

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Chris

Last Name: Maurer

Mailing Address: 812 Ridgewood ave

City: Ames

Country: United States

State or Province: IA

ZIP/Postal Code: 50010

Email Address:

Organization Name:

Comment: This is an awful idea that would stifle economic growth and moreover accelerate our throw away lifestyle, as everything these days has WiFi and would be locked out of updating firmware. Any security holes would be permanent and more it less brick a device. Please please do not enact this new rule

This is an awful idea that would stifle economic growth and moreover accelerate our throw away lifestyle, as everything these days has WiFi and would be locked out of updating firmware. Any security holes would be permanent and more it less brick a device. Please please do not enact this new rule

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Eugene

Last Name: Spagnuolo

Mailing Address: 51 Lakeside road

City: Mount Kisco

Country: United States

State or Province: NY

ZIP/Postal Code: 10549

Email Address: gene@teleology.com

Organization Name:

Comment: This proposal simply destroys any attempt to modify routers. It's only gain is for router manufacturers who want their devices to become obsolete.

Every modified router is a router that is not in the garbage, and not landfill. It's re-purposing older devices would have gone to waste.

Router modification is how we continue to secure our routers against hacking and security holes.

It is simply more regulation, and a limitation of our freedoms to use our devices to our liking. There is no general benefit or welfare. It's regulation to sell more devices, limiting the rights of Americans so that manufactures can continue to make money.

This proposal simply destroys any attempt to modify routers. It's only gain is for router manufacturers who want their devices to become obsolete.

Every modified router is a router that is not in the garbage, and not landfill. It's re-purposing older devices would have gone to waste.

Router modification is how we continue to secure our routers against hacking and security holes.

It is simply more regulation, and a limitation of our freedoms to use our devices to our liking. There is no general benefit or welfare. It's regulation to sell more devices, limiting the rights of Americans so that manufactures can continue to make money.

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: Pittman

Mailing Address: 355 West Ustick Road

City: Meridian

Country: United States

State or Province: ID

ZIP/Postal Code: 83646

Email Address:

Organization Name:

Comment: I vehemently oppose the proposed requirement, "We propose to modify the SDR-related requirements in Part 2 of our rules based in part on the current Commission practices regarding software configuration control. To minimize the potential for unauthorized modification to the software that controls the RF parameters of the device, we propose that grantees must 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."

I will assume good faith in the motive behind this proposed addition, but what problem is it trying to solve and what problems does this solution create? By attempting to authenticate (and thereby restrict the software on the device), the purported intent is to keep the radio within Compliance. This forcible restriction chokes off innovation from all but the well-funded (lobbyist) big businesses who will at best charge a hefty fee to enable a third party to provide authorized software. On the other hand, all such software restrictions are imperfect and will fail to stop a sophisticated attacker. As such, this flawed attempt at a preventative control will fail to stop the intended criminal and it will harm smaller innovators in this space. Additionally, consumers will have reduced market choices for products that they own, since as a direct result of this proposal, replacement firmware for home routers will either become cost prohibitive to cover the third party fees or completely unavailable if the vendor chooses not to allow a third party to write software for the device that the consumer purchased.

All in all, this sounds more like an attempt by lobbyists for the original equipment manufacturers to squeeze out the competition by manipulating regulations.

I vehemently oppose the proposed requirement, "We propose to modify the SDR-related requirements in Part 2 of our rules based in part on the current Commission practices regarding software configuration control. To minimize the potential for unauthorized modification to the software that controls the RF parameters of the device, we propose that grantees must 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."

I will assume good faith in the motive behind this proposed addition, but what problem is it trying to solve and what problems does this solution create? By attempting to authenticate (and thereby restrict the software on the device), the purported intent is to keep the radio within Compliance. This forcible restriction chokes off innovation from all but the well-funded (lobbyist) big businesses who will at best charge a hefty fee to enable a third party to provide authorized software. On the other hand, all such software restrictions are imperfect and will fail to stop a sophisticated attacker. As such, this flawed attempt at a preventative control will fail to stop the intended criminal and it will harm smaller innovators in this space. Additionally, consumers will have reduced market choices for products that they own, since as a direct result of this proposal, replacement firmware for home routers will either become cost prohibitive to cover the

third party fees or completely unavailable if the vendor chooses not to allow a third party to write software for the device that the consumer purchased.

All in all, this sounds more like an attempt by lobbyists for the original equipment manufacturers to squeeze out the competition by manipulating regulations.

