

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: Jeramie

Last Name: Wiseman

Mailing Address: 3387 Suncrest Ave.

City: San Jose

Country: United States

State or Province: CA

ZIP/Postal Code: 95132

Email Address: ho0kedonph0enix@yahoo.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. 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. These new rules will make it extremely difficult if not illegal, to make an open source baseband for cellphones to prevent rogue towers like Stingrays. It will also harm any attempts to build open source cell towers and systems.

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. 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. These new rules will make it extremely difficult if not illegal, to make an open source baseband for cellphones to prevent rogue towers like Stingrays. It will also harm any attempts to build open source cell towers and systems.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ryan

Last Name: Dietrich

Mailing Address: 4028 North Cove Drive

City: Provo

Country: United States

State or Province: UT

ZIP/Postal Code: 84604

Email Address: ryan.dietrich@gmail.com

Organization Name:

Comment: Please do not remove the ability to use DD-WRT/Tomato/Custom firmware.

Please do not remove the ability to use DD-WRT/Tomato/Custom firmware.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ryan

Last Name: Grogg

Mailing Address: 405 west church street

City: mason

Country: United States

State or Province: OH

ZIP/Postal Code: 45040

Email Address: ryan.grogg@gmail.com

Organization Name:

Comment: Public servants of the Federal Communications Commission,

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

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

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

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

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

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

bad" category of regulatory ideas.

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: Richard

Last Name: beavers

Mailing Address: 2822 74th pl

City: lubbock

Country: United States

State or Province: TX

ZIP/Postal Code: 79423

Email Address: r.t.beavers@gmail.com

Organization Name:

Comment: This is another appalling idea to limit the freedom of use of something I payed for and own. You can no more tell me what to do with my banana than my computer or router. Stop this now before it becomes embarrassing

This is another appalling idea to limit the freedom of use of something I payed for and own. You can no more tell me what to do with my banana than my computer or router. Stop this now before it becomes embarrassing

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Justin

Last Name: Dale

Mailing Address: 4065 Jamie Drive

City: Hamilton

Country: United States

State or Province: OH

ZIP/Postal Code: 45011

Email Address: justindale2@gmail.com

Organization Name:

Comment: Public servants of the Federal Communications Commission,

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

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

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

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

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

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

bad" category of regulatory ideas.

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: Geoffrey

Last Name: Wossum

Mailing Address: 4550 Excel Pkwy.

City: Addison

Country: United States

State or Province: TX

ZIP/Postal Code: 75001-5713

Email Address: gwossum@lrsus.com

Organization Name: Long Range Systems, LLC.

Comment: As both a professional embedded systems developer and a hobbyist, this new rule would create many issues.

Modifying off-the-shelf hardware is a way that new ideas can be prototyped. Depending on the design, off-the-shelf hardware running custom firmware can even be a final product. These new rules would create substantial obstacles to innovation in the wireless realm for both businesses and hobbyists. I strong advise against enacting these rules.

As both a professional embedded systems developer and a hobbyist, this new rule would create many issues. Modifying off-the-shelf hardware is a way that new ideas can be prototyped. Depending on the design, off-the-shelf hardware running custom firmware can even be a final product. These new rules would create substantial obstacles to innovation in the wireless realm for both businesses and hobbyists. I strong advise against enacting these 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: Allan

Last Name: Wegan

Mailing Address: Segeberger Chaussee 32

City: Norderstedt

Country: Germany

State or Province: Schleswig-Holstein

ZIP/Postal Code: 22850

Email Address: allanwegan@allanwegan.de

Organization Name: null

Comment: As i understand, the intention of the proposed rule is to protect the shared medium (radio frequency spectrum) against misbehaviour of radios contained in wireless networking devices. That intention is good and just. It is cheaply possible to guarantee standard-obeying operation of wireless transmitters without hindering the use of alternate router firmware (DDWrt, OpenWRT, other Linuxes). It only has to be the radio controller itself, that has to be modified so it could technically not violate the rules. There is no need to forbid the use of alternate firmware for the device containing the radio controller.

Please adjust the proposal so that it makes clear that the use of alternate router firmware such as DDWrt or OpenWrt would be still allowed as long as it does not lead to rule-violating operation of the radio controller. The freedom to use other firmwares or operationg systems on devices capable of wireless communication is important for a lot of commercial and non-commercial projects. One of wich is "Freifunk" who builds communal mesh networks that also allow the poor to participate in modern cultural life on the internet.

