

security reasons. These are drivers that anyone can run, study, modify, and redistribute verbatim or modified. Free drivers are inherently more secure than the non-Free/proprietary, locked down drivers that vendors distribute. Since anyone can study how a Free driver works and make changes to it, people ranging from hobbyists to security professionals are all able to fix security bugs before they're discovered by malicious crackers. Many vendors ignore bugs, which leads to a higher risk of being compromised, and users are unable to legally fix them themselves, despite the fact that it would be a very difficult task. Forcing vendors to lock down their RF devices hurts the security of computer users.

Secondly, both students and researchers will be set back. Researchers need to be able to control how their RF devices work in order to do what they do. Likewise, students will have yet another obstacle in their studies about RF devices. We want to foster interest, and thus development of RF devices, not obstruct it. By locking down these devices people will no longer be able to learn about how they work. Forcing vendors to lock down their RF devices hurts the development of RF technologies.

Thirdly, it's unethical. Computers are tools, and tools should help their users, not fight them. What would the carpentry situation be if hammers prevented their users from nailing in nails that a company doesn't like? The user should have the final say over how their computer works, not a company. People will still find ways to do illegal things, so it's better to protect the good than to destroy it all along with a small bit of bad. For the loss compared to gain, it's definitely not worth it. Forcing vendors to lock down their RF devices isn't worth the loss.

Those were three reasons why this would be wrong. Of course, there are plenty of other problems with locking down RF devices as well. Please do not destroy the control that we have over our RF devices.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jeff

Last Name: Whitney

Mailing Address: 4850s 4900w

City: Slc

Country: United States

State or Province: UT

ZIP/Postal Code: 84118

Email Address:

Organization Name:

Comment: People need to be able to modify any aspect of any hardware or software they rightfully purchased. Enough restrictions.

People need to be able to modify any aspect of any hardware or software they rightfully purchased. Enough restrictions.

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: Aled

Last Name: Cuda

Mailing Address: 7653 hillrose st

City: Tujunga

Country: United States

State or Province: CA

ZIP/Postal Code: 91042

Email Address: aledvirgil@gmail.com

Organization Name:

Comment: In modern times nearly every device we have is connected with every other through the internet, and most of that happens over wifi, and mobile networks. Along with this trend there has also been one to move towards more integrated systems, often storing firmware and software inseparably in one package for one specific embedded device. This presents an issue because the people who design the devices, and write software for them are generally incompetent or just don't care. This has led to many security issues especially in routers, that are simple to exploit and often never get fixed. If a router is breached then anyone anywhere with the right knowledge can listen to your webtraffic, capture it and change it potentially releasing a hoard of private data like credit card numbers, passwords, and emails. This however is not the worst of it, because beyond that it leaves the computer that is normally protected by NAT wide open to attack. The small, but incredibly talented community that has built up around these devices routinely finds these issues and fixes them, and many among them develop their own more capable, and more secure pieces of firmware that are used by private individuals and small businesses alike to secure and improve their networks. Unfortunately none of this would be possible without the right to modify the firmware of these devices. This however does not completely cover the issue, because embedded devices are not the only places where custom wireless firmware is common, because many operating systems load their own firmware at boot time so that they can communicate so the issue with wireless firmware is not limited to embedded devices it extends to laptops and desktops alike. The most common example of this aftermarket firmware is the operating system Linux, this operating system drives everything from the ISS (by the way all the laptops on the ISS use Linux and have wifi which means they use custom firmware and this frames the issue of security in standard, because when they used Windows they got a worm) to the LHC to our tanks and ships over seas. This is an operating system that was created by a hobiist who instead of being content with what he had, decided to turn it into something more and in an atmosphere like the one this bill proposes, that kind of innovation would be illegal because to create a successful operating system he would have to create his own third party wireless firmware. A large portion of the technological innovation that happens in this country happens because of hobiists who experiment and by passing this regulation you make that innovation illegal. Finally this could easily infringe on the Title 47, Section 19 rights of ham radio operators because most of these devices operate secondarily on the ISM bands on which Hams are usually primary, and under section 19 Ham radio operators are allowed to modify radios for their use as long as they comply with the restrictions on bandwidth, frequency, and transmit power (among others) that the FCC puts in place. This legislation effectively violates that right by removing their ability to modify radios which they routinely do.

In modern times nearly every device we have is connected with every other through the internet, and most of that happens over wifi, and mobile networks. Along with this trend there has also been one to move towards more integrated systems, often storing firmware and software inseparably in one package for one specific embedded device. This presents an issue because the people who design the devices, and write software for them are generally incompetent or just don't care. This has led to many security issues especially in routers, that are simple to exploit and often never get fixed. If a router is breached then anyone anywhere with the right knowledge can listen to your webtraffic, capture it and change it

potentially releasing a hord of private data like credit card numbers, passwords, and emails. This however is not the worst of it, because beyond that it leaves the computer that is normally protected by NAT wide open to attack. The small, but incredibly talented community that has built up around these devices routinely finds these issues and fixes them, and many among them develop there own more capable, and more secure pieces of firmware that are used by private individuals and small businesses alike to secure and improve their networks. Unfortunately none of this would be possible without the right to modify the firmware of these devices. This however does not completely cover the issue, because embeded devices are not the only places where custom wireless firmware is common, because many operating systems load there own firmware at boot time so that they can communicate so the issue with wireless firmware is not limited to embeded devices it extends to laptops and desktops alike. The most common example of this aftermarket firmware is the operating system Linux, this operating system drives everything from the ISS (by the way all the laptops on the ISS use Linux and have wifi which means they use custom firmware and this frames the issue of security in standard, because when they used Windows they got a worm) to the LHC to our tanks and ships over seas. This is an operating system that was created by a hobiest who instead of being content with what he had, decided to turn it into something more and in an atmosphere like the one this bill proposes, that kind of innovation would be illegal because to create a successful operating system he would have to create his own third party wireless firmware. A large portion of the technological inovation that happens in this country happens because of hobiests who experiment and by passing this regulation you make that innovation illegal. Finally this could easilly infringe on the Title 47, Section 19 rights of ham radio opperaters because most of these devices opperate secundarily on thi ISM vands on which Hams are usually primary, and under section 19 Ham radio operators are allowed to modify radios for their use as long as they comply with the restrictions on bandwidth, frequency,and transmit power (among others) that the Fcc puts in place. This legislation effectively violates that right by removing their ability to modify radios which they routinely do.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Mark

Last Name: Allshouse

Mailing Address: 201 Fiddlers Elbow Rd.