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: Dowley

Mailing Address: PO BOX 338

City: Staatsburg

Country: United States

State or Province: NY

ZIP/Postal Code: 12580

Email Address: j.dowley@hotmail.com

Organization Name:

Comment: The proposed scope is too broad and too restrictive on the class of devices such as WiFi routers and cell phones. PP 18 for example states that any modification of the device's software should be prohibited post FCC ID unless a new ID is applied for and granted. How would a home user modify basic features of a WiFi router (DHCP tables, routing tables, SSID properties) if the devices are all locked down at time of manufacturing?

This lack of limit in scope is very bad and has lots of unintended consequences beyond keeping the radio waves properly shared.

The proposed scope is too broad and too restrictive on the class of devices such as WiFi routers and cell phones. PP 18 for example states that any modification of the device's software should be prohibited post FCC ID unless a new ID is applied for and granted. How would a home user modify basic features of a WiFi router (DHCP tables, routing tables, SSID properties) if the devices are all locked down at time of manufacturing?

This lack of limit in scope is very bad and has lots of unintended consequences beyond keeping the radio waves properly shared.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Adam

Last Name: Sampson

Mailing Address: 15325 Redmond Way Apt Q-280

City: Redmond

Country: United States

State or Province: WA

ZIP/Postal Code: 98052

Email Address: adam.sampson@gmail.com

Organization Name:

Comment: I respectfully request the FCC reconsider its proposal on locking down devices containing wireless radios. Being able to install the software (including firmware) of my choosing is an important aspect of owning electronic devices. The vast innovation of the home computer movement owes itself in great part to the ability of device owners to tinker with and modify the software their devices run. Additionally, as devices get smaller and more connected an increasing number of wireless radio-containing devices will inhabit our homes. Being completely unable to modify these devices by law opens up consumers to vast opportunities to be exploited and used for profit with little to no choice in the matter. Stifling innovation alone is reason for pause in accepting this new regulation, but impinging upon the freedom of citizens to use the hardware that they own in the ways they see fit with no harm being done to their fellow citizens runs counter to the American way of life.

I respectfully request the FCC reconsider its proposal on locking down devices containing wireless radios. Being able to install the software (including firmware) of my choosing is an important aspect of owning electronic devices. The vast innovation of the home computer movement owes itself in great part to the ability of device owners to tinker with and modify the software their devices run. Additionally, as devices get smaller and more connected an increasing number of wireless radio-containing devices will inhabit our homes. Being completely unable to modify these devices by law opens up consumers to vast opportunities to be exploited and used for profit with little to no choice in the matter. Stifling innovation alone is reason for pause in accepting this new regulation, but impinging upon the freedom of citizens to use the hardware that they own in the ways they see fit with no harm being done to their fellow citizens runs counter to the American way of life.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Michael

Last Name: Bourgon

Mailing Address: 10100 chapel springs trl

City: fort worth

Country: United States

State or Province: TX

ZIP/Postal Code: 76116

Email Address: michael\_bourgon@yahoo.com

Organization Name:

Comment: Howdy. I use a wireless device with replaced firmware, and so I'm undoubtedly for the law continuing to allow me to continue. I have several reasons for doing so and I humbly request that the ability be continued.

1) When software bugs or vulnerabilities occur, some routers have had software bugs (some of which allow crackers to get into your home network), and require patches. Some manufacturers release patches, but those can take weeks to release - and some manufacturers simply DON'T release new the patches! At which point your options are limited - or nonexistent. Say it's a critical piece of hardware that you keep running because the company has gone out of business, and changing devices is not easy to do. Or that they find there's a new business model in charging me to fix my own device from mistakes they made originally. Or that they realize if they don't, maybe I'll just buy a brand new unit, even though the old one is under a year old. Which encourages crappy hardware - and in some instances, options are extremely limited and they have a de facto monopoly.

2) There has been a lot of work done by security engineers and the software community in finding bugs in wireless device software and firmware. Preventing them from working on it means that only the bad guys are looking for the exploits. Think of all the news lately about software bugs causing security holes. The bad guys certainly aren't telling us if they find them.

3) Sometimes the device is great, but the software that comes with it is garbage. My wireless router, out of the box, had a lot of subtle issues that took a while to track down. Rather than deal with an onerous return process or convincing the vendor to fix it, I took my own initiative and upgraded the software/firmware to what's called WRT. Now, it works great - but would be an unlawful activity.