As i understand, the intention of the proposed rule is to protect the shared medium (radio frequency spectrum) against misbehaviour of radios contained in wireless networking devices. That intention is good and just. It is cheaply possible to guarantee standard-obeying operation of wireless transmitters without hindering the use of alternate router firmware (DDWrt, OpenWRT, other Linuxes). It only has to be the radio controller itself, that has to be modified so it could technically not violate the rules. There is no need to forbid the use of alternate firmware for the device containing the radio controller.

Please adjust the proposal so that it makes clear that the use of alternate router firmware such as DDWrt or OpenWrt would be still allowed as long as it does not lead to rule-violating operation of the radio controller. The freedom to use other firmwares or operationg systems on devices capable of wireless communication is important for a lot of commercial and non-commercial projects. One of wich is "Freifunk" who builds communal mesh networks that also allow the poor to participate in modern cultural life on the internet.

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: stephane

Last Name: brun

Mailing Address: stefpc3@hotmail.fr

City: paris

Country: France

State or Province: paris

ZIP/Postal Code: 75000

Email Address:

Organization Name:

Comment: FREE WIFI

FREE 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: Guyader

Last Name: Ronan

Mailing Address: ksein.noir@gmail.com

City: Poitiers

Country: France

State or Province: Poitou-Charentes

ZIP/Postal Code: 86000

Email Address: ksein.noir@gmail.com

Organization Name:

Comment: Don't do that.

No.

Don't.

Don't do that.

No.

Don't.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Paolo

Last Name: Bologna

Mailing Address: Via Domenico di Somma, 5

City: Marano di Napoli

Country: Italy

State or Province: Napoli

ZIP/Postal Code: 80016

Email Address: pbologna@sitook.com

Organization Name: GE.S.I. srl

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: Paul

Last Name: McSpadden

Mailing Address: 226 8th ave north

City: Hopkins

Country: United States

State or Province: MN

ZIP/Postal Code: 55343

Email Address:

Organization Name:

Comment: As a consumer and someone in IT this is completely egregious. This proves I can't rely on corporations or the FCC to make the right decisions. If I'm to be given a walled garden box for wifi, I have to be able to trust the person giving me the box. When those same people make a living giving me back doors for me to spend the time fixing so that when a client tells me they've been compromised I don't have to say "well the FCC told me to leave you compromised". When a corporation has to consider doing dead drops for their clients just to get around the back doors left by the American government... why in the hell would I want to settle for such tyranny? If I can't alter the box that I'm given, what's to stop ANY government or lone hacker from compromising my security? This is the problem with the American government. You have no idea what security means. Security to you guys is helping terrorists, hackers, criminals, and corruption. There is no such thing as security through obscurity. If you rely solely on such tactics, it always fails. Look at Snowden for example. Obscurity failed because that was the only tactic used. So what does the NSA do? Puts more security holes in every god damn piece of hardware they can, to protect us from hackers and terrorists. I'm sick of this continued lie. The propaganda that just continues in this country. Basically if the US government wanted to play the good guy, they wouldn't have done every single tyrannical act you can possibly do that could get us in league with how awful china is. I mean they're jailing people who speak out against the US. So no, I'm not for this locking down of routers. It just leads to more ways the US government can fuck the world.

As a consumer and someone in IT this is completely egregious. This proves I can't rely on corporations or the FCC to make the right decisions. If I'm to be given a walled garden box for wifi, I have to be able to trust the person giving me the box. When those same people make a living giving me back doors for me to spend the time fixing so that when a client tells me they've been compromised I don't have to say "well the FCC told me to leave you compromised". When a corporation has to consider doing dead drops for their clients just to get around the back doors left by the American government... why in the hell would I want to settle for such tyranny? If I can't alter the box that I'm given, what's to stop ANY government or lone hacker from compromising my security? This is the problem with the American government. You have no idea what security means. Security to you guys is helping terrorists, hackers, criminals, and corruption. There is no such thing as security through obscurity. If you rely solely on such tactics, it always fails. Look at Snowden for example. Obscurity failed because that was the only tactic used. So what does the NSA do? Puts more security holes in every god damn piece of hardware they can, to protect us from hackers and terrorists. I'm sick of this continued lie. The propaganda that just continues in this country. Basically if the US government wanted to play the good guy, they wouldn't have done every single tyrannical act you can possibly do that could get us in league with how awful china is. I mean they're jailing people who speak out against the US. So no, I'm not for this locking down of routers. It just leads to more ways the US government can fuck the world.

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: Dorian

Last Name: Grosch

Mailing Address: doriangrosch@web.de

City: Berlin

Country: Germany

State or Province: Berlin

ZIP/Postal Code: 12157

Email Address:

Organization Name:

Comment: I wish to ask you to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

There are several reasons which oppose the passing of this proposal:

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

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

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

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

Thank you for understanding and choosing to act accordingly.