City: Middletown

Country: United States

State or Province: PA

ZIP/Postal Code: 17057-2912

Email Address: m.allshouse@gmail.com

Organization Name:

Comment: Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Wireless networking research depends on the ability of researchers to investigate and modify their devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the 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.

There is simply no god reason for implementing these unnecessarily restrictive regulations. Please reconsider. Thank you.

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

There is simply no god reason for implementing these unnecessarily restrictive regulations. Please reconsider. Thank you.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jose

Last Name: Mendoza

Mailing Address: 375 south royal poinciana blvd apt 10c

City: Miami Springs

Country: United States

State or Province: FL

ZIP/Postal Code: 33166

Email Address: joedoe47@gmail.com

Organization Name: null

Comment: the FCC should allow WIFI standards to remain as open as possible. You are requiring manufactures to "lock down" devices however there is a much impact that will have as follows.

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

I am not very familiar with R&D; however, we all know the scientific process. People who are doing R&D need to be able to debug and change parameters that would allow them to do their jobs. Having binaries that they can not edit, audit, or replace with their own, would prevent them from doing their job and perhaps bettering wifi.

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

We all know manufactures like to keep things at cost, as such things like security updates are sometimes held back, due to distributing patches and cost required to actually find and fix these critical bugs. As such we as individuals and as employees that support critical company infrastructure may need to be able to put in our own firmware and patches to ensure the security of our networks. Having manufactures take care of security will only make it difficult for individuals and enterprises to pick up the slack, so to speak.

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

As you may or not be aware, individuals in the FOSS community have solved very big problems when they have actually been allowed access to audit and contribute to code for wifi drivers, graphic drivers, etc. By leaving up to the manufacture, you are doing to make it possibly difficult for passionate users that want to contribute to your technology and thus, you will lose these resources.

\*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.

personally, I like to use hardware where I can load DDWRT on the router. I can also think of two companies that are using their own software to provide service to their users. We would likely have to either find alternatives or see how much we would have to pay, just to have the feature to adapt our own binaries/firmware. Personally I would be willing to pay a little extra to have the ability to have my own binaries; although I am not sure of these two companies, I don't represent them in anyway.

the FCC should allow WIFI standards to remain as open as possible. You are requiring manufactures to "lock down" devices however there is a much impact that will have as follows.

\*Wireless networking research depends on the ability of researchers to investigate and modify their devices. I am not very familiar with R&D; however, we all know the scientific process. People who are doing R&D need to be able to debug and change parameters that would allow them to do their jobs. Having binaries that they can not edit, audit, or replace with their own, would prevent them from doing their job and perhaps bettering wifi.

\*Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. We all know manufactures like to keep things at cost, as such things like security updates are sometimes held back, due to distributing patches and cost required to actually find and fix these critical bugs. As such we as individuals and as employees that support critical company infrastructure may need to be able to put in our own firmware and patches to ensure the security of our networks. Having manufactures take care of security will only make it difficult for individuals and enterprises to pick up the slack, so to speak.

\*Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. As you may or not be aware, individuals in the FOSS community have solved very big problems when they have actually been allowed access to audit and contribute to code for wifi drivers, graphic drivers, etc. By leaving up to the manufacture, you are doing to make it possibly difficult for passionate users that want to contribute to your technology and thus, you will lose these resources.

\*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. personally, I like to use hardware where I can load DDWRT on the router. I can also think of two companies that are using their own software to provide service to their users. We would likely have to either find alternatives or see how much we would have to pay, just to have the feature to adapt our own binaries/firmware. Personally I would be willing to pay a little extra to have the ability to have my own binaries; although I am not sure of these two companies, I don't represent them in anyway.

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: Collette

Mailing Address: 36 Windswept Way

City: Coventry

Country: United States

State or Province: CT

ZIP/Postal Code: 06488

Email Address: rcollette@yahoo.com

Organization Name:

Comment: I respectfully request that the FCC does not pass this rule. For years amateur radio operators have been providing useful, free, disaster services using modified wifi routers, such as in Haiti. This rule bans this use case, stifles innovation and prevents amateur radio operators from operating legally on channels they are authorized to use.

I respectfully request that the FCC does not pass this rule. For years amateur radio operators have been providing useful, free, disaster services using modified wifi routers, such as in Haiti. This rule bans this use case, stifles innovation and prevents amateur radio operators from operating legally on channels they are authorized to use.

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: Jose

Last Name: Mendoza

Mailing Address: 375 south royal poinciana blvd

City: miami springs

Country: United States

State or Province: FL

ZIP/Postal Code: 33166

Email Address: joedoe47@gmail.com

Organization Name: null

Comment: the FCC should allow WIFI standards to remain as open as possible. You are requiring manufactures to "lock down" devices however there is a much impact that will have as follows.

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

I am not very familiar with R&D; however, we all know the scientific process. People who are doing R&D need to be able to debug and change parameters that would allow them to do their jobs. Having binaries that they can not edit, audit, or replace with their own, would prevent them from doing their job and perhaps bettering wifi.

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

We all know manufactures like to keep things at cost, as such things like security updates are sometimes held back, due to distributing patches and cost required to actually find and fix these critical bugs. As such we as individuals and as employees that support critical company infrastructure may need to be able to put in our own firmware and patches to ensure the security of our networks. Having manufactures take care of security will only make it difficult for individuals and enterprises to pick up the slack, so to speak.

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

As you may or not be aware, individuals in the FOSS community have solved very big problems when they have actually been allowed access to audit and contribute to code for wifi drivers, graphic drivers, etc. By leaving up to the manufacture, you are doing to make it possibly difficult for passionate users that want to contribute to your technology and thus, you will lose these resources.

\*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.

personally, I like to use hardware where I can load DDWRT on the router. I can also think of two companies that are using their own software to provide service to their users. We would likely have to either find alternatives or see how much we would have to pay, just to have the feature to adapt our own binaries/firmware. Personally I would be willing to pay a little extra to have the ability to have my own binaries; although I am not sure of these two companies, I don't represent them in anyway.

the FCC should allow WIFI standards to remain as open as possible. You are requiring manufactures to "lock down" devices however there is a much impact that will have as follows.

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

I am not very familiar with R&D; however, we all know the scientific process. People who are doing R&D need to be able to debug and change parameters that would allow them to do their jobs. Having binaries that they can not edit, audit, or replace with their own, would prevent them from doing their job and perhaps bettering wifi.