Finally, the law technically reads that you're only banning the RADIO firmware, not the ROUTER firmware. However, experience has shown that companies are afraid of breaking the law, and so they'll lock down their hardware, potentially leaving us with insecure wireless devices.

Howdy. I use a wireless device with replaced firmware, and so I'm undoubtedly for the law continuing to allow me to continue. I have several reasons for doing so and I humbly request that the ability be continued.

1) When software bugs or vulnerabilities occur, some routers have had software bugs (some of which allow crackers to get into your home network), and require patches. Some manufacturers release patches, but those can take weeks to release - and some manufacturers simply DON'T release new the patches! At which point your options are limited - or nonexistent. Say it's a critical piece of hardware that you keep running because the company has gone out of business, and changing devices is not easy to do. Or that they find there's a new business model in charging me to fix my own

device from mistakes they made originally. Or that they realize if they don't, maybe I'll just buy a brand new unit, even though the old one is under a year old. Which encourages crappy hardware - and in some instances, options are extremely limited and they have a de facto monopoly.

2) There has been a lot of work done by security engineers and the software community in finding bugs in wireless device software and firmware. Preventing them from working on it means that only the bad guys are looking for the exploits. Think of all the news lately about software bugs causing security holes. The bad guys certainly aren't telling us if they find them.

3) Sometimes the device is great, but the software that comes with it is garbage. My wireless router, out of the box, had a lot of subtle issues that took a while to track down. Rather than deal with an onerous return process or convincing the vendor to fix it, I took my own initiative and upgraded the software/firmware to what's called WRT. Now, it works great - but would be an unlawful activity.

Finally, the law technically reads that you're only banning the RADIO firmware, not the ROUTER firmware. However, experience has shown that companies are afraid of breaking the law, and so they'll lock down their hardware, potentially leaving us with insecure wireless 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: John

Last Name: Hundley

Mailing Address: 24708 Napa ct.

City: Valencia

Country: United States

State or Province: CA

ZIP/Postal Code: 91355

Email Address: JThundley@JThundley.com

Organization Name:

Comment: I understand that bad things can happen if a person instructs a wireless radio to broadcast out of range, but that isn't a good reason for barring people from controlling the hardware that they own. Yes, there should be a rule saying that one is not permitted to interfere with other radio signals, but the wrong way to do that is to force someone to only use the proprietary software that was shipped with their device. Please don't lock out open source enthusiasts as well as tinkerers, the ends don't justify the means.

I understand that bad things can happen if a person instructs a wireless radio to broadcast out of range, but that isn't a good reason for barring people from controlling the hardware that they own. Yes, there should be a rule saying that one is not permitted to interfere with other radio signals, but the wrong way to do that is to force someone to only use the proprietary software that was shipped with their device. Please don't lock out open source enthusiasts as well as tinkerers, the ends don't justify the means.

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: Rausch

Mailing Address: 19115 E. Country Hollow

City: Orange

Country: United States

State or Province: CA

ZIP/Postal Code: 92869

Email Address:

Organization Name:

Comment: Please do not implement rules that restrict the rights of technological device users to install the (legally procurable) software they wish on the devices they own. Part of what makes America great is our upholding of individual liberties, and this rule would attack those liberties. The institution of this rule will certainly stunt sales of the products it applies to: this regulation removes the rights of users to replace default proprietary, or non-free, software on their purchased hardware with FOSS (Free and Open Source Software), which respects users' rights. This incompatibility with full software freedom would be a deal-breaker in a purchasing decision for me and many others. Thanks for upholding the rights of the American people, and please continue to do so by shutting down this rule.

Regards,

Benjamin Rausch

Please do not implement rules that restrict the rights of technological device users to install the (legally procurable) software they wish on the devices they own. Part of what makes America great is our upholding of individual liberties, and this rule would attack those liberties. The institution of this rule will certainly stunt sales of the products it applies to: this regulation removes the rights of users to replace default proprietary, or non-free, software on their purchased hardware with FOSS (Free and Open Source Software), which respects users' rights. This incompatibility with full software freedom would be a deal-breaker in a purchasing decision for me and many others. Thanks for upholding the rights of the American people, and please continue to do so by shutting down this rule.

Regards,

Benjamin Rausch

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Adam

Last Name: Selker

Mailing Address: 4225 Sw. Agate Ln.