I wish to ask you to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

There are several reasons which oppose the passing of this proposal:

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

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

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

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

Thank you for understanding and choosing to act accordingly.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Logan

Last Name: Overton

Mailing Address: P.O. Box 801

City: Cottage Grove

Country: United States

State or Province: OR

ZIP/Postal Code: 97424

Email Address:

Organization Name:

Comment: Please do not restrict the ability to install custom software on internet accessibility devices. The very idea is tantamount to disallowing installation of third-party operating systems on home computing systems and can easily be justified in the same way, to "prevent harmful interference" via custom software. This is the main reason I see fit to be against this measure, in addition to the fact that it is a largely unnecessary restriction on consumer's rights for virtually no benefit.

Please do not restrict the ability to install custom software on internet accessibility devices. The very idea is tantamount to disallowing installation of third-party operating systems on home computing systems and can easily be justified in the same way, to "prevent harmful interference" via custom software. This is the main reason I see fit to be against this measure, in addition to the fact that it is a largely unnecessary restriction on consumer's rights for virtually no benefit.

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: Burchett

Mailing Address: 13681 Water Springs Ct

City: Centreville

Country: United States

State or Province: VA

ZIP/Postal Code: 20121

Email Address:

Organization Name:

Comment: Please reconsider this move to implement restrictive DRM on all wifi devices. By doing so, you would essentially allow companies to stop selling devices to people and forcing people to give up ownership of the things they buy. This is a bad move for a number of reasons.

It limits security. People will no longer be able to solve problems with security on their devices unless the manufacturer sees fit to do so. Research into new and improved tech for this field will be monopolized by those who are already in control, as much of the research and development requires openness of these existing devices.

By closing down wifi, the government is essentially standing behind corporations and giving them free reign to exploit users further. Please stand behind citizens, not corporations.

Please reconsider this move to implement restrictive DRM on all wifi devices. By doing so, you would essentially allow companies to stop selling devices to people and forcing people to give up ownership of the things they buy. This is a bad move for a number of reasons.

It limits security. People will no longer be able to solve problems with security on their devices unless the manufacturer sees fit to do so. Research into new and improved tech for this field will be monopolized by those who are already in control, as much of the research and development requires openness of these existing devices.

By closing down wifi, the government is essentially standing behind corporations and giving them free reign to exploit users further. Please stand behind citizens, not corporations.

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: Ed

Last Name: Naylor

Mailing Address: 2804 Mecca

City: Austin

Country: United States

State or Province: TX

ZIP/Postal Code: 78733

Email Address: gordongekko@austin.rr.com

Organization Name:

Comment: The FCC will have a Negative effect on User Freedom,Security,Emergency Preparedness and have a negative Economic Impact.

User Freedom

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.

Security

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.

Emergency Preparedness

Emergency preparedness would be hindered by restrictions on the modification of router hardware. Mesh networking is a key component of disaster response in our modern world. In disasters, amateur radio operators create mesh networks for disaster response. These operators use firmware like Broadband-Hamnet to create mesh networks on low-cost commodity routers operating at frequencies and power levels legally authorized for hams but not for other users. By modifying the device in such ways, wireless networks can be organized to cover much larger swaths of area to first-responders and emergency personnel. These restrictions would delay the exchange of emergency information and put lives at risk. The value of modified router hardware to assist in disaster response is recognized by emergency managers. In 2013, the International Association of Emergency Managers [6] designated Broadband-Hamnet as their US Technology and Innovation Award winner and Global Technology and Innovation Award winner.

Economic Impact

Millions of dollars of economic activity depend on third-party firmware. Major semiconductor and wireless hardware manufacturers use OpenWrt as the base of their router software.[1][2][3][4][5] At the same time, OpenWrt is managed and developed primarily by a community of individuals modifying their own routers and installing customized versions of OpenWrt on their own routers. Sometimes these routers originally had OpenWrt on them while others did not. Strong industry-community collaboration reduces the costs of maintenance and increases quality for manufacturers. This mutually-beneficial collaboration can only exist if users can replace their firmware on their router with a customized version of OpenWrt. By preventing firmware replacement, these regulations will strangle this community in the US thereby increasing costs to hardware manufacturers which could be passed along to customers and employees.

The FCC will have a Negative effect on User Freedom, Security, Emergency Preparedness and have a negative Economic Impact.

User Freedom

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.

Security

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.