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

We all know manufactures like to keep things at cost, as such things like security updates are sometimes held back, due to distributing patches and cost required to actually find and fix these critical bugs. As such we as individuals and as employees that support critical company infrastructure may need to be able to put in our own firmware and patches to ensure the security of our networks. Having manufactures take care of security will only make it difficult for individuals and enterprises to pick up the slack, so to speak.

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

As you may or not be aware, individuals in the FOSS community have solved very big problems when they have actually been allowed access to audit and contribute to code for wifi drivers, graphic drivers, etc. By leaving up to the manufacture, you are doing to make it possibly difficult for passionate users that want to contribute to your technology and thus, you will lose these resources.

\*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.

personally, I like to use hardware where I can load DDWRT on the router. I can also think of two companies that are using their own software to provide service to their users. We would likely have to either find alternatives or see how much we would have to pay, just to have the feature to adapt our own binaries/firmware. Personally I would be willing to pay a little extra to have the ability to have my own binaries; although I am not sure of these two companies, I don't represent them in anyway.

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: Jose

Last Name: Mendoza

Mailing Address: 375 south royal poinciana blvd

City: miami springs

Country: United States

State or Province: FL

ZIP/Postal Code: 33166

Email Address: joedoe47@gmail.com

Organization Name: null

Comment: the FCC should allow WIFI standards to remain as open as possible. You are requiring manufactures to "lock down" devices however there is a much impact that will have as follows.

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

I am not very familiar with R&D; however, we all know the scientific process. People who are doing R&D need to be able to debug and change parameters that would allow them to do their jobs. Having binaries that they can not edit, audit, or replace with their own, would prevent them from doing their job and perhaps bettering wifi.

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

We all know manufactures like to keep things at cost, as such things like security updates are sometimes held back, due to distributing patches and cost required to actually find and fix these critical bugs. As such we as individuals and as employees that support critical company infrastructure may need to be able to put in our own firmware and patches to ensure the security of our networks. Having manufactures take care of security will only make it difficult for individuals and enterprises to pick up the slack, so to speak.

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

As you may or not be aware, individuals in the FOSS community have solved very big problems when they have actually been allowed access to audit and contribute to code for wifi drivers, graphic drivers, etc. By leaving up to the manufacture, you are doing to make it possibly difficult for passionate users that want to contribute to your technology and thus, you will lose these resources.

\*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.

personally, I like to use hardware where I can load DDWRT on the router. I can also think of two companies that are using their own software to provide service to their users. We would likely have to either find alternatives or see how much we would have to pay, just to have the feature to adapt our own binaries/firmware. Personally I would be willing to pay a little extra to have the ability to have my own binaries; although I am not sure of these two companies, I don't represent them in anyway.

the FCC should allow WIFI standards to remain as open as possible. You are requiring manufactures to "lock down" devices however there is a much impact that will have as follows.

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

I am not very familiar with R&D; however, we all know the scientific process. People who are doing R&D need to be able to debug and change parameters that would allow them to do their jobs. Having binaries that they can not edit, audit, or replace with their own, would prevent them from doing their job and perhaps bettering wifi.

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

We all know manufactures like to keep things at cost, as such things like security updates are sometimes held back, due to distributing patches and cost required to actually find and fix these critical bugs. As such we as individuals and as employees that support critical company infrastructure may need to be able to put in our own firmware and patches to ensure the security of our networks. Having manufactures take care of security will only make it difficult for individuals and enterprises to pick up the slack, so to speak.

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

As you may or not be aware, individuals in the FOSS community have solved very big problems when they have actually been allowed access to audit and contribute to code for wifi drivers, graphic drivers, etc. By leaving up to the manufacture, you are doing to make it possibly difficult for passionate users that want to contribute to your technology and thus, you will lose these resources.

\*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.

personally, I like to use hardware where I can load DDWRT on the router. I can also think of two companies that are using their own software to provide service to their users. We would likely have to either find alternatives or see how much we would have to pay, just to have the feature to adapt our own binaries/firmware. Personally I would be willing to pay a little extra to have the ability to have my own binaries; although I am not sure of these two companies, I don't represent them in anyway.

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: Jose

Last Name: Mendoza

Mailing Address: 375 south royal poinciana blvd

City: miami springs

Country: United States

State or Province: FL

ZIP/Postal Code: 33166

Email Address: joedoe47@gmail.com

Organization Name: null

Comment: the FCC should allow WIFI standards to remain as open as possible. You are requiring manufactures to "lock down" devices however there is a much impact that will have as follows.

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

I am not very familiar with R&D; however, we all know the scientific process. People who are doing R&D need to be able to debug and change parameters that would allow them to do their jobs. Having binaries that they can not edit, audit, or replace with their own, would prevent them from doing their job and perhaps bettering wifi.

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

We all know manufactures like to keep things at cost, as such things like security updates are sometimes held back, due to distributing patches and cost required to actually find and fix these critical bugs. As such we as individuals and as employees that support critical company infrastructure may need to be able to put in our own firmware and patches to ensure the security of our networks. Having manufactures take care of security will only make it difficult for individuals and enterprises to pick up the slack, so to speak.

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

As you may or not be aware, individuals in the FOSS community have solved very big problems when they have actually been allowed access to audit and contribute to code for wifi drivers, graphic drivers, etc. By leaving up to the manufacture, you are doing to make it possibly difficult for passionate users that want to contribute to your technology and thus, you will lose these resources.

\*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.

personally, I like to use hardware where I can load DDWRT on the router. I can also think of two companies that are using their own software to provide service to their users. We would likely have to either find alternatives or see how much we would have to pay, just to have the feature to adapt our own binaries/firmware. Personally I would be willing to pay a little extra to have the ability to have my own binaries; although I am not sure of these two companies, I don't represent them in anyway.

the FCC should allow WIFI standards to remain as open as possible. You are requiring manufactures to "lock down" devices however there is a much impact that will have as follows.

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

I am not very familiar with R&D; however, we all know the scientific process. People who are doing R&D need to be able to debug and change parameters that would allow them to do their jobs. Having binaries that they can not edit, audit, or replace with their own, would prevent them from doing their job and perhaps bettering wifi.

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

We all know manufactures like to keep things at cost, as such things like security updates are sometimes held back, due to distributing patches and cost required to actually find and fix these critical bugs. As such we as individuals and as employees that support critical company infrastructure may need to be able to put in our own firmware and patches to ensure the security of our networks. Having manufactures take care of security will only make it difficult for individuals and enterprises to pick up the slack, so to speak.

