging from entirely new designs, models and protocols to software implementations, would basically come to an halt, severely harmed by the unavailability of low-cost, readily-available solutions upon which to experiment. Community Mesh Networks are entirely reliant on the ability to customize low-cost networking equipment.

\* These rules are overreaching and not even helping in ensuring compliance. Virtually none of the FCC rule breaches is due to 3rd-party software modification. It is however \*still\* possible to trivially enable non-compliant modes on unmodified devices on major wireless equipment manufactures.

Thanks for listening.

I ask the FCC to refrain from implementing such measures on restricting the modification of U-NII devices. It will hamper security, commerce, and innovation.

\* manufacturers are known for their terrible record in providing security fixes, most of the devices involved are \*never\* updated during their lifetime, instead preferring to just ignore current devices and iterate on a new product. This has come to its ultimate consequences recently, when a software bug affecting a \*billion\* of smartphones has been discovered and wont be fixed for almost all of the affected devices. 3rd-party firmwares are the only safeguard against this kind of situations: manufactures are not and cannot be forced to provide security fixes.

\* Without the ability to modify the software running on these devices, nothing more than the very limited, more

lucrative use cases addressed by the manufacturer would be implemented. This leaves behind advanced and/or custom scenarios which businesses could integrate on their services/products with very small costs by replacing the software.

\* Research and innovation in wireless communications, ranging from entirely new designs, models and protocols to software implementations, would basically come to an halt, severely harmed by the unavailability of low-cost, readily-available solutions upon which to experiment. Community Mesh Networks are entirely reliant on the ability to customize low-cost networking equipment.

\* These rules are overreaching and not even helping in ensuring compliance. Virtually none of the FCC rule breaches is due to 3rd-party software modification. It is however *\*still\** possible to trivially enable non-compliant modes on unmodified devices on major wireless equipment manufactures.

Thanks for listening.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Charles

Last Name: Cotton

Mailing Address: 110 Eagle Lakes Dr.

City: Friendswood

Country: United States

State or Province: TX

ZIP/Postal Code: 77546

Email Address:

Organization Name:

Comment: I am opposed to the proposed rule. It is both unnecessary and is fertile ground for unintended consequences.

An example of the harm this rule would cause can be seen in the Amateur Radio service development of the HSMM-MESH system. This voluntary system is being developed to serve as an RF system for data and voice communication much like the Internet. It can be deployed in minutes to disaster areas that have lost data transmission capability through the Internet. The HSMM-MESH system used WiFi routers by "flashing" or changing the firmware. The proposed rule would bring this much-needed service to Americans to a halt.

This is but one example of how the proposed rule would stymie research and innovation.

Respectfully,  
Charles Cotton

I am opposed to the proposed rule. It is both unnecessary and is fertile ground for unintended consequences.

An example of the harm this rule would cause can be seen in the Amateur Radio service development of the HSMM-MESH system. This voluntary system is being developed to serve as an RF system for data and voice communication much like the Internet. It can be deployed in minutes to disaster areas that have lost data transmission capability through the Internet. The HSMM-MESH system used WiFi routers by "flashing" or changing the firmware. The proposed rule would bring this much-needed service to Americans to a halt.

This is but one example of how the proposed rule would stymie research and innovation.

Respectfully,  
Charles Cotton

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: Marlon

Last Name: Sherman

Mailing Address: 4134 Redding Street

City: Oakland

Country: United States

State or Province: CA

ZIP/Postal Code: 94619

Email Address: marloony@gmail.com

Organization Name:

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.

- 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.
- Not fixing security holes either feeds cyberthreats or increases electronic waste.

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.

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.

- 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.
- Not fixing security holes either feeds cyberthreats or increases electronic waste.

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: Jeroen

Last Name: Hillegers

Mailing Address: Le Mairehof 5

City: Arnhem

Country: Netherlands

State or Province: Gelderland

ZIP/Postal Code: 6828RA

Email Address:

Organization Name:

Comment: As a citizen of the sovereign nation of the kingdom of the Netherlands, wish to submit a formal complaint against the illegalization of modified firmware for radio-devices like routers or similar. I am against this propopsal from the FCC, because the FCC has broad power that can influence the manufacturing of devices even if they aren't produced or sold in the United States of America. That effecively could mean regulatory oppression from the FCC in nations it has no jurisdiction over. The United States has since it's existense Always been a champion in the realm of individual and busisness freedom and that freedom is seriously impeded with this proposal. There are good rpractical reasons that such kind of restriction can also have grave negative consequences that actually undermine the principles of the FCC and consumer protection. For example: Individual or groups of users will no longer be able to modify firmware to suit specific reasonable needs without fear of potential reprisal. Researchers can no longer find weaknesses in firmware and path them before and if manufacturers are able and wiling to patch dangerous firmware flaws. The impediment to the survival of open firmware businessess, router manufacturers, researchers and enthousisast, even carying the risk of stiffling innovation and destroying much goodwill. And the most essential consumer right it infringes upon is the freedom for a consumer to use and modify in a reasonable manner, that has no negative impact on others, which is immoral and should in fact be that what should be considered illegal. I thank you for your time and consideration.