Emergency Preparedness

Emergency preparedness would be hindered by restrictions on the modification of router hardware. Mesh networking is a key component of disaster response in our modern world. In disasters, amateur radio operators create mesh networks for disaster response. These operators use firmware like Broadband-Hamnet to create mesh networks on low-cost commodity routers operating at frequencies and power levels legally authorized for hams but not for other users. By modifying the device in such ways, wireless networks can be organized to cover much larger swaths of area to first-responders and emergency personnel. These restrictions would delay the exchange of emergency information and put lives at risk. The value of modified router hardware to assist in disaster response is recognized by emergency managers. In 2013, the International Association of Emergency Managers [6] designated Broadband-Hamnet as their US Technology and Innovation Award winner and Global Technology and Innovation Award winner.

Economic Impact

Millions of dollars of economic activity depend on third-party firmware. Major semiconductor and wireless hardware manufacturers use OpenWrt as the base of their router software.[1][2][3][4][5] At the same time, OpenWrt is managed and developed primarily by a community of individuals modifying their own routers and installing customized versions of OpenWrt on their own routers. Sometimes these routers originally had OpenWrt on them while others did not. Strong industry-community collaboration reduces the costs of maintenance and increases quality for manufacturers. This mutually-beneficial collaboration can only exist if users can replace their firmware on their router with a customized version of OpenWrt. By preventing firmware replacement, these regulations will strangle this community in the US thereby increasing costs to hardware manufacturers which could be passed along to customers and employees.

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: Samarin

Mailing Address: 19821 Hamilton Avenue

City: Torrance

Country: United States

State or Province: CA

ZIP/Postal Code: 90502

Email Address: samarin@motivoengineering.com

Organization Name: Motivo Engineering

Comment: In what seems to support the current trend of federal agencies forming regulations that attack symptoms rather than treating underlying causes, some parts of this Proposed Rule inherently stifle progress, creativity, and freedom.

Part 3.b.39 is one part of this proposal to cause this problem.

This part is specifically creating a situation where if a creative and motivated end user would like to update their device with software that provides security fixes (see mobile phone carrier delays in patching Android vulnerabilities), additional functionality, etc., they would need to navigate the time intensive and prohibitively costly route to FCC registration, testing, and approval.

Let's consider that every user wishing to update a personal device is willing and able to follow the steps outlined in the Proposal. Does the FCC have the resources to handle this highly increased demand in a timely fashion? My guess is not, at LEAST until the next federal budget cycle.

PLEASE reconsider some of these rules and their impact on the development of new devices, the security and longevity of existing devices, and the on the rapidly growing DIY electronics community.

In what seems to support the current trend of federal agencies forming regulations that attack symptoms rather than treating underlying causes, some parts of this Proposed Rule inherently stifle progress, creativity, and freedom.

Part 3.b.39 is one part of this proposal to cause this problem.

This part is specifically creating a situation where if a creative and motivated end user would like to update their device with software that provides security fixes (see mobile phone carrier delays in patching Android vulnerabilities), additional functionality, etc., they would need to navigate the time intensive and prohibitively costly route to FCC registration, testing, and approval.

Let's consider that every user wishing to update a personal device is willing and able to follow the steps outlined in the Proposal. Does the FCC have the resources to handle this highly increased demand in a timely fashion? My guess is not, at LEAST until the next federal budget cycle.

PLEASE reconsider some of these rules and their impact on the development of new devices, the security and longevity of existing devices, and the on the rapidly growing DIY electronics community.

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 Edwin

Last Name: Ocampo

Mailing Address: 510 5th Ave.

City: Santa Maria

Country: United States

State or Province: CA

ZIP/Postal Code: 93458

Email Address:

Organization Name:

Comment: I strong advise redrafting this proposal. The FCC should take in more data before such harsh action like this is taken.

I strong advise redrafting this proposal. The FCC should take in more data before such harsh action like this is taken.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jason

Last Name: Balicki

Mailing Address: 12148 Sunnycrest Pl

City: Maryland Heights

Country: United States

State or Province: MO

ZIP/Postal Code: 63043

Email Address: sakodak@gmail.com

Organization Name:

Comment: Manufacturers have a history of failing to patch vulnerable devices, especially legacy devices.

Forcing them to lock down firmware is a terrible idea. The end user will have no way to protect themselves against attackers exploiting known vulnerabilities that the manufacturers will not fix.

Please do not put this proposed rule in place. It will not make us safer, it will do the opposite.

Manufacturers have a history of failing to patch vulnerable devices, especially legacy devices.

Forcing them to lock down firmware is a terrible idea. The end user will have no way to protect themselves against attackers exploiting known vulnerabilities that the manufacturers will not fix.

Please do not put this proposed rule in place. It will not make us safer, it will do the opposite.