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

As you may or not be aware, individuals in the FOSS community have solved very big problems when they have actually been allowed access to audit and contribute to code for wifi drivers, graphic drivers, etc. By leaving up to the manufacture, you are doing to make it possibly difficult for passionate users that want to contribute to your technology and thus, you will lose these resources.

\*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.

personally, I like to use hardware where I can load DDWRT on the router. I can also think of two companies that are using their own software to provide service to their users. We would likely have to either find alternatives or see how much we would have to pay, just to have the feature to adapt our own binaries/firmware. Personally I would be willing to pay a little extra to have the ability to have my own binaries; although I am not sure of these two companies, I don't represent them in anyway.

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: Larry

Last Name: Boles

Mailing Address: 100 NE 6TH AVE 223

City: HOMESTEAD

Country: United States

State or Province: FL

ZIP/Postal Code: 33030

Email Address: GIVEROFDOOM@COMCAST.NET

Organization Name:

Comment: I am totally against this new rule. We have enough government regulations controlling Armature Radio, and digital based communications. There is no benefit to anyone with these new rules other then to regulate the people.

I do understand as members of a commission your jobs are to create rules and regulations. Every once in a while the rules and regulations are a benefit to us all. All to often like these new proposed rules the only benefit is to the government and more control over the people.

How about you guys leave this one alone and spend a good day on the golf course?

Sincerely,

Larry A Boles

KM4KPU

I am totally against this new rule. We have enough government regulations controlling Armature Radio, and digital based communications. There is no benefit to anyone with these new rules other then to regulate the people.

I do understand as members of a commission your jobs are to create rules and regulations. Every once in a while the rules and regulations are a benefit to us all. All to often like these new proposed rules the only benefit is to the government and more control over the people.

How about you guys leave this one alone and spend a good day on the golf course?

Sincerely,

Larry A Boles

KM4KPU

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: Phil

Last Name: Heid

Mailing Address: 227 Main Street

City: North Creek

Country: United States

State or Province: NY

ZIP/Postal Code: 12853

Email Address: philphun@gmail.com

Organization Name: null

Comment: This bad for people and slows innovation and advance of technology. People bought and own these devices.

They should be free to do anything they want with them that doesn't harm or interfere with other people.

This bad for people and slows innovation and advance of technology. People bought and own these devices. They should be free to do anything they want with them that doesn't harm or interfere with other people.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Moon

Last Name: Quddus

Mailing Address: 16 Pomeroy Street

City: Cardiff

Country: United Kingdom

State or Province: South Glamorgan

ZIP/Postal Code: CF10 5GS

Email Address: moonquddus@gmail.com

Organization Name: null

Comment: This is the worst idea I've ever heard. I have a WiFi adapter on my PC, and I would hate to have it locked down; unable to install any other OS. Aren't regulations meant to prevent things like monopolies? Why are you handing one to Microsoft on a silver platter?

This is the worst idea I've ever heard. I have a WiFi adapter on my PC, and I would hate to have it locked down; unable to install any other OS. Aren't regulations meant to prevent things like monopolies? Why are you handing one to Microsoft on a silver platter?

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: Shaun

Last Name: Reich

Mailing Address: 459 Bernhardt Dr

City: Buffalo

Country: United States

State or Province: NY

ZIP/Postal Code: 14226

Email Address: Sreich02@gmail.com

Organization Name: null

Comment: This is an absolutely terrible step backwards. When I buy hardware , I deserve to be able to modify it as I see fit. Locking these systems down just results in a worse experience for everyone. It also stifles competition. Eg openwrt and dd-wrt, two of the most common roms for routers, have had a feature set such that it has forced routers from large companies to incorporate such necessary features.

I'm allowed to work on my car, I should always be allowed to work on my electronics.

Additionally, this is even worse of an idea these r recent years and onto the future, where routers and software all over the world are getting exploits weekly.. We need to be able to patch these ourselves.

This is an absolutely terrible step backwards. When I buy hardware , I deserve to be able to modify it as I see fit. Locking these systems down just results in a worse experience for everyone. It also stifles competition. Eg openwrt and dd-wrt, two of the most common roms for routers, have had a feature set such that it has forced routers from large companies to incorporate such necessary features.

I'm allowed to work on my car, I should always be allowed to work on my electronics.

Additionally, this is even worse of an idea these r recent years and onto the future, where routers and software all over the world are getting exploits weekly.. We need to be able to patch these ourselves.

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: M

Last Name: Corish

Mailing Address: 1 Queen street

City: Charlottetown

Country: Canada

State or Province: Prince Edward Island

ZIP/Postal Code: C1a4h4

Email Address: null

Organization Name: null

Comment: Regulations lime this will be of no help, other than to hinder the ability for people to be able to innovate, explore and improve devices. Having no ability to flash a custom ROM for an android phone, or being able to install a UNIX/Linux operating system also hinders work in areas such as computer science, and development of applications in general.

Please understand the ramifications of doing something like this affects no one else other than those with the ability to help innovate.

Regulations lime this will be of no help, other than to hinder the ability for people to be able to innovate, explore and improve devices. Having no ability to flash a custom ROM for an android phone, or being able to install a UNIX/Linux operating system also hinders work in areas such as computer science, and development of applications in general.

Please understand the ramifications of doing something like this affects no one else other than those with the ability to help innovate.

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: Josh

Last Name: D

Mailing Address: 2052 October Dr

City: Durham

Country: United States

State or Province: NC

ZIP/Postal Code: 27703

Email Address: joshuadorion@gmail.com

Organization Name: null

Comment: I respectfully ask the FCC not to implement any rule that would take away the ability to install software of my choosing on my router. This not only allows me to extend the functionality of my router, but also fix many issues (security and otherwise) before the vendor can. With these rules, we would be relying entirely upon the manufacturer to fix security holes, instead of the much larger open-source community.

In addition, there have been many other issues that have cropped up on older hardware where the vendor has dropped support. Thanks to users of the older hardware, new firmware versions continue to come out to fix these issues as they occur.

These rules would be extremely limiting, and although I understand the \*purpose\* of them, I feel as though they would primarily affect users of these devices negatively, rather than positively.

I respectfully ask the FCC not to implement any rule that would take away the ability to install software of my choosing on my router. This not only allows me to extend the functionality of my router, but also fix many issues (security and otherwise) before the vendor can. With these rules, we would be relying entirely upon the manufacturer to fix security holes, instead of the much larger open-source community.

In addition, there have been many other issues that have cropped up on older hardware where the vendor has dropped support. Thanks to users of the older hardware, new firmware versions continue to come out to fix these issues as they occur.