City: Portland

Country: United States

State or Province: OR

ZIP/Postal Code: 97239

Email Address: aselker319@gmail.com

Organization Name: null

Comment: As a computer hobbyist and electronics enthusiast, I am nervous regarding the proposed rules which would require devices operating around 5GHz to resist firmware modification. More generally, I do not believe that rules restricting what programs a user may run on their electronics are rarely necessary and are often harmful.

In this particular case, these rules would harm anyone who uses 5GHz routers -- essentially, anyone who uses WiFi. Open-source router firmware allows users to fix bugs and improve security, as well as adding whatever features they would like to. In essence, this creates wealth at no cost, since the firmware is free and is usually easy to install. The rules would also impact anyone who wishes to use router hardware for any purpose other than creating WiFi networks, such as communications research.

Lastly, these rules would discourage foreign manufacturers from selling their products in the United States. If a Chinese seller creates a new, low-cost router, they would be required to lock it down -- discouraging buyers globally -- in order to sell it in the United States. Instead, they would be likely to simply not offer the device in the country.

Thank you for maintaining the freedom of American consumers to use their products as they would like.

As a computer hobbyist and electronics enthusiast, I am nervous regarding the proposed rules which would require devices operating around 5GHz to resist firmware modification. More generally, I do not believe that rules restricting what programs a user may run on their electronics are rarely necessary and are often harmful.

In this particular case, these rules would harm anyone who uses 5GHz routers -- essentially, anyone who uses WiFi. Open-source router firmware allows users to fix bugs and improve security, as well as adding whatever features they would like to. In essence, this creates wealth at no cost, since the firmware is free and is usually easy to install. The rules would also impact anyone who wishes to use router hardware for any purpose other than creating WiFi networks, such as communications research.

Lastly, these rules would discourage foreign manufacturers from selling their products in the United States. If a Chinese seller creates a new, low-cost router, they would be required to lock it down -- discouraging buyers globally -- in order to sell it in the United States. Instead, they would be likely to simply not offer the device in the country.

Thank you for maintaining the freedom of American consumers to use their products as they would like.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: William

Last Name: Carpenter

Mailing Address: 19216 90th PL NE

City: Bothell

Country: United States

State or Province: WA

ZIP/Postal Code: 98011

Email Address: bill-federalregister@carpenter.org

Organization Name: self

Comment: To the extent that this regulation would, in practice, prevent independent updates of the non-radio parts of firmware, I think it is a bad policy. Highly integrated devices quite often use a single firmware image for all components. Even though the firmware for different components might be developed independently and in a modular manner, the final firmware images must often be deployed as a single atomic unit.

I understand and am sympathetic with the desire to closely control transmitter operations. The regulations should allow for the use of arbitrary firmware images as long as the manufacturer's radio transmitter firmware component is somehow included as some kind of tamper-proof sealed unit, by digital signature or other means.

Without such a provision, it will be difficult or impossible to apply security or functional updates to a manufacturer's legacy or abandoned devices. Thus, it present a significant obstacle to both good security and third-party innovation.

To the extent that this regulation would, in practice, prevent independent updates of the non-radio parts of firmware, I think it is a bad policy. Highly integrated devices quite often use a single firmware image for all components. Even though the firmware for different components might be developed independently and in a modular manner, the final firmware images must often be deployed as a single atomic unit.

I understand and am sympathetic with the desire to closely control transmitter operations. The regulations should allow for the use of arbitrary firmware images as long as the manufacturer's radio transmitter firmware component is somehow included as some kind of tamper-proof sealed unit, by digital signature or other means.

Without such a provision, it will be difficult or impossible to apply security or functional updates to a manufacturer's legacy or abandoned devices. Thus, it present a significant obstacle to both good security and third-party innovation.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Joel

Last Name: Klein

Mailing Address: 9523 Clement Road

City: Silver Spring

Country: United States

State or Province: MD

ZIP/Postal Code: 20910

Email Address: joel.e.klein@gmail.com

Organization Name:

Comment: For home routers, I think I should be able to change the firmware. A lot of firmware on domestic routers is found to be vulnerable within a few months of its release, and I should have the right as the purchaser to fix that.