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: Eugene

Last Name: Evans

Mailing Address: 151 Taylor Court, Apt 311

City: Princeton

Country: United States

State or Province: NJ

ZIP/Postal Code: 08540

Email Address: null

Organization Name: null

Comment: Whether intentional or not, the proposed rules would criminalize the act of installing third-party operating systems (notably the open source Linux-based DD-WRT firmware) on wireless routers. This would irrevocably damage the ability of end users to use their purchased hardware to its fullest extent and leave consumers at the mercy of device manufacturers. Do not approve this rule change as is.

Whether intentional or not, the proposed rules would criminalize the act of installing third-party operating systems (notably the open source Linux-based DD-WRT firmware) on wireless routers. This would irrevocably damage the ability of end users to use their purchased hardware to its fullest extent and leave consumers at the mercy of device manufacturers. Do not approve this rule change as is.

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: Nirmalendu

Last Name: khan

Mailing Address: dhanmondi

City: Dhaka

Country: Bangladesh

State or Province: Barisal

ZIP/Postal Code: 8145

Email Address: khan.nupur@gmail.com

Organization Name: Diu

Comment: I reject this because security and privacy is important to me.I want my freedom.

I reject this because security and privacy is important to me.I want my freedom.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Steven

Last Name: Harper

Mailing Address: 208 E 1st STreet

City: Cle Elum

Country: United States

State or Province: WA

ZIP/Postal Code: 98922

Email Address: timesaverpc@gmail.com

Organization Name: TimesaverPC

Comment: This Proposal is luduicrous - Stop it now

This Proposal is luduicrous - Stop it now

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: Grant

Last Name: Saunders

Mailing Address: 6823 Westmoreland Rd.

City: Falls Church

Country: United States

State or Province: VA

ZIP/Postal Code: 22042

Email Address: grant.saunders@gmail.com

Organization Name: null

Comment: I use DD-WRT to stay connected with my parents network and these proposed rule changes would cut them off from me by making this illegal.

The FCC should not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Additional points of emphasis you include:

1. Wireless networking research depends on the ability of researchers to investigate and modify their devices.
2. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
3. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
4. 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 use DD-WRT to stay connected with my parents network and these proposed rule changes would cut them off from me by making this illegal.

The FCC should not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Additional points of emphasis you include:

1. Wireless networking research depends on the ability of researchers to investigate and modify their devices.
2. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
3. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
4. 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: D

Last Name: R

Mailing Address: Private

City: Falls Church

Country: United States

State or Province: VA

ZIP/Postal Code: 22043

Email Address:

Organization Name:

Comment: I very much like the idea of making wireless devices certifiably more secure, but this should never come at the expense of the ability for consumers to choose to install custom firmware. It is very reasonable for a company to attempt to prevent modification of their devices, as well as for these modifications to void any warranties. However, I will always want the choice to be able modify my own devices whenever I choose to accept the risk of breaking them. I want security researchers to be able to modify devices so that they are able to investigate and create security fixes when the vendor does not provide them on their own, and I want the ability to apply these fixes to my devices if I choose to.

I very much like the idea of making wireless devices certifiably more secure, but this should never come at the expense of the ability for consumers to choose to install custom firmware. It is very reasonable for a company to attempt to prevent modification of their devices, as well as for these modifications to void any warranties. However, I will always want the choice to be able modify my own devices whenever I choose to accept the risk of breaking them. I want security researchers to be able to modify devices so that they are able to investigate and create security fixes when the vendor does not provide them on their own, and I want the ability to apply these fixes to my devices if I choose to.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Andrew

Last Name: Greenwood

Mailing Address: 302 pine wood drive

City: Greenville

Country: United States

State or Province: SC

ZIP/Postal Code: 29607

Email Address: greenwood.andy@gmail.com

Organization Name:

Comment: These rules would unfairly restrict users from doing what they wish with the product they have purchased.

While that may or may not have been the author's intent, this document needs clarification either here, or in court.

These rules would unfairly restrict users from doing what they wish with the product they have purchased. While that may or may not have been the author's intent, this document needs clarification either here, or in court.

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: bipul

Last Name: roy

Mailing Address: bplbipuldomar@gmail.com

City: Dhaka

Country: Bangladesh

State or Province: dhaka

ZIP/Postal Code: 1215

Email Address: bipulroybpl@gmail.com

Organization Name:

Comment: I object this because security and privacy is important to me.

I object this because security and privacy is important to me.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Peter

Last Name: Lovett

Mailing Address: 6212 SE 28th Ave

City: Portland

Country: United States

State or Province: OR

ZIP/Postal Code: 97202

Email Address: pelovett@gmail.com

Organization Name:

Comment: This is bill holds an inherent threat to the ability of Americans to thrive in the digital age and should be reconsidered and edited to produce a bill that makes all parties happy.