These rules would be extremely limiting, and although I understand the \*purpose\* of them, I feel as though they would primarily affect users of these devices negatively, rather than positively.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Michael

Last Name: Keller

Mailing Address: 1911 W Easton Place

City: Tulsa

Country: United States

State or Province: OK

ZIP/Postal Code: 74127

Email Address: keller.michael.s@gmail.com

Organization Name:

Comment: Locking down devices is, figuratively speaking, throwing out the baby with the bath water.

If I can't modify software in products I own, then I don't really own those products.

Enforce RF limits the proper way, by enforcement actions against infringing individuals.

Don't make it hard or impossible for hobbyists to make their devices more usable.

Locking down devices is, figuratively speaking, throwing out the baby with the bath water.

If I can't modify software in products I own, then I don't really own those products.

Enforce RF limits the proper way, by enforcement actions against infringing individuals.

Don't make it hard or impossible for hobbyists to make their devices more usable.

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: Francesco

Last Name: Marcelli

Mailing Address: 505 Cummer Avenue

City: Toronto

Country: Canada

State or Province: Ontario

ZIP/Postal Code: M2K2L8

Email Address: ginoboytoronto@yahoo.com

Organization Name:

Comment: Thank you for the proposed revisions overall. However, there is concern regarding the restrictions on allowing alternate firmware for various wireless routing switch equipment (aka home routers). There are various manufacturers which benefit from proven, vetted open-source derived firmware that has been successfully implemented. These updates have also been implemented into production/official firmware releases by some manufacturers (such as ASUS). Products that have reached end of life formal support gain additional longevity potentially by use of alternate firmware being supported. To deny these benefits (inferred and verified) is poor choice for empowering users and manufacturers alike.

Thank you for the proposed revisions overall. However, there is concern regarding the restrictions on allowing alternate firmware for various wireless routing switch equipment (aka home routers). There are various manufacturers which benefit from proven, vetted open-source derived firmware that has been successfully implemented. These updates have also been implemented into production/official firmware releases by some manufacturers (such as ASUS). Products that have reached end of life formal support gain additional longevity potentially by use of alternate firmware being supported. To deny these benefits (inferred and verified) is poor choice for empowering users and manufacturers alike.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Karl

Last Name: Bolingbroke

Mailing Address: 347 Pointe Loma Blvd

City: Lake St Louis

Country: United States

State or Province: MO

ZIP/Postal Code: 63367

Email Address:

Organization Name:

Comment: I strongly urge you to reconsider the proposed ban on firmware modifications for WiFi routers. This is something that is very commonly done today, not only by individuals experimenting, but by businesses trying to create a new, derivative product. I myself have considered using this approach--buying off-the-shelf WiFi routers and modifying the firmware to provide higher security than what is commercially available, and then selling the modified routers. This type of business adds value, but would become illegal under the proposed rule change.

I urge you to consider the full impact of the rule change to existing businesses and to the new, disruptive businesses that will create our future technologies.

Thank you for your time,

Karl Bolingbroke

I strongly urge you to reconsider the proposed ban on firmware modifications for WiFi routers. This is something that is very commonly done today, not only by individuals experimenting, but by businesses trying to create a new, derivative product. I myself have considered using this approach--buying off-the-shelf WiFi routers and modifying the firmware to provide higher security than what is commercially available, and then selling the modified routers. This type of business adds value, but would become illegal under the proposed rule change.

I urge you to consider the full impact of the rule change to existing businesses and to the new, disruptive businesses that will create our future technologies.

Thank you for your time,

Karl Bolingbroke

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Derek

Last Name: Hoffman

Mailing Address: 605 4th Ave S

City: South St Paul

Country: United States

State or Province: MN

ZIP/Postal Code: 55075

Email Address:

Organization Name:

Comment: I am writing to respectfully request that the FCC not adopt any rules that would limit consumer's ability to install software or firmware on computing devices that they have legally purchased and own.

1. Wireless research depends on the ability of researchers to access and modify these devices in the development of new and exciting communications systems.
2. Everyday users and consumers need to have the ability to modify devices in order to fix security issues that the original manufacture has chosen to ignore or simply not fix in a timely manner.
3. Many businesses use customized software/firmware on Wifi routers to provide Hotspot services to their customers. These rules would prevent these small businesses access to this extra source of revenue.

I am writing to respectfully request that the FCC not adopt any rules that would limit consumer's ability to install software or firmware on computing devices that they have legally purchased and own.

1. Wireless research depends on the ability of researchers to access and modify these devices in the development of new and exciting communications systems.
2. Everyday users and consumers need to have the ability to modify devices in order to fix security issues that the original manufacture has chosen to ignore or simply not fix in a timely manner.
3. Many businesses use customized software/firmware on Wifi routers to provide Hotspot services to their customers. These rules would prevent these small businesses access to this extra source of revenue.

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: Lewis

Mailing Address: 13743 SW Leah Terrace

City: Tigard

Country: United States

State or Province: OR

ZIP/Postal Code: 97224-1593

Email Address: davelewis.pdx@gmail.com

Organization Name:

Comment: I'd respectfully argue against any rule that prevents the user from being able to install any open source software on a router, smart phone or any other device that has software on it that can "expire" due to outdated security measures on those devices.

I have two specific examples of what I'm talking about. First, wireless telephone ISPs (Verizon and AT&T for example) have a horrible record of loong term support on devices that they have sold. After about 18 months after the device went on the market the product updates are abandoned. These vendors want to sell you a new phone. Being able to flash updated software, often by 3rd party developers, that include improved security measures is a benefit to the consumer so that they can extend the benefits of their smart phone investment.

In the second case, the same abandonment by vendors applies to routers. Security protocols are updated and the user needs to be able to update their own equipment when vendors have stopped supplying updates.

As the power output of these devices seem to be the root of this proposed rules change I'd make two suggestions.

First, place the maximum power constraints on the manufacturers of the device radios. Provide rules that prevent software manipulation of maximum power output.

Second, supply measuring devices to investigators who can go on site to any places suspected to be causing interference caused by exceeding the power output. This was done by the FCC in the 50's and 60's for both CB radio and amateur radio. Why not do this instead of reducing user flexibility and raising costs to the user?

Thanks for giving me the opportunity to respond to your proposed rules changes.

I'd respectfully argue against any rule that prevents the user from being able to install any open source software on a router, smart phone or any other device that has software on it that can "expire" due to outdated security measures on those devices.