As a citizen of the sovereign nation of the kingdom of the Netherlands, wish to submit a formal complaint against the illegalization of modified firmware for radio-devices like routers or similar. I am against this propopsal from the FCC, because the FCC has broad power that can influence the manufacturing of devices even if they aren't produced or sold in the United States of America. That effecively could mean regulatory oppression from the FCC in nations it has no jurisdiction over. The United States has since it's existense Always been a champion in the realm of individual and busisness freedom and that freedom is seriously impeded with this proposal. There are good rpractical reasons that such kind of restriction can also have grave negative consequences that actually undermine the principles of the FCC and consumer protection. For example: Individual or groups of users will no longer be able to modify firmware to suit specific reasonable needs without fear of potential reprisal. Researchers can no longer find weaknesses in firmware and path them before and if manufacturers are able and wiling to patch dangerous firmware flaws. The impediment to the survival of open firmware businessess, router manufacturers, researchers and enthousisast, even carying the risk of stiffling innovation and destroying much goodwill. And the most essential consumer right it infringes upon is the freedom for a consumer to use and modify in a reasonable manner, that has no negative impact on others, which is immoral and should in fact be that what should be considered illegal. I thank you for your time and 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: Jeremy

Last Name: Karpenske

Mailing Address: 635 Northern Mdws #102

City: Menomonie

Country: United States

State or Province: WI

ZIP/Postal Code: 54751

Email Address: stormpix1@gmail.com

Organization Name:

Comment: Please do not take away our freedom to install the software of our choosing on our wireless devices. This will severely limit the stability, features, and security of our devices. For instance, on my ASUS router, I use a custom firmware that is patched and improved more often than the default firmware. In fact, some of the patches and fixes that the custom firmware's author implements are then adopted by ASUS and incorporated into their stock firmware. This cooperation and innovation would be halted if users are not allowed to install custom software on the devices they own. Please support freedom, security, and innovation by not implementing rules that restrict or remove our ability to install the software of our choice.

Please do not take away our freedom to install the software of our choosing on our wireless devices. This will severely limit the stability, features, and security of our devices. For instance, on my ASUS router, I use a custom firmware that is patched and improved more often than the default firmware. In fact, some of the patches and fixes that the custom firmware's author implements are then adopted by ASUS and incorporated into their stock firmware. This cooperation and innovation would be halted if users are not allowed to install custom software on the devices they own. Please support freedom, security, and innovation by not implementing rules that restrict or remove our ability to install the software of our choice.

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: Olekandr

Last Name: PikoZh

Mailing Address: Not specified to protect privacy

City: Kiev

Country: Ukraine

State or Province: Kyivska oblast

ZIP/Postal Code: 01034

Email Address:

Organization Name:

Comment: The following text:

"Manufacturers of any radio including certified modular transmitters which includes a software defined radio must take steps to ensure that only software that has been approved with a particular radio can be loaded into that radio. The software must not allow the installers or end-user to operate the transmitter with operating frequencies, output power, modulation types or other radio frequency parameters outside those that were approved. Manufacturers may use means including, but not limited to the use of a private network that allows only authenticated users to download software, electronic signatures in software or coding in hardware that is decoded by software to verify that new software can be legally loaded into a device to meet these requirements." (80 FR 46922)

creates fear, that if the proposed rule will be accepted, opportunities of regular device users for setting up free/alternative firmwares on their devices will decrease.

This may slow down scientific and technical progress in fields related to usage of radio devices (e.g. finding vulnerabilities in protocols, creating experimental mesh networks, etc).

The following text:

"Manufacturers of any radio including certified modular transmitters which includes a software defined radio must take steps to ensure that only software that has been approved with a particular radio can be loaded into that radio. The software must not allow the installers or end-user to operate the transmitter with operating frequencies, output power, modulation types or other radio frequency parameters outside those that were approved. Manufacturers may use means including, but not limited to the use of a private network that allows only authenticated users to download software, electronic signatures in software or coding in hardware that is decoded by software to verify that new software can be legally loaded into a device to meet these requirements." (80 FR 46922)

creates fear, that if the proposed rule will be accepted, opportunities of regular device users for setting up free/alternative firmwares on their devices will decrease.

This may slow down scientific and technical progress in fields related to usage of radio devices (e.g. finding vulnerabilities in protocols, creating experimental mesh networks, etc).

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: Dorsey

Mailing Address: 212 Thomas Nelson Ln.

City: Williamsburg

Country: United States

State or Province: VA

ZIP/Postal Code: 23185

Email Address:

Organization Name:

Comment: Please do not implement rules prohibiting users from installing the software of their choice on the hardware of their choice.

Prohibiting manufacturers from allowing users to make firmware updates is basically freezing configurations so that any bugs, any vulnerabilities, are forever stuck on those machines. The beauty of the digital world is that equipment can be readily upgraded and bugs fixed in the field.

In a day when new security holes are being found right and left, doing something that makes it harder for users to fix known security holes seems like a very foolish thing to do.

Please do not implement rules prohibiting users from installing the software of their choice on the hardware of their choice.

Prohibiting manufacturers from allowing users to make firmware updates is basically freezing configurations so that any bugs, any vulnerabilities, are forever stuck on those machines. The beauty of the digital world is that equipment can be readily upgraded and bugs fixed in the field.

In a day when new security holes are being found right and left, doing something that makes it harder for users to fix known security holes seems like a very foolish thing to do.

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: Kiss

Last Name: Pista

Mailing Address: kipi@freemail.hu

City: Budapest

Country: Hungary

State or Province: BP

ZIP/Postal Code: 1111

Email Address:

Organization Name:

Comment: Nincs szksgnk tbb vendorlockin eszkzre.

Nincs szksgnk tbb vendorlockin eszkzre.