This is bill holds an inherent threat to the ability of Americans to thrive in the digital age and should be reconsidered and edited to produce a bill that makes all parties happy.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Matthew

Last Name: Herren

Mailing Address: 1002 Burlington Beach Rd.

City: Valparaiso

Country: United States

State or Province: IN

ZIP/Postal Code: 46383

Email Address: mattherren@gmail.com

Organization Name: null

Comment: What you are proposing will literally set us back decades. We have always been a nation of tinkerers - where entrepreneurship and innovation are encouraged. Putting such needless regulations in place will only damage that... not to mention solve nothing in respect to security.

What you are proposing will literally set us back decades. We have always been a nation of tinkerers - where entrepreneurship and innovation are encouraged. Putting such needless regulations in place will only damage that... not to mention solve nothing in respect to security.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Kaf

Last Name: Taba

Mailing Address: 1 City Hall Sq, Rm 703

City: Boston

Country: United States

State or Province: MA

ZIP/Postal Code: 02201-2021

Email Address: dfsfsdf@hotmail.com

Organization Name:

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

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

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

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

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

I am respectfully asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

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

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

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

Billions of dollars of commerce, such as secure wifi vendors, 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: Matthew

Last Name: Dugan

Mailing Address: 680 Butchart Dr

City: Prosper

Country: United States

State or Province: TX

ZIP/Postal Code: 75078

Email Address:

Organization Name:

Comment: To whom it concerns,

Please ensure that any rule does not restrict consumer freedom to upgrade, flash, or otherwise overwrite the default operating system on consumer grade wireless devices. The closed, proprietary default operating systems on consumer wireless devices often have security holes and go without security updates for much of the life of the device, which are corrected by applying a new and open operating system to the device. Even if security issues or a lack of updates are not present, a rule providing for labeling and equipment authorization would restrict consumer freedoms to learn and experiment with the hardware they have purchased - in many cases for such a purpose.

Open Source projects like DD-WRT, Tomato, OpenWRT, etc allow consumers to flash many such devices with more capable operating environments allowing for advanced security controls and more secure operation. As well, it allows for individuals with STEM education or STEM interests more flexibility to learn and experiment outside of being bound by enterprise equipment and enterprise licenses (and enterprise costs). A rule that forbids or otherwise restricts or impairs the ability of such projects or of consumers to choose to apply such project code to the devices they have purchased would hamper consumer freedom, hamper self education and experimentation, and contribute to an insecure, out of date network element in the expanding broadband consumer space of consumer home networks.

Thanks and regards.

To whom it concerns,

Please ensure that any rule does not restrict consumer freedom to upgrade, flash, or otherwise overwrite the default operating system on consumer grade wireless devices. The closed, proprietary default operating systems on consumer wireless devices often have security holes and go without security updates for much of the life of the device, which are corrected by applying a new and open operating system to the device. Even if security issues or a lack of updates are not present, a rule providing for labeling and equipment authorization would restrict consumer freedoms to learn and experiment with the hardware they have purchased - in many cases for such a purpose.

Open Source projects like DD-WRT, Tomato, OpenWRT, etc allow consumers to flash many such devices with more capable operating environments allowing for advanced security controls and more secure operation. As well, it allows for individuals with STEM education or STEM interests more flexibility to learn and experiment outside of being bound by enterprise equipment and enterprise licenses (and enterprise costs). A rule that forbids or otherwise restricts or impairs the ability of such projects or of consumers to choose to apply such project code to the devices they have purchased would hamper consumer freedom, hamper self education and experimentation, and contribute to an insecure,

out of date network element in the expanding broadband consumer space of consumer home networks.

Thanks and regards.

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: Leonard

Last Name: Knig

Mailing Address: leonard.r.koenig@googlemail.com

City: Berlin

Country: Germany

State or Province: Berlin

ZIP/Postal Code: 14193

Email Address:

Organization Name:

Comment: No

So the lobby succeeded - again? Just because those people don't want to spend a bit money and intelligence on developing secure protocols or hard-'coding' the frequencies? SERIOUSLY?

You know what? If the US and the EU are *really* going to have this, what country would have a more free internet? Russia, China, Arab Emirates. Are you *kidding*?

Those 'unfree' countries which ban so much freedom are gonna be allowed to use any firmware they want, transmit on any frequencies they want. They are laughing at us 'free citizens'.

No

So the lobby succeeded - again? Just because those people don't want to spend a bit money and intelligence on developing secure protocols or hard-'coding' the frequencies? SERIOUSLY?

You know what? If the US and the EU are *really* going to have this, what country would have a more free internet? Russia, China, Arab Emirates. Are you *kidding*?