I have two specific examples of what I'm talking about. First, wireless telephone ISPs (Verizon and AT&T for example) have a horrible record of loong term support on devices that they have sold. After about 18 months after the device went on the market the product updates are abandoned. These vendors want to sell you a new phone. Being able to flash updated software, often by 3rd party developers, that include improved security measures is a benefit to the consumer so that they can extend the benefits of their smart phone investment.

In the second case, the same abandonment by vendors applies to routers. Security protocols are updated and the user needs to be able to update their own equipment when vendors have stopped supplying updates.

As the power output of these devices seem to be the root of this proposed rules change I'd make two suggestions.

First, place the maximum power constraints on the manufacturers of the device radios. Provide rules that prevent software manipulation of maximum power output.

Second, supply measuring devices to investigators who can go on site to any places suspected to be causing interference caused by exceeding the power output. This was done by the FCC in the 50's and 60's for both CB radio and amateur radio. Why not do this instead of reducing user flexibility and raising costs to the user?

Thanks for giving me the opportunity to respond to your proposed rules changes.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Clinton

Last Name: Popovich

Mailing Address: 9557 W San Juan Cir #301

City: Littleton

Country: United States

State or Province: CO

ZIP/Postal Code: 80128

Email Address: crpopovich@kernelcommando.org

Organization Name: null

Comment: Doing this will further put users at the mercy of big business. currently cheap off the shelf routers can be modified to do what expensive routers can. You are taking away our freedom and giving it to big business once again. This will also enable router manufacturers to remove features of products i purchased. Please rethink this move.

Doing this will further put users at the mercy of big business. currently cheap off the shelf routers can be modified to do what expensive routers can. You are taking away our freedom and giving it to big business once again. This will also enable router manufacturers to remove features of products i purchased. Please rethink this move.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jonathan

Last Name: O'Neil

Mailing Address: 277 Patton Dr.

City: Pearl

Country: United States

State or Province: MS

ZIP/Postal Code: 39208

Email Address:

Organization Name: Individual

Comment: FCC,

This requirement is misguided and very likely to be chilling across a broad spectrum of the wireless device industry in several ways that taken together have a great deal more negative impact than any positive impact intended.

For instance:

- 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.

Surely some language carving out an exception for after market and / or open source firmwares could be added or some other compromise reached short of the current plan.

Thanks for your consideration.

FCC,

This requirement is misguided and very likely to be chilling across a broad spectrum of the wireless device industry in several ways that taken together have a great deal more negative impact than any positive impact intended.

For instance:

- 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.

Surely some language carving out an exception for after market and / or open source firmwares could be added or some other compromise reached short of the current plan.

Thanks for your consideration.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ronald

Last Name: Ruble

Mailing Address: 4509 W 170th Street

City: Cleveland

Country: United States

State or Province: OH

ZIP/Postal Code: 44135

Email Address: ronruble.5@gmail.com

Organization Name:

Comment: Restricting the right to update firmware opens up consumers to an unending slew of security issues. Many WIFI Routers and simiilar devices are released to the public and never properly updated for security vulnerabilities. Replacing the firmware with alternatives in the only protection available,

Restricting the right to update firmware opens up consumers to an unending slew of security issues. Many WIFI Routers and simiilar devices are released to the public and never properly updated for security vulnerabilities. Replacing the firmware with alternatives in the only protection available,

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: Richardson

Mailing Address: 6007 10 ave NW

City: Edmonton

Country: Canada

State or Province: Alberta

ZIP/Postal Code: t6l 3a5

Email Address:

Organization Name:

Comment: Hello,

the proposed rules would stifle industry and creativity for many people, blocking firmware upgrades / open source development for many platforms. There should be availability for choice.

Please reconsider the rules on this, to allow for custom firmwares to be loaded onto devices by the consumer, as well as the manufacturer.

Hello,

the proposed rules would stifle industry and creativity for many people, blocking firmware upgrades / open source development for many platforms. There should be availability for choice.

Please reconsider the rules on this, to allow for custom firmwares to be loaded onto devices by the consumer, as well as the manufacturer.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: John

Last Name: Kruse

Mailing Address: 4880 Curly Horse Dr

City: Center Valley

Country: United States

State or Province: PA

ZIP/Postal Code: 18034

Email Address: jkruser@gmail.com

Organization Name:

Comment: As an engineer with practical experience in RF design, I feel that the proposed rules would be detrimental to customers best interests, despite the good intentions of concept.

While the quality of stock firmware in new devices has been improving, limiting a customers ability to replace often buggy, slow, or poorly documented proprietary code with open source code with better understood features solves many more problems than it creates.

There is also the practical side of the requirements, based on a long line of broken digital locks in consumer electronics, it is highly unlikely that these rules would keep programmers out of the devices they want to alter.

As an engineer with practical experience in RF design, I feel that the proposed rules would be detrimental to customers best interests, despite the good intentions of concept.

While the quality of stock firmware in new devices has been improving, limiting a customers ability to replace often buggy, slow, or poorly documented proprietary code with open source code with better understood features solves many more problems than it creates.

There is also the practical side of the requirements, based on a long line of broken digital locks in consumer electronics, it is highly unlikely that these rules would keep programmers out of the devices they want to alter.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Michael

Last Name: McBride

Mailing Address: 166 Valley St

City: Providence

Country: United States

State or Province: RI

ZIP/Postal Code: 02909

Email Address: mpmcbride7@yahoo.com

Organization Name:

Comment: I would like to address my concern with the FCC's current proposed changes. In specific I am concerned about the phrase "grantees would have to implement well-defined measures to ensure that certified equipment is not capable of operating with RF-controlling software for which it has not been approved. "

There are a number of RF products (home Wi-Fi routers probably the most commonly encountered) which provide a basic set of hardware for communication.

The current regulations allow for end users (customers who bought and now own the hardware) to install their own software packages which may provide additional security measures to their device.

Your regulation would prevent the home user from securing their device with advanced software systems.

As the US enters the age of "the internet of things" where appliances, tablets, network attached storage devices, DVR's, home automation and technologies not yet fully developed all need access to the internet it will be IMPERATIVE that the home user is able to secure their home from network intrusion.

The FCC will be strangling the effort of the home user to provide high quality security to their network with this ruling.

I urge the FCC to reword the regulation so that the end user is capable of installing whatever software they feel is appropriate for the device to increase the security of the device. If the FCC feels the need for additional control this control should be specified (i.e. "new software installation can not be allowed if it allows for the transmittal of RF signals outside the signal band of the original software") or something to that effect.