For home routers, I think I should be able to change the firmware. A lot of firmware on domestic routers is found to be vulnerable within a few months of its release, and I should have the right as the purchaser to fix that.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Daniel

Last Name: Chateau

Mailing Address: 2100 S Conway Road Apt G4

City: Orlando

Country: United States

State or Province: FL

ZIP/Postal Code: 32812

Email Address: me@danielchateau.com

Organization Name:

Comment: Not being able to modify my router's firmware harms my ability to secure myself from security threats on the Internet as well as from war-driving that could be done near my home. This restriction will do nothing to stop the types of behavior or actions it is attempting to stop and only serves to allow manufacturer's to control the market in a way that will make us all less secure and not allow for us to have the option to improve the hardware that vendors refuse to support with timely and future updates.

Not being able to modify my router's firmware harms my ability to secure myself from security threats on the Internet as well as from war-driving that could be done near my home. This restriction will do nothing to stop the types of behavior or actions it is attempting to stop and only serves to allow manufacturer's to control the market in a way that will make us all less secure and not allow for us to have the option to improve the hardware that vendors refuse to support with timely and future updates.

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: Akshay

Last Name: Bhat

Mailing Address: 3304 Charlemagne Road

City: Pittsburgh

Country: United States

State or Province: PA

ZIP/Postal Code: 15237

Email Address:

Organization Name:

Comment: The proposed regulation can lead to the below drawbacks:

1. Security issues related to router firmware might not be patched in a timely manner by all vendors leading to customer devices getting compromised.
2. Lack of ability for users to install certain software on router (eg: OpenVPN etc.) will limit the choice of routers inturn forcing them to buy more expensive and potentially less capable devices. Consumers will not only have to research the hardware quality/capability of the router but also research about the software capability/stability.
3. Stock firmware on many routers are of poor quality and have stability issues. Some consumers work around that by installing custom firmware. Locking down the firmware will no longer give the ability to do the same.

The proposed regulation can lead to the below drawbacks:

1. Security issues related to router firmware might not be patched in a timely manner by all vendors leading to customer devices getting compromised.
2. Lack of ability for users to install certain software on router (eg: OpenVPN etc.) will limit the choice of routers inturn forcing them to buy more expensive and potentially less capable devices. Consumers will not only have to research the hardware quality/capability of the router but also research about the software capability/stability.
3. Stock firmware on many routers are of poor quality and have stability issues. Some consumers work around that by installing custom firmware. Locking down the firmware will no longer give the ability to do the same.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Eric

Last Name: Busse

Mailing Address: 220 CIRCLE DR W

City: CANASTOTA

Country: United States

State or Province: NY

ZIP/Postal Code: 13032

Email Address: embusse@gmail.com

Organization Name: -

Comment: Please do not implement these rules as they will take away the ability of users to install the software of their choosing on their computing devices. Additionally these rules will also limit:

- 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 implement these rules as they will take away the ability of users to install the software of their choosing on their computing devices. Additionally these rules will also limit:

- 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: David

Last Name: Erickson

Mailing Address: 1175 Glin Ter

City: Sunnyvale

Country: United States

State or Province: CA

ZIP/Postal Code: 94089

Email Address: daviderrickson@forwardnetworks.com

Organization Name:

Comment: FCC-

Please do not implement rules that take away the freedom for owners to install the software of their choice on their computing devices. There is a long list of limitations inherent in being stuck with running the software provided by manufacturers including:

-Wireless networking research depends on the ability of researchers to investigate and modify their devices. I know because I was involved in the team that was doing this during my PhD at Stanford. Without the ability to replace the software with our own custom versions, this would have potentially prevented the break through research on Software Defined Networking that is now permeating all of the networking ecosystem.

-Manufacturers frequently abandon or provide very limited software updates for devices after they are initially sold, and often there are exploits and vulnerabilities discovered in software that is no longer supported. The only way for an owner of a device with such a problem to solve it is to be able to replace the software.

-Often the capabilities of the software are vastly limited compared to mature open source software such as DD-WRT. This is bad for consumers.

Please also consider what happened with locking cellphones, this was enacted then overridden because consumers deserve the right to have choice, and to operate their devices with the software of their choosing. What made the personal computer market explode, and have all the amazing impact it has had on the world, was the ability for the owner of that computer to put the software and applications of their choosing on it. If it had been locked down from the very beginning, we would be in a very different, and worse, world.

FCC-

Please do not implement rules that take away the freedom for owners to install the software of their choice on their computing devices. There is a long list of limitations inherent in being stuck with running the software provided by manufacturers including:

-Wireless networking research depends on the ability of researchers to investigate and modify their devices. I know because I was involved in the team that was doing this during my PhD at Stanford. Without the ability to replace the software with our own custom versions, this would have potentially prevented the break through research on Software Defined Networking that is now permeating all of the networking ecosystem.