Those 'unfree' countries which ban so much freedom are gonna be allowed to use any firmware they want, transmit on any frequencies they want. They are laughing at us 'free citizens'.

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: Brandon

Last Name: Zehm

Mailing Address: 3258 N Yellow Peak Pl

City: Meridian

Country: United States

State or Province: ID

ZIP/Postal Code: 83646

Email Address: brandon@zehm.org

Organization Name:

Comment: In summary I'm very concerned about any provision which hampers innovation or the ability for the open source community to create firmware for RF devices.

As per the "Free Wifi" campaign, my recommendations in are:

1) The regulations on software defined radios should not restrict the ability to replace software on computing devices. As written, the regulations require that manufacturers prevent modification of all software computing devices which use software defined radios. The Commission should amend the regulations in a manner which protects the traditional right of law abiding users to understand and improve the software on their devices.

2) The regulations on e-labels should not restrict the ability to replace software on computing devices. The signers appreciate the need for proper labeling of wireless devices and the requirements set by Congress in the E-Label Act. The Commission should amend the regulations to guarantee electronic labels do not interfere with the ability of downstream parties to install any software they so choose.

In summary I'm very concerned about any provision which hampers innovation or the ability for the open source community to create firmware for RF devices.

As per the "Free Wifi" campaign, my recommendations in are:

1) The regulations on software defined radios should not restrict the ability to replace software on computing devices. As written, the regulations require that manufacturers prevent modification of all software computing devices which use software defined radios. The Commission should amend the regulations in a manner which protects the traditional right of law abiding users to understand and improve the software on their devices.

2) The regulations on e-labels should not restrict the ability to replace software on computing devices. The signers appreciate the need for proper labeling of wireless devices and the requirements set by Congress in the E-Label Act. The Commission should amend the regulations to guarantee electronic labels do not interfere with the ability of downstream parties to install any software they so choose.

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: Harold

Last Name: Felton

Mailing Address: 1099 N. Hudson Ave.

City: Pasadena

Country: United States

State or Province: CA

ZIP/Postal Code: 91104

Email Address:

Organization Name:

Comment: Please modify this Proposed Rule:

1 - Customers should retain the right to use (and abuse) any product which they purchase as long as that right does not infringe on others.

2 - The wireless devices in question are not able to create any significant disruption to services which the FCC regulates.

3 - These regulations infringe on a customers reasonable use of their purchased wireless devices - with no measureable gains for anyone.

Please modify this Proposed Rule:

1 - Customers should retain the right to use (and abuse) any product which they purchase as long as that right does not infringe on others.

2 - The wireless devices in question are not able to create any significant disruption to services which the FCC regulates.

3 - These regulations infringe on a customers reasonable use of their purchased wireless devices - with no measureable gains for anyone.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Federico

Last Name: Tiberi

Mailing Address: Via Dell'Aquila, 6/P

City: Terni

Country: Italy

State or Province: Terni

ZIP/Postal Code: 05100

Email Address: fedetiberi@gmail.com

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.

* Regarding the above statements I'd like to point out my personal experience. I've got a VPN Router whom manufacturer stopped any support/bug fix: the only way to improve my VPN security was to buy a new model. However I replaced the original firmware to an open-source one and I've gave new life to my router, including the latest and modern security features.

* 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.

* Regarding the above statements I'd like to point out my personal experience. I've got a VPN Router whom manufacturer stopped any support/bug fix: the only way to improve my VPN security was to buy a new model. However I replaced the original firmware to an open-source one and I've gave new life to my router, including the latest and modern security features.

* 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: Paride

Last Name: Dominici

Mailing Address: Via Bonconte da Montefeltro, 30

City: Urbino

Country: Italy

State or Province: PU

ZIP/Postal Code: 61029

Email Address: paride.dominici@gmail.com

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: clifford

Last Name: jennings

Mailing Address: hillbilly72@comcast.net

City: riverdale

Country: United States

State or Province: UT

ZIP/Postal Code: 84405

Email Address:

Organization Name:

Comment: i believe it would be detrimental to the security and future of router firmware if this becomes law.companies do not design routers with security in mind the people have stepped up and designed their own software for a safer environment for all. please do not vote for this issue.

i believe it would be detrimental to the security and future of router firmware if this becomes law.companies do not design routers with security in mind the people have stepped up and designed their own software for a safer environment for all. please do not vote for this issue.

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: Harold

Last Name: Dost

Mailing Address: 326 Marlin Ave

City: Royal Oak

Country: United States

State or Province: MI

ZIP/Postal Code: 48067

Email Address: harolddost@gmail.com

Organization Name:

Comment: Closing the ability to change software on devices such as wireless routers is overly intrusive into consumers lives. Additionally closing this ability to allow custom firmware only encourages companies to do less in terms of providing better software features within their routers. This could include piecemeal features where every "advance" function requires some sort additional payment. It's already done I'm so many other areas. This rule will just allow companies to be crappy as ever. There should be a better way than flat out banning custom software.