The FCC has a mandate to protect telecommunications and other electronic communications but the overhanded prohibition on installing new software on devices is an overreach when more finely tuned regulations will suffice.

Please consider projects such as: OpenWRT (<https://openwrt.org/>), DD-WRT (<https://en.wikipedia.org/wiki/DD-WRT>), and Tomato (<http://www.polarcloud.com/tomato>)

Your ruling would prohibit end users from installing these more secure firmware systems leaving their networks open to attacks.

I would like to address my concern with the FCC's current proposed changes. In specific I am concerned about the phrase "grantees would have to implement well-defined measures to ensure that certified equipment is not capable of

operating with RF-controlling software for which it has not been approved. "

There are a number of RF products (home Wi-Fi routers probably the most commonly encountered) which provide a basic set of hardware for communication.

The current regulations allow for end users (customers who bought and now own the hardware) to install their own software packages which may provide additional security measures to their device.

Your regulation would prevent the home user from securing their device with advanced software systems.

As the US enters the age of "the internet of things" where appliances, tablets, network attached storage devices, DVR's, home automation and technologies not yet fully developed all need access to the internet it will be IMPERATIVE that the home user is able to secure their home from network intrusion.

The FCC will be strangling the effort of the home user to provide high quality security to their network with this ruling.

I urge the FCC to reword the regulation so that the end user is capable of installing whatever software they feel is appropriate for the device to increase the security of the device. If the FCC feels the need for additional control this control should be specified (i.e. "new software installation can not be allowed if it allows for the transmittal of RF signals outside the signal band of the original software") or something to that effect.

The FCC has a mandate to protect telecommunications and other electronic communications but the overhanded prohibition on installing new software on devices is an overreach when more finely tuned regulations will suffice.

Please consider projects such as: OpenWRT (<https://openwrt.org/>), DD-WRT (<https://en.wikipedia.org/wiki/DD-WRT>), and Tomato (<http://www.polarcloud.com/tomato>)

Your ruling would prohibit end users from installing these more secure firmware systems leaving their networks open to attacks.

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: Luke

Last Name: Hall

Mailing Address: 3101 E 203rd St

City: Westfield

Country: United States

State or Province: IN

ZIP/Postal Code: 46074

Email Address:

Organization Name:

Comment: Just stating my piece regarding the proposed regulation changes to U-NII band radios. As a tinkerer and hobbyist, I believe that the proposed changes will hinder a great deal of technological freedom that we currently have. These changes locking down the radios from modification only serves to make what projects are common within hackerspaces largely illegal when those projects are harmless to the original manufacturers. There are already regulations in place which serve the purpose of protecting the bands which are restricted. So long as individuals are not directly or indirectly infringing upon the rights of the patent holder or violating any current standing laws in how they are modifying these pieces of hardware and software, why do you see it as necessary to impose further restrictions rendering simple, harmless projects as illegal?

Thank you for any consideration and I hope that if you move forward with the proposed regulation that it is refined to account for those of us who do operate within the spectrum of the law.

Just stating my piece regarding the proposed regulation changes to U-NII band radios. As a tinkerer and hobbyist, I believe that the proposed changes will hinder a great deal of technological freedom that we currently have. These changes locking down the radios from modification only serves to make what projects are common within hackerspaces largely illegal when those projects are harmless to the original manufacturers. There are already regulations in place which serve the purpose of protecting the bands which are restricted. So long as individuals are not directly or indirectly infringing upon the rights of the patent holder or violating any current standing laws in how they are modifying these pieces of hardware and software, why do you see it as necessary to impose further restrictions rendering simple, harmless projects as illegal?

Thank you for any consideration and I hope that if you move forward with the proposed regulation that it is refined to account for those of us who do operate within the spectrum of the law.

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: Hunter

Last Name: Morgan

Mailing Address: 1211 University Terrace Apt E

City: Blacksburg

Country: United States

State or Province: VA

ZIP/Postal Code: 24060-8413

Email Address: automaticgiant@gmail.com

Organization Name:

Comment: Please stop the limiting of our freedoms:

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 stop the limiting of our freedoms:

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: benjamin

Last Name: deering

Mailing Address: 16 Katahdin st

City: Bangor

Country: United States

State or Province: ME

ZIP/Postal Code: 04401

Email Address:

Organization Name:

Comment: Preventing users from updating firmware on RF devices they own is a bad idea.

Innovation in the field of embedded RF devices is happening so much faster than the speed of regulation, that the FCC should not attempt to stifle it. IoT has potential to be the great technology transformation of the 2010's but only if hackers are allowed to develop their new ideas.

Device manufacturers fail to provide needed security updates for their RF SDR devices and the hacker community has stepped in with innovations like open-wrt, dd-wrt, etc to fill the need.

Preventing users from updating firmware on RF devices they own is a bad idea.

Innovation in the field of embedded RF devices is happening so much faster than the speed of regulation, that the FCC should not attempt to stifle it. IoT has potential to be the great technology transformation of the 2010's but only if hackers are allowed to develop their new ideas.

Device manufacturers fail to provide needed security updates for their RF SDR devices and the hacker community has stepped in with innovations like open-wrt, dd-wrt, etc to fill the need.

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: James

Last Name: Heyneman

Mailing Address: 8587 Gold Leaf Ln

City: Dublin

Country: United States

State or Province: OH

ZIP/Postal Code: 43016

Email Address: heyneman.james@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: Emil

Last Name: Asdf

Mailing Address: emilio@tfwno.gf

City: Jamestown

Country: United States

State or Province: AK

ZIP/Postal Code: 10-110

Email Address: emilio@tfwno.gf

Organization Name:

Comment: I have to say that this is a very bad idea. This restricts the user from customizing the hardware, and it generally disrespects ones freedoms. I say no.

I have to say that this is a very bad idea. This restricts the user from customizing the hardware, and it generally disrespects ones freedoms. I say no.

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: Hollabaugh

Mailing Address: 54 Haytown Rd.

City: Lebanon

Country: United States

State or Province: NJ

ZIP/Postal Code: 08833

Email Address: haytown@embarqmail.com

Organization Name:

Comment: Simply put, I do not agree with this legislation. This infringes on my ability and right to use the software of my choice on hardware products I buy. As an amateur radio operator and software engineer I fully understand the reasoning behind the proposed changes and find it is not needed at all.

Simply put, I do not agree with this legislation. This infringes on my ability and right to use the software of my choice on hardware products I buy. As an amateur radio operator and software engineer I fully understand the reasoning behind the proposed changes and find it is not needed at all.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Nick

Last Name: LeClair

Mailing Address: 383 Rollingwood Dr.