-Manufacturers frequently abandon or provide very limited software updates for devices after they are initially sold, and

often there are exploits and vulnerabilities discovered in software that is no longer supported. The only way for an owner of a device with such a problem to solve it is to be able to replace the software.

-Often the capabilities of the software are vastly limited compared to mature open source software such as DD-WRT. This is bad for consumers.

Please also consider what happened with locking cellphones, this was enacted then overridden because consumers deserve the right to have choice, and to operate their devices with the software of their choosing. What made the personal computer market explode, and have all the amazing impact it has had on the world, was the ability for the owner of that computer to put the software and applications of their choosing on it. If it had been locked down from the very beginning, we would be in a very different, and worse, world.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Sean

Last Name: Davis

Mailing Address: 2735 W. Heroy Ave.

City: Spokane

Country: United States

State or Province: WA

ZIP/Postal Code: 99206

Email Address: kuhlboarder@yahoo.com

Organization Name:

Comment: Please continue to allow end users to modify their wifi hardware's firmware as they wish. Sometimes OEMs leave gaping loopholes in security, or simply orphan old hardware in pursuance of newer hardware. Allowing me to modify my own hardware makes it much more possible for everyone to be secure.

Thank you!

Please continue to allow end users to modify their wifi hardware's firmware as they wish. Sometimes OEMs leave gaping loopholes in security, or simply orphan old hardware in pursuance of newer hardware. Allowing me to modify my own hardware makes it much more possible for everyone to be secure.

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: Stephen

Last Name: Zurcher

Mailing Address: 89-235 Pua Avenue

City: Waianae

Country: United States

State or Province: HI

ZIP/Postal Code: 96792

Email Address: steve+fccwifi@szurcher.com

Organization Name: Self employed

Comment: Please reconsider the portions of this proposal that will affect the use of open source wifi routing software. You will probably (hopefully) receive a large number of comments that cover the points made at [https://libreplanet.org/wiki/Save\\_WiFi](https://libreplanet.org/wiki/Save_WiFi) from folks who can make much more informed (on a technical or experience level) arguments. So I will just submit my own anecdotal experience with wifi routers:

Every brand name router I've used (be it Linksys, Netgear, Belkin, etc.) has had absolutely horrible firmware. The systems could not maintain operation for more than a few days at best without requiring a hardware reset. Every single one of them had this problem. If anything, Linksys got WORSE after being absorbed into Cisco. Enter the glorious wonder that is DD-WRT and its children, Tomato being the one I use with my ASUS wifi router. It just runs. It does not fail after a few hours, a few days, weeks, etc. It especially doesn't fail, work for an hour and then fail again. The router is a piece of equipment that once set up should be absolutely transparent to the users. With the functional open source firmware not only is this the case, but the benefits as listed at the Save WiFi site such as improved security and freedom from vendor indifference are also applied.

I recognize the need for regulation of shared communication mediums. My hope is the clever folk both working for the regulatory committees and from the public can produce a proposal that promotes and encourages innovative improvements and functionality from all sectors, rather than quashing same through increased restrictions and licenses.

Thank you for your time and your efforts in preserving the rights and freedoms we all enjoy.

Please reconsider the portions of this proposal that will affect the use of open source wifi routing software. You will probably (hopefully) receive a large number of comments that cover the points made at [https://libreplanet.org/wiki/Save\\_WiFi](https://libreplanet.org/wiki/Save_WiFi) from folks who can make much more informed (on a technical or experience level) arguments. So I will just submit my own anecdotal experience with wifi routers:

Every brand name router I've used (be it Linksys, Netgear, Belkin, etc.) has had absolutely horrible firmware. The systems could not maintain operation for more than a few days at best without requiring a hardware reset. Every single one of them had this problem. If anything, Linksys got WORSE after being absorbed into Cisco. Enter the glorious wonder that is DD-WRT and its children, Tomato being the one I use with my ASUS wifi router. It just runs. It does not fail after a few hours, a few days, weeks, etc. It especially doesn't fail, work for an hour and then fail again. The router is a piece of equipment that once set up should be absolutely transparent to the users. With the functional open source firmware not only is this the case, but the benefits as listed at the Save WiFi site such as improved security and freedom from vendor indifference are also applied.