Closing the ability to change software on devices such as wireless routers is overly intrusive into consumers lives. Additionally closing this ability to allow custom firmware only encourages companies to do less in terms of providing better software features within their routers. This could include piecemeal features where every "advance" function requires some sort additional payment. It's already done I'm so many other areas. This rule will just allow companies to be crappy as ever. There should be a better way than flat out banning custom software.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Fabio

Last Name: Ferrari

Mailing Address: via don carlo giorgi, 10

City: Silvano Pietra

Country: Italy

State or Province: PV

ZIP/Postal Code: 27050

Email Address: mc.gyver77@gmail.com

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: Benjamin

Last Name: Cronce

Mailing Address: 2015 sherri ln apt #B

City: Wisconsin Rapids

Country: United States

State or Province: WI

ZIP/Postal Code: 54494

Email Address: bcronce@gmail.com

Organization Name:

Comment: I understand the need to have some basic restrictions like max power output and other things, but if any restrictions are made, the wording needs to be 3rd-party firmware friendly. We need to be able to mod home routers to have better safer firmware than stock, which is nutritiously horrible and manufacturers rarely care about security nor keep up with the constant inflow of security patches.

I understand the need to have some basic restrictions like max power output and other things, but if any restrictions are made, the wording needs to be 3rd-party firmware friendly. We need to be able to mod home routers to have better safer firmware than stock, which is nutritiously horrible and manufacturers rarely care about security nor keep up with the constant inflow of security patches.

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: Kokandy

Mailing Address: 1105 Eagle Way

City: Ashland

Country: United States

State or Province: OH

ZIP/Postal Code: 44805

Email Address: drkokandy@gmail.com

Organization Name:

Comment: I strongly and sincerely urge the FCC not to restrict end-user consumer ability to replace firmware on WiFi routers.

Restrictions on replacing router software will have a serious impact on internet 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. Read more here: <http://www.cnet.com/news/top-wi-fi-routers-easy-to-hack-says-study/>

Not only are these unpatched security holes dangerous for end-user consumers, unpatched routers which get hacked also are a significant contributing factor to the spread of malware and botnets online.

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.

I strongly and sincerely urge the FCC not to restrict end-user consumer ability to replace firmware on WiFi routers.

Restrictions on replacing router software will have a serious impact on internet 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. Read more here: <http://www.cnet.com/news/top-wi-fi-routers-easy-to-hack-says-study/>

Not only are these unpatched security holes dangerous for end-user consumers, unpatched routers which get hacked also are a significant contributing factor to the spread of malware and botnets online.

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.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Thomas

Last Name: Beals

Mailing Address: 171 Willow St.

City: Acton

Country: United States

State or Province: MA

ZIP/Postal Code: 01720

Email Address: tbeals1@gmail.com

Organization Name: private

Comment: The FCC's document is being represented to the computing public as potentially preventing practices that are both common, and that are viewed as vital aspects of maintaining secure and private communications: the loading of open-source software onto hardware and firmware that is on the open market.

The proposed rule (Document Citation: 80 FR 46900 - Equipment Authorization and Electronic Labeling for Wireless Devices) lacks a plain language summary, and this alone should be enough to prevent its acceptance. I ask that you prepare a summary statement with pointers to relevant sections in the complete document. That summary statement should clearly state the purpose of the proposed rule. The summary statement should make clear what currently lawful practices, if any, will be made unlawful by the proposed rule. The summary statement should also state what restrictions on currently marketed devices, if any, will be removed from the open market by the proposed rule.

This request, with appropriate introductory material, will be copied to my Senators and Congressional representatives.

The FCC's document is being represented to the computing public as potentially preventing practices that are both common, and that are viewed as vital aspects of maintaining secure and private communications: the loading of open-source software onto hardware and firmware that is on the open market.

The proposed rule (Document Citation: 80 FR 46900 - Equipment Authorization and Electronic Labeling for Wireless Devices) lacks a plain language summary, and this alone should be enough to prevent its acceptance. I ask that you prepare a summary statement with pointers to relevant sections in the complete document. That summary statement should clearly state the purpose of the proposed rule. The summary statement should make clear what currently lawful practices, if any, will be made unlawful by the proposed rule. The summary statement should also state what restrictions on currently marketed devices, if any, will be removed from the open market by the proposed rule.

This request, with appropriate introductory material, will be copied to my Senators and Congressional representatives.