City: Newport

Country: United States

State or Province: NC

ZIP/Postal Code: 28570

Email Address: nnmleclair@mailccc.net

Organization Name:

Comment: I'm writing this in opposition to the proposed software security requirements for U-NII devices. The proposed software security rules will hinder third-party open-source wireless router software development by end-users being locked out of loading non-OEM approved firmware.

This will also be a hindrance to amateur radio operators who wish to create/upgrade/expand wireless mesh networks as this requires flashing wireless routers with firmware from a third-party. Firmware provided by most wireless router OEM's typically does not provide the capabilities to create a wireless mesh network. Lastly, demanding that an entire device be locked down if it contains a U-NII radio seems extremely heavy-handed approach to a small problem. The commission's resources would be better spent dealing with actual RFI.

I'm writing this in opposition to the proposed software security requirements for U-NII devices. The proposed software security rules will hinder third-party open-source wireless router software development by end-users being locked out of loading non-OEM approved firmware.

This will also be a hindrance to amateur radio operators who wish to create/upgrade/expand wireless mesh networks as this requires flashing wireless routers with firmware from a third-party. Firmware provided by most wireless router OEM's typically does not provide the capabilities to create a wireless mesh network. Lastly, demanding that an entire device be locked down if it contains a U-NII radio seems extremely heavy-handed approach to a small problem. The commission's resources would be better spent dealing with actual RFI.

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: Taimoor

Last Name: Qureshi

Mailing Address: 1205 Gladstone dr

City: Rockville

Country: United States

State or Province: MD

ZIP/Postal Code: 20851

Email Address: Taimoorq@gmail.com

Organization Name: null

Comment: This is a terrible idea. Stop interfering with devices owned by private citizens.

This is a terrible idea. Stop interfering with devices owned by private 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: Alex

Last Name: Rusk

Mailing Address: 15311 N. 2120th Ave

City: Geneseo

Country: United States

State or Province: IL

ZIP/Postal Code: 61254

Email Address: nelith999@gmail.com

Organization Name: null

Comment: Locking down mobile devices only adds to the ridiculous restrictions put into place by most carriers and makes it exceptionally hard to get security updates to their devices in a reasonable time. I have the Moto X 2013 through Verizon and have only seen one update in the last year, which was to fix 911 calling not working properly (which took a long time to release). There are still no signs of a fix for the stagefright vulnerability coming through. In an open and unlocked phone, custom ROM developers are adept at implementing these fixes quickly, along with improving the user experience.

This measure seems to be intended to prevent people from using these devices in harmful ways, but they will always be able to find a new way to do that. If anything, this measure would reduce the security of the average person against such an attack.

Locking down mobile devices only adds to the ridiculous restrictions put into place by most carriers and makes it exceptionally hard to get security updates to their devices in a reasonable time. I have the Moto X 2013 through Verizon and have only seen one update in the last year, which was to fix 911 calling not working properly (which took a long time to release). There are still no signs of a fix for the stagefright vulnerability coming through. In an open and unlocked phone, custom ROM developers are adept at implementing these fixes quickly, along with improving the user experience.

This measure seems to be intended to prevent people from using these devices in harmful ways, but they will always be able to find a new way to do that. If anything, this measure would reduce the security of the average person against such an attack.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: joe

Last Name: nloggs

Mailing Address: 78 Dixon drive florham park

City: orange county

Country: United States

State or Province: NJ

ZIP/Postal Code: 09737

Email Address: paddy844@live.com

Organization Name: null

Comment: This is a very bad idea this is a free country and I should be allowed to do what I want

This is a very bad idea this is a free country and I should be allowed to do what I want

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: Regis

Last Name: Trashuns

Mailing Address: 1234 Main Street

City: Atlanta

Country: United States

State or Province: GA

ZIP/Postal Code: 30309

Email Address: null

Organization Name: null

Comment: Modifications are the sole reason we have technology improvements. Without free ideas, we wouldn't advance this far. Besides it's immoral. Leave it alone.

Modifications are the sole reason we have technology improvements. Without free ideas, we wouldn't advance this far. Besides it's immoral. Leave it alone.

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: Macfarlan

Mailing Address: 3115 Ivydale Drive

City: Charlotte

Country: United States

State or Province: NC

ZIP/Postal Code: 28212

Email Address: tmacfarlan@gmail.com

Organization Name:

Comment: As a consumer who has modified the software on his personal home router, I would be in violation of this new rule. This is unfortunate since the modification allows me to have a more secure home networking environment, as well as an enriched administration experience.

Since the rules will disallow modification of the radio firmware in the 5Ghz range and modern home routers utilize a "SoC" or System on Chip, the CPU and wireless firmware are integrated into a single chip and one cannot be modified without the other.

Manufacturing is unlikely to change their practice since it would drive up complexity and cost. This leaves the consumer with a locked-in, insecure, and disappointing experience.

Please reconsider the rules as proposed. Thank you.

As a consumer who has modified the software on his personal home router, I would be in violation of this new rule. This is unfortunate since the modification allows me to have a more secure home networking environment, as well as an enriched administration experience.

Since the rules will disallow modification of the radio firmware in the 5Ghz range and modern home routers utilize a "SoC" or System on Chip, the CPU and wireless firmware are integrated into a single chip and one cannot be modified without the other.

Manufacturing is unlikely to change their practice since it would drive up complexity and cost. This leaves the consumer with a locked-in, insecure, and disappointing experience.

Please reconsider the rules as proposed. Thank you.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Alberto

Last Name: Marquez

Mailing Address: 714 Rollerton Rd. Apt 106

City: Charlotte

Country: United States

State or Province: NC

ZIP/Postal Code: 28205

Email Address: almarquez182@hotmail.com

Organization Name:

Comment: FCC, please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices, 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. Thanks!

FCC, please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices, 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. Thanks!

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: Petteri

Last Name: Aimonen

Mailing Address: Lapiotie 93

City: Espoo

Country: Finland

State or Province: Espoo

ZIP/Postal Code: 01001

Email Address: jpa@fcc.kapsi.fi

Organization Name:

Comment: I oppose the lock-down of WIFI router firmwares. The lock down will limit the use of these devices a lot, while not really stopping radio violations. Those who want to violate regulations will just buy unlocked devices from abroad.

I oppose the lock-down of WIFI router firmwares. The lock down will limit the use of these devices a lot, while not really stopping radio violations. Those who want to violate regulations will just buy unlocked devices from abroad.