I recognize the need for regulation of shared communication mediums. My hope is the clever folk both working for the regulatory committees and from the public can produce a proposal that promotes and encourages innovative improvements and functionality from all sectors, rather than quashing same through increased restrictions and licenses.

Thank you for your time and your efforts in preserving the rights and freedoms we all enjoy.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Julian

Last Name: Lowe

Mailing Address: 32 Bradley Bow Road

City: Jericho

Country: United States

State or Province: VT

ZIP/Postal Code: 05465

Email Address:

Organization Name:

Comment: Require the radio (and only the radio) transmitter be locked buy the manufacture.

This rule will dampen or kill development, while hackers and off shore vendors will continue to provide what you are banning.

You are not solving the problem, only hiding it under 'rules'

Require the radio (and only the radio) transmitter be locked buy the manufacture.

This rule will dampen or kill development, while hackers and off shore vendors will continue to provide what you are banning.

You are not solving the problem, only hiding it under 'rules'

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Brandon

Last Name: Fotiu

Mailing Address: 7755 22 Mile Road #183340

City: Shelby Township

Country: United States

State or Province: MI

ZIP/Postal Code: 48317

Email Address:

Organization Name:

Comment: Hello,

<br>

My name is Brandon Fotiu and I oppose the FCC establishing rules that will remove the legal right of users to install the software of their choosing on devices they own. In the past I have benefited from the efforts of many talented programmers who have modified and extended the functionality of my hardware devices, including cell phones and wireless routers. There have been many cases where enthusiasts have taken up abandoned hardware and software projects and have sparked renewed interest and economic impact and I support these projects.

As long as these projects reside within the bounds of the law and public safety I believe it is our right to modify consumer electronics and I strongly oppose any efforts to limit that right.

Thank you for your time,

Brandon Fotiu

7755 22 Mile Road #183340

Shelby Township MI, 48317

Hello,

<br>

My name is Brandon Fotiu and I oppose the FCC establishing rules that will remove the legal right of users to install the software of their choosing on devices they own. In the past I have benefited from the efforts of many talented programmers who have modified and extended the functionality of my hardware devices, including cell phones and wireless routers. There have been many cases where enthusiasts have taken up abandoned hardware and software projects and have sparked renewed interest and economic impact and I support these projects.

As long as these projects reside within the bounds of the law and public safety I believe it is our right to modify consumer electronics and I strongly oppose any efforts to limit that right.

Thank you for your time,

Brandon Fotiu  
7755 22 Mile Road #183340  
Shelby Township MI, 48317

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: Seegar

Last Name: Mason

Mailing Address: 146 Apollo Road

City: River Falls

Country: United States

State or Province: WI

ZIP/Postal Code: 54022

Email Address: rigortortoise@yahoo.com

Organization Name:

Comment: This rule will defeat amateur hobbyists and professional researchers alike by essentially close-sourcing all software for these devices. In the past there have been security lapses in firmware distributed by many large manufacturers of wi-fi devices which they either couldn't or wouldn't fix. It was the open source firmware community that stepped up to resolve these issues. This rule would effectively make that action illegal, instead putting security fixes into the hands of people who can't or won't fix them, essentially willfully allowing our networks to grow more and more insecure.

Furthermore, our technological advancement is frequently made by small actors working on their own or in small groups with low or no funding. By placing this additional restriction on them, their advancements will instead be made in other countries by people with more freedom to innovate.

Respectfully,  
Seegar Mason

This rule will defeat amateur hobbyists and professional researchers alike by essentially close-sourcing all software for these devices. In the past there have been security lapses in firmware distributed by many large manufacturers of wi-fi devices which they either couldn't or wouldn't fix. It was the open source firmware community that stepped up to resolve these issues. This rule would effectively make that action illegal, instead putting security fixes into the hands of people who can't or won't fix them, essentially willfully allowing our networks to grow more and more insecure.

Furthermore, our technological advancement is frequently made by small actors working on their own or in small groups with low or no funding. By placing this additional restriction on them, their advancements will instead be made in other countries by people with more freedom to innovate.

Respectfully,  
Seegar Mason

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: Rosie

Last Name: Lukeywood

Mailing Address: rosielukeywood@gmail.com

City: Sheffield

Country: United Kingdom

State or Province: South Yorthshire

ZIP/Postal Code: s66fb

Email Address:

Organization Name:

Comment: I ask the FCC to not implement these rules that would stop people from changing the software on there computers.

It would unesseserly take away pepoles freedom to run there own systems on wifi capable computers if there is certain behavior that it causes problem then this behavior should be banned there is no reason to ban pepole running custom software on there computers.

I ask the FCC to not implement these rules that would stop people from changing the software on there computers.

It would unesseserly take away pepoles freedom to run there own systems on wifi capable computers if there is certain behavior that it causes problem then this behavior should be banned there is no reason to ban pepole running custom software on there computers.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Joseph

Last Name: Philipps

Mailing Address: 105 Susan Ln.

City: Cheektowaga

Country: United States

State or Province: NY

ZIP/Postal Code: 14225-2105

Email Address: joe.philipps@gmail.com

Organization Name:

Comment: It seems a little silly that a recurring theme of this simplification process means testing laboratories do not have to meet criteria (mentioned in 9. as "accredited testing facilities would not be required"). It would seem anyone could call themselves a testing lab and submit reports which could say just about anything, without having any grounding in reality. It would not seem to meet any goals of the Commission concretely (for example, keeping harmful interference in control). It would seem rather like the fox guarding the henhouse.

Coming up with the concept of "family of products" under the same ID is a really good idea.

If you will insist that radio-controlling software be subject to control of the manufacturer (for example, so as to prevent operating the radio outside of authorized frequencies), I think consumers need some rules for protection so that only those functions strictly relevant to the Commission's/public's interests be under the manufacturer's control. As an example, this is already practiced in the cellular domain with Android's RIL (Radio Interface Layer). As I understand it, this is a separate ROM partition which holds only code relevant to operating a device's transceivers. Within the constraints of the device itself (amount of RAM, available processor cycles, etc.) and the RIL API, the "main" software is free to invoke the RIL in any way it chooses, and it is the responsibility of the RIL code to make sure the device cannot operate illegally. Furthermore, I think it's feasible that these should be field-upgradeable (and not be "set in stone" at time of manufacture) because there is plenty of digital signature technology which can validate the authenticity of RIL code updates before such updates are stored into EEPROM/flash or used. In fact, software flaws are found "all the time," so field updates are essential.

In other words, all other implementation details, such as WPA, IP, routing, logging, or other higher level protocols and functions **MUST** remain user-defined. For consumers to be protected, a manufacturer/vendor should be prohibited from disallowing the use of software not provided by them; again, there needs to be isolation to **ONLY** the software for the RIL.

It seems a little silly that a recurring theme of this simplification process means testing laboratories do not have to meet criteria (mentioned in 9. as "accredited testing facilities would not be required"). It would seem anyone could call themselves a testing lab and submit reports which could say just about anything, without having any grounding in reality. It would not seem to meet any goals of the Commission concretely (for example, keeping harmful interference in control). It would seem rather like the fox guarding the henhouse.

Coming up with the concept of "family of products" under the same ID is a really good idea.

If you will insist that radio-controlling software be subject to control of the manufacturer (for example, so as to prevent operating the radio outside of authorized frequencies), I think consumers need some rules for protection so that only those functions strictly relevant to the Commission's/public's interests be under the manufacturer's control. As an example, this is already practiced in the cellular domain with Android's RIL (Radio Interface Layer). As I understand it, this is a separate ROM partition which holds only code relevant to operating a device's transceivers. Within the constraints of the device itself (amount of RAM, available processor cycles, etc.) and the RIL API, the "main" software is free to invoke the RIL in any way it chooses, and it is the responsibility of the RIL code to make sure the device cannot operate illegally. Furthermore, I think it's feasible that these should be field-upgradeable (and not be "set in stone" at time of manufacture) because there is plenty of digital signature technology which can validate the authenticity of RIL code updates before such updates are stored into EEPROM/flash or used. In fact, software flaws are found "all the time," so field updates are essential.

In other words, all other implementation details, such as WPA, IP, routing, logging, or other higher level protocols and functions **MUST** remain user-defined. For consumers to be protected, a manufacturer/vendor should be prohibited from disallowing the use of software not provided by them; again, there needs to be isolation to **ONLY** the software for the RIL.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Paul

Last Name: Taylor

Mailing Address: 17 Currajong Avenue

City: Mount Evelyn

Country: Australia

State or Province: Victoria

ZIP/Postal Code: 3796

Email Address:

Organization Name:

Comment: These Rules would hurt WiFi communication progress and innovation across the world.

Specifically:

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

\* The world needs 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.

These Rules would hurt WiFi communication progress and innovation across the world.

Specifically:

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

\* The world needs 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.